Szép új világ - vegyék, vigyék

2008.01.03. 16:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: usb biztonság sandisk online kulcs mentés aes

Az **Aldous Huxley-tól kölcsönvett cím** korántsem a véletlen műve: kicsit elméláztunk azon, hogy merre is halad ez a számítógépes világ. Abba még muszáj valahogy beletörődni, hogy hová és hogyan fejlődnek a kártevők: hiszen sokszor kész helyzet elé állítanak minket. A **válaszlépések, a fejlesztés, a választott biztonság** viszont rajtunk múlik, és abban jó lenne a helyes irányt legalább körvonalakban kirajzolódva szimpatikusnak látni.

Az hogy a "Ne kattints fiacskám gyanús email mellékletre" típusú figyelmeztetés kissé már elavult, érezzük. Illetve **nem is csak erről van szó**, inkább talán az a lényeg, hogy emellett jöhet **a kártevő már URL link formájában csevegő üzenetben, szerepelhet fertőzött vagy eltérített weboldalakon, sőt blogbejegyzésekben is** - a repertoár széles.

A december egyik slágere volt **a fürdőruhás lányokkal ékesített mikulásos képernyővédő**, jár a plusz pont a rosszfiúk csapatának - ötletekért nem kell a szomszédba menniük. Ami apró érdekesség, mosolyogni való, az most megmutatjuk két különböző gyártó:
az F-Secure weblogjában

és Symantec weboldalán:

Akár a régi Füles újságot is idézheténk: **fedezzen fel EGY különbséget a két kép között** :-) Emitt láthatólag éberen őrködnek erkölcseink felett!

Visszatérve a vizionalizált jövőképre, olvasom magyarul, olvasom angolul, de valahogy akkor sem lesz szimpatikus, inkább nagytesósnak érzem a dolgot a magam paranoid kis agyával: **ki akarja, hogy a dokumentumairól másolat készüljön, maradjon, őrződjön**, gyűjtenek így is épp elég adatot rólam.

Írtam már egy helyen, hogy hőőő, meg hajrá a Google, és minden ilyesmi, de azért **a cégem összes dokumentumát mégsem tenném önként és dalolva az online irodájukba**. Igaz valamelyest **szépít a dolgon a beépített AES (Advanced Encryption Standard) titkosítási lehetőség**. Persze ez is egy üzleti modell: a termék megvásárlása után 6 hónapig ingyenes az online mentés, utána viszont már évente 30 dollárért kell/lehet hosszabbítanunk. Szóval - bár különben le a kalappal a SanDisk előtt - nekem ez az online irány valahogy kevésbé tetszik, de biztos lesz olyan, akinek ez majd bejön.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/283175

Kommentek:

Nincsenek hozzászólások.

Adathalászat a Facebook oldalán

2008.01.04. 16:23 | Csizmazia István [Rambo] | 6 komment

Címkék: facebook phising adathalászat

Még meg sem száradt a tinta a januári PC World "Megtévesztők - Social engineering és ami mögötte van" című cikken, máris jön és jön az újabb neverending story: **ezúttal a Facebook közösségi portálra startoltak rá az adathalászok**.

Itt tényleg már csak a kutya oltási bizonyítványának száma hiányzik, meg a "kulcs a lábtörlő alatt" szlogen...

Jó időben kaptuk a fülest, dél körül még mindig elérhető volt a phising oldal. Igazából itt **most kell tennünk egy kis kitérőt**. A legtöbb biztonsági és hírportál van annyira körültekintő, hogy amíg aktív, élő egy ilyen link, kitakarja egy részét vagy az URL egészét, nehogy az olvasók megfertőződjenek, ezért **néha nehéz kideríteni a teljes címet**.

Egy korábbi postban magunk is így jártunk el. Azért némi kis munkával - ami **a kitakart rész rajzprogrammal való visszacsalogatása**, illetve olyan blogok nézegetése, ahol még a nem kitakart cím szerepel, eredményre szokott vezetni a nyomozásan.

MIVEL A LINK MÉG MINDIG ÉLŐ, senki ne adja meg ott az adatait!

Kártékony kód ezúttal nem próbálkozott letöltődni, az ESS figyelt közben. A Netcraft Toolbar viszont szépen jelez a phisingre

Értékes adatokkal segíthetjük a kolléga adatgyűjtését ;-)

Ennél feltűnőbb figyelmeztető jelzés aztán már tényleg nem létezik

Íme a domain adatai

Rápillantunk a Phistank adatbázisra, jelzi szépen, hogy ez egy már lejelentett, ellenőrzött adathalász oldal.

Egy biztos, sajnos nem ez volt az utolsó ilyen felhasználók hasonló elleni kísérlet.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/284688

Kommentek:

zvaragabor 2008.01.27. 13:54:52

Tegnap áldozatul estem egy phising oldalnak. Barátom jött MSN-en, hogy egy haverja küldött egy linket, ami egy olyan oldalra mutat, ahol ha bejelentkezek az msn-es felhasználó/jelszavammal, akkor megmutatja, hogy mely partnereim tiltottak le. (Azt nem mondta, hogy az ő haverja csak úgy elküldte-e a linket, vagy ajánlotta.) Mondom jól van, kipróbálom, a kíváncsoság nagy úr. Adatok be, tiltó partnerek megjelennek az oldalon. Rendben, mondom biztos, nem zavar, hogy pár ember letiltott, én is tiltottam már le 1-2 partnert. Azonban tegnap este szól egyik partnererem, hogy küldtem egy linket. Mondom: -Mivan? :S Én nem küldtem semmilyen linket. -Kértem, hogy küldje el, hogy mit küldtem, bemásolt egy linket, rákattintok, és bejön ez az ominózus oldal. Itt kicsit furcsállottam, hogy más a link, mint amit én kaptam először a barátomtól, és más, mint az oldal igazi URL-je. De már este volt, agy nem foglalkoztam vele a továbbiakban. Ma nővérem ír, hogy ő is kapott egy linket. Kérdezte, hogy vírus-e, mondom nem, de ne kattintson rá. Itt tudatosult bennem, hogy ez egy phising site. Nem sokkal utánna a barátom is ír, hogy ő is küldözget linkeket. Elmagyaráztam neki is, hogy ez nem vírus, hanem egy adathalász akció, gyűjtögetik a

felhasználó/jelszó-t. Szóltam neki, hogy változtassa meg a jelszavát, én is ezt teszem. Aztán eszembe jutott az antivirus.blog, mert itt szoktam látni a Netcraft anti-phising toolbart, gondolom kipróbálom, ha már a Firefox beépítettje nem jelzett. Netcraft telepít, ominózus oldal betölt...hopp...nem tölt, mert a toolbar riaszt, hogy nagy nagy valószínűséggel phising site. Tiltottam, de kíváncsi voltam, hogy mit ír rá a toolbar konkrétan, ezért megnyitottam mégegyszer, ezúttal engedélyeztem. Az oldal új, egy kínai szerveren van.

Jelszavamat megváltoztattam, jó lecke volt legközelebb odafigyelek, hogy mit adok meg, és minek. :)

És az oldal: h..p://www.msnliststatus.com/

zvaragabor 2008.01.27. 14:03:30

Azt elfelejtettem írni, hogy furfangos ám az oldal(vagy aki mögötte áll), mert valószínű úgy küldi tovább a linket, hogy botok jelentkeznek be tömegesen a megszerzett fiókokba, és akkor kiküldik minden elérhető partnernek a linket.

Hopp, a blog motor is furfangos, linkké alakítja a domain címet "" tag nélkül is. :)

zvaragabor 2008.01.27. 14:13:57

Az első hsz-emben a "barátom" csak a haverom, mielőtt még félreértené valaki.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.31. 16:59:18

Szia Gábor!
Köszi a frontvonalról, elsőkézből származó beszámolót, szerintem nem csak neked, hanem mostantól minden olvasónak egy igen tanulságos történet lesz ez, örülök hogy a végén azért kikeveredtél belőle.
Ja és szerintem senki nem értette félre az identitásodat ;-)

zvaragabor 2008.02.01. 17:51:28

Nincs mit. Legalább ilyennel is volt dolgom. Ezt is ki kell próbálni egyszer. :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.03. 22:37:26

Adatainkkal bizniszelnek a közösségi portálok :
www.privatbankar.hu/html/techtud/it.php?kommentar=29072

Veszélyes új eszközök

2008.01.07. 14:38 | Csizmazia István [Rambo] | 3 komment

Címkék: usb vírus eszköz új boeing fertőzött victory autostart gyári tweakui

Mi is beszámoltunk már korábban olyan **boltban megjelent, új számítástechnikai gépekről, részegységekről, amelyek a gyártás folyamán fertőződtek meg vírussal, és így kerültek sorozatban a boltok a polcaira**. Stoned.Angelina a noteszgépen, Maxtor és a trójaiak - hogy csak a két legismertebb esetre utaljunk, de **volt már TomTom gyártmányú navigációs eszközön is kártevő**. És bizony volt, aki a karácsonyfa alá tett MP3 lejátszót is vírusmentesnek hitte.

A szóban forgó eszköz egy **Victory LT-200 típusú zenelejátszó, amin hát hogy is mondjuk, a Worm.Win32.Fujack.aa féreg játszotta a prímet**. Nagyon helyesen elmélkedik a cikk a Windowsos gépek Autostart funkciójáról, illetve **ennek kikapcsolása is hasznos** ötletnek számít.

Például a jó kis TweakUI programmal kinderspiel kikapcsolni az automatikus indulási lehetőségeket. A tanulság talán az lehet, hogy a vadonatúj merevlemezeket, memóriakártyákat is **érdemes formattálni** - biztos ami biztos alapon. Na és persze **egy naprakész víruskereső futtatása sem hiányozhat** a kelléktárból.

Amikor éppen nem egy vírus van az új eszközön, akkor viszont **újkeletű sebezhetőségekről kapjuk a híradásokat**, és ez egy USB lejátszónál picivel nagyobb gépnél is okozhat problémát :-O

A Boeing új 787-es Dreamliner modelljénél komoly biztonsági hibára figyelmeztetnek a szakértők: az utasok internetezés közben használt hálózata egy tervezési malőr folytán nincs szétválasztva a gép navigációs, irányítási és hírközlő rendszerétől.

Talán ebből azért valamivel kevesebb volt a karácsonyfák alatt...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Ez történik a weben egy perc alatt
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/288134

Kommentek:

Charlie Brown 2008.01.22. 08:45:41

Csakhogy.. Az USB meghajtókon az autorun.inf nem csak az automatikus indulást definiálja, hanem a duplakattintásos megnyitásra induló default parancsot is! Tehát hiába van kikapcsolva az automatikus futtatás, ha a pendrive duplaklikkes megnyitása azonnal lefuttatja a meghajtóra elrejtett vírust. Ez továbbvihető egy lépéssel, amikor nem új default parancsot hoz létre a vírus szerzője, hanem egy meglévő, ártatlan parancsot "térít el", ez esetben jobbgombos menü/megnyitás -ra is elsőnek a vírus indul. Mióta ezzel szembesültem, minden usb meghajtót csak és kizárólag Total Commanderből nyitok meg. Nem kényelmes, mit mondjak... Ördögért nem lehet a registryben letiltani az usb meghajtókról való programfuttatást?! :((

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 09:12:13

Szia Charlie!
Én is TC hívő vagyok, de szerintem amit te keresel, az a TWeakUI program, azzal pik-pak egyszerűen kikapcsolható minden ilyen autorun dolog...

Charlie Brown 2008.01.22. 10:00:40

Én nem vagyok TC hívő, az a felület kb a DOSszal együtt elavult, de kénytelen vagyok használni, ha egyszer a windowson belül már nem lehet biztonságosan megnyitni egy vacak pendriveot. :(

TweakUI: "PowerToys only work with U.S. English regional settings" :((Azért megnézem, hátha mégis.

Sarah18

2008.01.08. 14:37 | Csizmazia István [Rambo] | 3 komment

A Messengeren kopogtatnak című postra reagált kedves olvasónk, és **egy ropogós, friss trójai támadásáról készült képernyőképpel** örvendeztetett meg minket. A sejtetett 18+ tartalom helyett persze egy backdoor trójai található a ZIP csomagban. Nekünk a fájlnév alapján Wagner B. György nagysikerű könyve, a "Sarah bugyiban - avagy a hazug embert hamarabb utólérni, ha sánta" című nagysikerű műve ugrott be szabad asszociációként - ezt jószívvel ajánljuk mindenkinek lazításképpen vagy csak úgy, látókörtágítás-ügyileg ;-)

A megjelölt **weboldal egy már évek óta tényked legális fórumoldal**, tehát nem egy kifejezetten kártevők terjesztésére szakosodott tiszavirág életű weblap kísérel megmerényelni bennünket.

Az Egyesült Államokban üzemeltettett oldal **bejegyzési adatai és körülményei is tisztának látszanak**.

Ennek ellenére az a bizonyos állomány még mindig elérhető a megjelölt helyről, de szerencsére vírusirtónk a résen volt. VÍRUSIRTÓ NÉLKÜL senki ne próbálkozzon!

Hogy egyáltalán letölthessük, ideiglenesen kikapcsoljuk és megnézzük közelebbről. A "sarah.zip" esetünkben egy "IMG_8783.scr" kiterjesztésű, azaz képernyő védő futtatható állományt rejt magában, a futtatható kód EXE fejléccel rendelkezik és **gyaníthatóan Morphine típusú packer** segítségével van összetömörítve. Itt már **kevés jóindulatot sejthetünk, hiszen a trükkös exepackerek nem csak a kisebb méret okán használatosak, hanem segítségükkel igyekeznek a gyanús kódokat leplezni, illetve a visszafejtésüket nehezíteni**.

A VirusTotallal vizsgálva jól látszik, hogy a jelentősebb víruskeresők már ismerik.

A vizsgálat eredményét nem befolyásolta, hogy a ZIP-et vagy magát az SCR-t vizsgáltuk.

A táblázat alján a Prevx kínál bővebb információt, ebben elég részletesen írnak róla. Spanyolországban és Magyarországon észlelték, legtöbbször WKSSVR.EXE néven bukkant fel és képes processzeket eltéríteni a memóriában, HTTP prokollon keresztül képes másik számítógéppel kommunikálni, és hasonlók, íme itt a részletes lista:

Az **azonnali üzenetküldő programok egyre inkább közkedvelt támadási célpontok a vírusírók számára**, mivel a felhasználók általában **gyanútlanok a kapcsolataikkal szemben, akik gyakran barátok, vagy közeli ismerősök, kollégák**. Ezáltal **könnyebben fogadnak el tőlük fájlokat, linkeket**, hiszen azok nem idegentől, ismeretlen forrásból, hanem egy megbízhatónak vélt személytől érkeznek. Ne tegyük!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/289268

Kommentek:

balint96 2008.01.18. 14:55:39

Hello!
Bocs hogy ilyen későn írok(végül is én adtam az ötletet :-))Kösz hogy ilyen részletesen leírtad, nekem sajna nincs időm,szakértelmem utánanyomozni.Amúgy azt elfelejtettem megírni hogy a vírus anyukámnál az egyik ismerősétől érkezett akit pár héttel azelőtt tiltott le mert valami miatt állandóan újracsatlakozott, a csilingelő hang pedig élénk sztepptáncot okozott a sorban elpattanó idegszálakon :D.

balint96 2008.01.18. 15:00:01

Ui.:Jé,törölték a kwickfix.org-ot(legalábbis nekem nem jön be)

titan 2010.04.27. 10:03:52

Sajnos tapasztalat. Ha a malware-ek gazdái ftp-jelszavakhoz jutnak, ártatlan oldalakra tehetik fel ezeket a programokat. Így "tiszta" környezetből töltődnek le, megbízható forrásúnak tűnnek és mivel a google is csak az ártatlan oldalt fogja büntetni, így gyakorlatilag a fent említett gazdák más f***val verik a csalánt. (Webhosting cégem van, elég sokat küzdöttem már az ügyfelek oldalaiért...)

Antonio Banneres

2008.01.09. 15:44 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hirdetés portál banner fertőzés trójai rbot sdbot spybot

Csekélységem eddig sem jeleskedett **a bannerekre való kattintgatás frontján**, nagyjából egy kezemen meg tudom számolni az elmúlt évekre vonatkozó ilyen eseteket, de hát állítólag az ilyen emberekre is szükség van, ellensúlyozni kell a statisztikákat. (No meg Murphy szerint minden jó valamire, ha másra nem, hát elrettentő példának.) A mondanivaló jelen esetben az lehetne, hogy akik nem ennyire szélsőségesen szakadárok és elutasítóak az ilyen szimpatikus hirdetési formákkal szemben, azoknak nehéz idők jönnek: **fellendülőben vannak a neves webhelyeken előforduló, rosszindulatú kódokat terjesztő bannerek**.

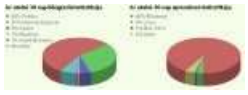
Komoly olvasótábort fogadó hír- és közösségiportálok esetében komoly veszélyt jelent az ilyesmi, és most pontosan ez történt. A Heise.de jelentése többek közt a MySpace (aki nem is először áll támadások középpontjában), az Excite valamint a svájci Blick magazin weboldalán történt esetekről számol be. A fertőzött bannerek SDBot, RBot, SpyBot trójai programokat próbáltak telepíteni a látógatok gépeire különféle biztonsági rések kihasználásával. Emellett hasonlóan a Hamis kémirtók című cikkben szereplő esetekhez, itt is felajánlkozik egy "ingyenes" alkalmazás, ami PerformanceOptimizer-nek hívja magát - magyarul rendszeroptimalizáló vagy gyorsító lehetne - de ez **csak hamis riasztásokat jelenít meg nemlétező problémákról**, amiket viszont már csak a fizetős verzió javítana ki - állítólag. (egy bölcs amerikai közmondás szerint ami nem romlott el, azt nem kell megjavítani)

Kamu a köbön: nem létező problémákkal riogatnak

A védekezéssel kapcsolatos intelmek felsorolása kicsit már imamalmosan hangzik, ezt a részt mostantól már csak kopi-pasztával fogom mindig idehelyezni:

Védekezésül érdemes naprakész víruskeresővel és kémirtóval felfegyverkezni, rendszeresen frissíteni az operációs rendszerünket és a használt alkalmazásainkat (**nem megfeledkezve a Flash Player, QuickTime Player és hasonló programokról sem**), amihez a Windows automatikus frissítését, valamint a Secunia Software Inspectort is segítségül hívhatjuk.

Ha egy mód van rá, használjunk az Internet Explorer helyett biztonságosabb Opera vagy FireFox böngészőt, utóbbira remek beépülő modulok léteznek, **például a JavaScriptek automatikus futását megakadályozó** NoScript plugin.



Az antivirus.blog olvasói már eddig is **haladócsoportosnak számítottak**, örvendetesen sokan érkeznek Tűzrókával és Operával (ez utóbbi nem az, amikor valakit leszúrnak, de utána még félóráig énekel).

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/290984

Kommentek:

Nincsenek hozzászólások.

Izgalmakkal teli iPhone firmware frissítés

2008.01.10. 21:41 | Csizmazia István [Rambo] | Szólj hozzá!

Leáldozóban az email mellékletben érkező vírusoknak, lassan már a bejglisütésben megőszült nagymamák, és az alkalmi számítógép használó tisztes háziasszonyok is fújják, hogy ezekkel vigyázni kell. A weboldalakon, bannerekben közlekedő kártékony kódokkal való együttélést, védekezést most tanuljuk, de **van itt még egy érdekes terület, a hackelt, feltört, nem gyári, ismeretlenek által készített szoftverek világa**, ami sok érdekes kérdést felvet. Most az iPhone firmware esetében azt, hogy mi történhet, ha valaki az iPhone 1.1.3 frissítést letöltötte az internetről.

Réges régen, mikor még a hülyét pontos j-vel írták, azt a dajkamesét kaptuk az orcánkba, **azért kell ám jogtiszta szoftvert használni, mert ezzel a módszerrel eredményesen megóvhatjuk magunkat a vírusoktól**. Az összefügges persze valamilyen szinte létezik, de ennél a sommás megállapításnál sokkal árnyaltabban. Azóta már sok víz lefolyt a Dunán, egészen fiatal lánykák és ősz halántékú aggastyánok kivételével kevesen adnak hitelt egy-az-egyben ilyesféle híreszteléseknek, meg aztán a sok fertőzött gyári szoftver és hardvereszköz ha nem is megcáfolta, de alaposan megtépázta ezt a tételt. Láttunk aztán fake letöltéseket, trójaival fertőzött keygent, és **jogosan merül fel a kérdés, biztos hogy vakon meg kell bízni minden újonnan kijött programban, javításban, segédprogramban?** A többségében igen, de mindig lesznek majd kivételek, amikről előbb (jó heurisztika megfogja) vagy utóbb (weblogok, biztonsági cikkei megírják) kiderül majd a csalafintaság.

Az új programokkal kapcsolatosan idősebbek és katonaviseltek még emlékezhetnek arra az igen hasznos mondásra, miszerint okos ember csak akkor kezd el használni egy operációs rendszert, ha arra már kijött az első Service Pack. További izgalmas eset volt, amikor az Ubuntu frissítő szervereit törték fel hackerek, és mérgezték meg a letölthető frissítő csomagokat. Szóval nem árt időnként kételkedni, mindemellett mitikusan Robin Hoodként tiszteljük azokat, aki leleményesen mégis lehetővé tették, hogy szolgáltatófüggetlenül használható legyen ez a jó kis telefon.

Most azonban a modmyiphone oldalon olvashattuk az első figyelmeztetést arról, hogy **senki ne telepítse az 1.1.3-as csomagot**. Persze itt is volt kedvcsináló: a csomag segítségével disk módba kapcsolhatjuk a telefont, vagyis hordozható flashmeghajtóként is használhatjuk, valamint a hangrögzítéssel (voice recording mode) is bővül az igénybevehető funkciók köre. Ezek után ki nem tölt le egy ilyen jó kis updatet? Az 1.1.3 program **eltávolítási kísérleténél derül ki csak, hogy az a telepítéskor hasznos állományokat is eltávolít, illetve telepítésnél már felülírt**. A Symantec jelentéséből kiderül, hogy az úgynevezett Erica Utilities (ezek parancssori segédprogramok) és az OpenSSH esnek áldozatul az esetnél. Bár igazi veszélyt nem okoz a dolog, tippet ad a kártevőkészítőknek, és ez már baj.

Figyelmeztetésüket csak megszívlelni lehet: **megbízhatatlan helyről származó csomagot NE telepítsünk a telefonunkra sem**. Sajnos gyaníthatóan ezt az első próbákozást továbbiak fogják majd követni.

Utóirat: ha valakinek van gyakorlati tapasztalata, közvetlen élménye erről a bizonyos 1.1.3-as frissítésről, ezúton kérjük, ossza meg velünk komment formájában, előre is köszönjük.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/291885

Kommentek:

Nincsenek hozzászólások.

Kovács Nikolett ma korán kelt...

2008.01.14. 13:08 | Csizmazia István [Rambo] | 5 komment

Címkék: spam iwiw ip ügynök kovács trójai kéretlen nikoletta hyde

Jó húsz éve, amikor a világ még nem TV-re, hanem a Kossuth rádióra ébredt, nagyon szerettem Havel József párizsi kiküldött tudósító reggeli jegyzeteit, szellemesek voltak. Emlékszem volt egy rész, aminek az volt a címe: **Párizsban a kakasok ma korán keltek**. Fentnevezett hölgy talán már ekkor is rádiót hallgatott, esetleg olvasta a Három kismalac című alapművet, és ennek hatása alatt már **hajnali 3:40-kor ~~kiment a répaföldre~~, akarom mondani ismeretlenül és KÉRETLENÜL beterítette jópár IWIW-es emberke postaládáját** csúnya spamjével.

A reggeli postabontás az alábbi levelet hozta nekünk és több ismerősnek is:

```
Szia!
Bocsi de...
Először bocsánatot szeretnék kérni hogy így ismeretlenül
írok neked, de szerintem ez téged is érdekel!
 Van egy oldal ami azzal foglalkozik hogy, hogyan maradjunk
 névtelenek, és láthatatlanok az interneten, szörfozés közben!
 Na meg így nem tudnak   kitiltani fórumokról, blogokról meg
 ilyenek...
Íme az oldal címe:
http://hidemyip.uw.hu/

 Mégegyszer bocsika a zavarásért!
```

Íme az ajánlott weboldal, ez még működik, a linkek azonban már nem élnek. Nem tudjuk megmondani, hogy sajnos vagy hál' Istennek...

Szép dolog az irgalmas szamaritánus szerepében tetszelegni és jótékonyan segíteni (átvezetni az úttesten a vak nénit, aki eredetelig nem is akart volna átmenni), de itt biztosan nem nemesveretű szándékokról van szó. Kicsit gyanús már **a szöveg fordítása is, több magyartalanságot tartalmaz (pl. jelszavak helyet jelszók**, stb.).

Időközben az állítólagos Kovács Nikolett ki lett tiltva, regisztrációja helyén kráter tátong.

Ha belenézünk az általa belinkelt oldal forrásába, érdekes dolgokra lehetünk figyelmesek. Mondjuk első körben, **aki Windows-1250-es ékezettel készíti a weblapját, sikeres ember nem lehet :-D** Van azonban más izgalmas dolog is, a szemlátomást **tegnap lefoglalt Google hirdetési kód**:

```
<script type="text/javascript"><!--
google_ad_client = "pub-7565379255544103";
//120x600, létrehozva 2008.01.13.
google_ad_slot = "4445184336";
google_ad_width = 120;
google_ad_height = 600;
//--></script>
<script type="text/javascript"
src="http://pagead2.googlesyndication.com/pagead/show_ads.js">

</script>
```

Talán ez gyűjtheti be a részletesebb felhasználói adatokat. Aztán **a lánclevelek és a piramisjátékok világából lehet ismerős a link után látható "/?id=2033" paraméter** is, amely ügynökünk munkáját hivatott naplózni: a sok hasonló ajánló oldal közül a főoldal nyilvántartja, honnan hányan érkeztek és nyilván jutalékot ígérhettek a letöltések és/vagy a shareware programot megvásárlók száma után.

Van persze **egy logikai bukfenc is** benne: tegyük fel valaki anonim akar maradni (ez már azért haladó csoportos kívánság), könnyen megtalálja a módját: Tort használ, proxy mögé áll, nyitott proxykat keresgél és valószínüleg talál is. De ez **a weboldalon jelzett veszélyekre: biztonságban lenni a csúnya hacker bácsik elől, nehogy ellopjanak, töröljenek, módosítsanak adatokat az anonim IP NEM MEGOLDÁS**. A **valódi megoldás egy jó Internet Security csomag - például az ESS a vírus és kémprogramok ellen** is remek, benne plusz **a kétirányú tűzfal, legyen minden program (OS és felhasználói) rendszeresen frissítve**, végül pedig a paranoiásabbak egészítsék ki még **SpyBot és/vagy Spyware Terminatorral, NoScriptes Firefoxxal** és jöjjön hacker... Itt azonban **jól látható, hogy itt a kattintásra akarják rábírni** a gyanútlan és tudatlan netezőt.

Azóta az oldalt is kikapcsolták már.

A DomainTools szerint nincs probléma az oldallal, nem egy friss kínai regisztrációról van szó, bár az adatok szerint a két éve foglalt cím idén február elején lejár.

Tanulság talán az lehet, hogy itthon is ideje figyelmesebben használni a közösségi oldalakat, hiszen külföldi példák mutatják, hogy egyre inkább célpontot jelentenek a kártevő terjesztők számára. **Ha pedig (ügynöki) munkát ajánlanak, akkor ne tartozzon a munkaköri feladatok közé a tömeges kéretlen levélírás se**, inkább legyünk bébiszitterek, mint szabálysértők ;-)

Egyébként pedig megbocsátunk, nincs harag. Jah, és bocsika, de **kéretlen leveleket, kéretlen üzeneteket továbbra SEM várjuk**

fiókjainkba...

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/296809

Kommentek:

buherator · http://buhera.blog.hu 2008.01.14. 18:57:32

"Valószínű, de még bizonyításra váró lehetőség: a segítségükkel hamisítható a digitális aláírás"
Vajon Rivest bácsi tud már erről? XD

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.14. 19:23:42

Halihó :-)
Sőt valószínű, de még bizonyításra váró lehetőség, hogy segítségükkel összecseréli a fogkrémes tubust a cipőkrémes tubussal ;-)

Vidi Rita · http://www.hosnok.hu 2008.01.17. 14:56:45

Szia!
Elég jól egyszerre éreztünk rá erre a témára:))
Sose szerettem órákat iwiw-ezni, de ezek miatt már csak akkor lépek be, ha muszáj:S

Viszont azt veszem észre, hogy a felhasználók meg ott állnak az üzenet előtt tanácstalanul.

Úgyhogy jó, hogy külön erről írtál, mert sokan érdeklődnek, hogy mi a helyzet ezzel és a hasonló üzenetekkel.

Úgy valagba tudnám rúgni a küldőket:))

Egy kis kötözködés: nem Firefoxxal, hanem Firefox-szal:) Ha jól tévedek:)) de lehet, hogy Firefoxszal... nem, inkább a kötőjeles... najó, húzok;)

egy kérdés: nem túlzás ez a spam-ellenes captcha-izé , meg még a regisztrációhoz kötött hozzászólás együtt? ennyire támadják a blog.hus blogokat?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.17. 16:01:25

Szia Rita!
Igen, láttam hogy Csabival konzultáltál :-) Remélem nem égett le a keménylemez .-D
XX VS X-sz ügyben sorry vagyok, a kommentek NEM szerkeszthetőek, ezért az elütések is örökre vasalva maradnak;-)
A Captcha a blog.hu rendszer része, alapszinten jól véd a scriptes automatizált tömeges kommentek ellen, nehogy a szervert túlterhelje valami köbgyök.
Ha már IWIW, te nem kaptál ilyen Dubai MLM izét?
antivirus.blog.hu/2008/01/15/gyujtsunk_emailcimeket_a_nagy_dubai_atve

GYUSZI BACSI · http://www.fizetesem.com 2008.01.22. 17:03:29

ezt a hülyeséget honnan veszed hogy a google gyűjti be a titkos adatokat valami kezdő spammernek ...

különben a NOD32 tök jó, nagyon elégedett vagyok vele és másnak is ajánlom

A selejt bosszúja és a nagybetűs ÉLET

2008.01.15. 09:17 | Csizmazia István [Rambo] | 2 komment

Címkék: windows linux ubuntu hamis biztonsági kockázat

A számítógépes biztonság területén **többnyire pont nem azok szorulnának több segítségre, akik egy ilyen blogot is rendszeresen olvasnak**, hanem azok, akik egyáltalán nem is sejtik, hogy veszélyben vannak, és persze fogalmuk sincs, hogyan védekezhetnének.

Környezetemben két példát is láttam arra, hogy viselkedik egy gyanútlan átlagember. X család kedves, rendes és rendezett anyagi körülmények közt élnek, a számítógépüket főleg a két középiskolás gyerek birtokolja, a szülőknek többnyire elegendő a munkahelyen töltött idő, ők viszonylag ritkábban használják az otthoni gépet: híreket olvasnak, fotókat rendszereznek, TV műsort keresnek.

A gépen kémirtó egyáltalán nincs, csak az XP beépített tűzfala fut (ami ugye közismerten erős;-), és egy valahonnan kapott ősöreg Norton árválkodik rajta. Internet persze fut, böngészés, e-mail, Skype, Messenger, Sztaki szótár, stb. A gyerekek persze **tudják, hogy léteznek frissítések, de mivel a Windows nem legális, ezért direkt kikapcsolták az automatikus frissítéseket**

A másik példában egy idősebb házaspár szerepel: Y-ék, akik - le a kalappal - élénken érdeklődnek az új technikai vivmányok után, és **felnőtt gyereküktől megkapva régi számítógépét, aktívan használják is**: itt nézik meg a menetrendet, az időjárást, itt olvasnak újságot, ingyen hívják skypos ismerőseiket, sőt a kultúrális rendezvényekről is itt tájékozódnak, talán még blogokat is olvasnak, de erre már nem tértünk ki. Itt már legalább egy ingyenes AVG futott a gépen, bár kémprogramról és tűzfalról még életükben nem hallottak.

A nagypapa korú férfi arról panaszkodott, hogy **minduntalan megjelenik egy nem eredeti Windows példány ablak a jobb sarokban, és hogy pár óránként a számítógép lefagy. Ilyenkor ki- és visszakapcsolják**, de egyszer már kértek valakitől segítséget, akkor az illető mint egyetlen lehetséges gyógymódot használva: formázta és újratelepítette a teljes rendszert. Elképzelem, hogy egy ilyen gépen az automatikus ESS csomag milyen csodákra lehetne képes.

ESET Smart Security - az angol már itt van, a magyar nyelvű változat pedig heteken belül megjelenik

Pillantás a hídról a közelmúltba: a Sasser féreg a terjedése érdekében kihasználta a Microsoft MS04-011 jelű sérülékenységét, és ezzel az LSASS.EXE (Local Security Authority Subsystem Service) programban található puffertúlcsordulási hiba miatt távolról történő kódfuttatást tett lehetővé az érintett rendszeren, mely által a támadó teljesen átvehette a távoli számítógép vezérlését.

Az utóbbi időszak tendenciáit nézve egyértelműnek látszik, hogy **a kártékony kódok szinte mindig kihasználható biztonsági réseken keresztül fertőzik meg az áldozatok gépeit**, ezért nehéz nyugodtnak maradni. Ha valaki nem ért hozzá, az önmagában még nem tragédia, de az már igenis az, **ha probléma esetén nincs kitől segítséget kérni (gyerek, rokon, ismerős, munkahelyi rendszergazda, szomszéd Pistike, stb.)**. Itt az illegális Windows miatti frissítés hiánya olyan helyzetet eredményez, mintha nem zárnánk be a lakásunk ajtaját.

Különbség a Windows és a Mac juzerek között ;-)

A nyitottabbak persze próbálhatnak más, biztonságosabb platformokra átállni - igaz a Mac irány ha anyagilag nem is, viszont technikailag valóban kedvez ennek. A másik jó szívvel ajánlható, és ráadásul ingyenes lehetőség a Linux használat lehet, az Ubuntu például hihetetlenül felhasználóbarát, **könnyen konfigurálható, alacsony gépigényű és nagy csapást jelenthet az imperializmusra, hogy az erre a platformra írt vírusok száma mindössze alig néhány tíz - szemben a Windows-os többszázezerhez képest**. Szinte minden Windows alkalmazásnak megtalálható a Linuxos megfelelője, de az ingyenes VirtualBox emulátorral **akár Windows-t is futtathatunk** annak a néhány alkalmazásnak, amelyhez mindenképpen szükséges ez a környezet. A barátkozást eleinte lehet egy Live CD-vel kezdeni, aztán a folytatásból már bármi lehet: multiboot, OS váltás, stb.

Íme egy full-extrás Ubuntu, ingyenes OpenOffice, GIMP, Skype, és sok más földi jó...

Visszatérve a példákra, mit kockáztatnak ezek az emberek? Az X családban a két középiskolás továbbtanulásával valószínűleg megoldódnak a legális operációs rendszer gondjaik a felvételi után, a Campus licenc kedvező feltételeinek köszönhetően, az odafigyelést és hozzáállást azonban már most is komolyabban kellene venniük.

Y-éknak a kb. 20 ezer forint bruttó OEM Windows XP-t javasoltam, úgy tűnik, hajlandóak is erre. Ők talán már egy új rendszert (Linux, Mac) nem igazán tudnának megszokni, de persze az élet még rám cáfolhat a későbbiekben, hiszen érdeklődőek és nyitottak. Arra már nem is tértünk ki a családokkal, vajon bankolnak-e a gépekről, de mindenesetre **szemlátomást nincsenek tudatában, milyen veszélyeknek tették és teszik ki magukat, valamint az összes gépben tárolt adatukat**.

Hiába színes, tudok rajta írni, rajzolni, zenét hallgatni, netezni, ha a frissítésekből ki vagyok zárva, **egy lopott Windows, amihez nincs támogatás, frissítés, csökkent értékű**. Ha semmilyen biztonsági program nem védi az internetes gépet, az csökkent értékű, és igenis konkrét veszélyeknek teszi ki tulajdonosát. Szerintem ezt a biztonsági kockázatot **kellene széleskörűen ismertetni, tudatosítani az úgynevezett "átlagfelhasználói" körrel és máris sokat javulhatna a világ folyása.**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt

- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/296583

Kommentek:

virkid 2008.01.22. 09:41:11

Véleményem szerint a linux nem alternatíva még. A legtöbb gép amit középiskolások használnak általában játékgép. Bármilyen jó az emulátor a win-es tökéletes futást nem lehet megismételni. A mai játékok a gép teljes erőforrását kihasználják. Aki informatikával foglalkozik, tudja, hogy a fejlesztés egyik legnagyobb mozgatórugója a játékok. Nem véletlen a HALO2-Vista kapcsolat sem.
Campus szerződés lejár a felsőoktatási intézményből való kikerüléssel, elvileg ellenőrzi a Microsoft. Tehát ez sem megoldás.
Mindkét esetben látható, hogy a felhasználó nem foglalkozik a biztonsággal, mert úgy gondolja nincs védendő adata.
A megoldás a tiszta (vagy tisztára mosott) win, egy profin beállított védelemmel. (Szentháromság: vírusirtó, spyirtó, tűzfal).
Aminek szintén jogtisztának kéne lenni.
Sasser levétele egy gépről egy szakembernek laza csuklómozdulatnak kell lenni, tehát ezzel példálozni nagyon erős, és marketing szagú.
A szakembert meg kell fizetni, és hozzájuk fordulni. Az autókat sem a szomszéd garázsba szereli az ismerős. Szerencsére.

BenkoG 2008.02.05. 14:58:38

Virkid: a próféta szól belőled, azt gondolom. Még egy két dolgot hadd fűzzek hozzá: Linux azért nem alternatíva, mert a PC-s programok nem futnak rajta.... ez egyfajta rövidlátás, mert az esetek túlnyomó többségében ALAPBÓl tartalmazza az adott Linux disztri azt az alkalmazást, amit a kedves endjúzer hiányol.
Másik az utolsó bekezdésed, amivel mint szerviz nagyon is egyetértek. Azt szoktuk mondani (főleg a mai pénzhiányos-ínséges időkben, amikor inkább új cipőt vesznek a népek a gyereknek a kínaiban mint Windowsot) ráadásul erősen poénosan: a számítestechnikai szerviz legnagyobb konkurrencuája a "Pisti gyerek a szomszéd lépcsőházból, aki ért hozzá".
Sírjak vagy nevessek? Persze a tendenciák az én kedvemtől nem változnak, de próbáljunk meg ebből építeni valamit.

Dubai e-mailcím gyűjtés

2008.01.15. 18:39 | Csizmazia István [Rambo] | 34 komment

Címkék: spam dubai mlm átverés kéretlen

Dubai a világ nyolcadik csodája: az Egyesült Arab Emírségek második legnagyobb városa. Olajkincsének köszönhetően hihetetlen felvirágzás jutott osztályrészéül: hatalmas luxusvillák, fényűző szállodák, de jó is ilyen rohadt sötét, ködös télen ábrándozni, másokat hülyének nézni, nomeg spameket kilóra küldözgetni...

Friss lendületet nyertek hát a magyarnyelvű akciók is, semmivel sem vagyunk lemaradva a kapitalistáktól, illetve egy pár dologban azért picit mégis, de az már túlnyúlik e cikk keretein. **Beesett hát a nagy lehetőség, mosolygós smiley subjecttel ékesített levélben**, Fel hát ti kedves tetemek - énekelhetné Pipacs bácsi, a munkahelyekről azonnal kilépkétek, trallala-trallala, csak ne féljetek, itt a csalhatatlan recept - és csak úgy sorakoznak a címzettek a KÉRETLEN levélben:

Dubai MLM - Az elsöprő lendület

Még nem késő feliratkoznod a jövő bankjába!
Most még ingyen megteheted, köszönve az arab olaj-mágnásoknak és üzletembereknek!

Magyarországon is hódít a Dubai MLM, melyben szédületes tempóban halad a hálózatépítés.
A marketing terv bináris szisztémára épül, mely a legjobb az ismert tervek közül.
Jelenleg az INGYENES előregisztrációk folynak, ennek keretében a közös ágra lehet regisztrálni a tagokat. Ebből adódóan a közös ág fantasztikusan gyorsan épül.
Rögtön cselekedni kell, egy óra késlekedés kb 300 tag elvesztését eredményezi.
Jelentkezz kockázatmentesen!

http://oriental.dubaimlm.com

Semmibe sem kerül, nem kapsz spam-eket!
Egy idő után Bank-kártyát bírsz majd igényelni tőlük!

"A hatalmas kőolajtartalékoknak köszönhetően hihetelenül magas színvonalú az élet Dubaiban. A GDP 33%-a közvetlenül a kőolajtermeléshez kapcsolódik. A jelenlegi felmérések szerint a kőolaj még legalább száz évre elegendő. Az országot off-shore területként tartják számon. Abu-Dzabi és Dubai pénzügyi központ. A GNP becsült értéke 51 milliárd USD. Az 1 főre jutó GDP becsült értéke 21 100 USD körül van. A kivitel 45%-át kizárólag a kőolajtermékek teszik ki. Ezek nagy részét Japánnak, Szingapúrnak adja el..."

Ez a jövő bankja! Internet explorer használata ajánlott a programhoz

Hööhö, ez jó: kapok egy spamet, és az azt ígéri, hogy "**nem kapsz majd spamet**" :-) MegaLOL! A klasszikus elem azonban mégis ez: "**Rögtön cselekedni kell** (nehogy időd legyen gondolkozni), **egy óra késlekedés 300 tag elvesztését eredményezi**. Mézesmadzag kell, jó zsaru - rossz zsaru, fenyegetés és igérgetés kedvező arányú elegye, hatni kell az áldozatra. Ja és persze "**Internet explorer (így kis e-vel írva) használata ajánlott**", mert azt könnyebben lehet activescriptelni, minő meglepetés! NoScriptes FireFox-szal ne akarjál milliomos lenni kisapám vagy Operával, hát nem furcsa?! A "**bankkártyát bírsz igényelni tőlük**" mondat magyartalanságát már nem is hánytorgatom fel. Már tényleg annyi intő jel van, hogy szinte egy állatorvosi lóról szól a poszt :-)

Nem lehet nem észrevenni az újonnan beszervezett ügynökök sisere hadát, mi a 236950-es sorszám tulajdonosától kaptuk. Ha valaki egy új, eddig ismeretlen trójai programot szeretne majd a jövőben elterjeszteni, itt a remek recept, dől a sok balek be az ajtón, önként és dalolva kattint és kattint. Esetünkben inkább **a piramisjátékos csalás és/vagy az email címek spamlistára való ipari méretű gyűjtése lehet a cél,** nézzük hát a weboldalt!

A bejelentkező oldal baloldalán, **mintegy kaszinó feletti világítótáblán a jackpot összege, ott virítanak a dollár milliók**, ezúton kívánjuk minden kedves olvasónknak, hogy legyen neki szerencséje. Ha majd átvette a sok-sok pénzt, legyen olyan jó, és hívjon meg majd egy sörre, a Heineken a kedvencem ;-)

Az oldalt 2007. december 3-án regisztrálták egy gmailes (dubaimlm@gmail.com) emailcímről - **hát nem furcsa, hogy ilyen szuperkomoly, tőkeerős cég nem saját domain névvel levelezik?! A sejkeknek már egy saját domain is smafu?**

Akinek még maradt kedve, regisztrálhat is - **csak aztán nem sokat tetvészkedni kérem szépen, mert minden óra késlekedés 300 elszalasztott tagot jelent, két óra késlekedés 600-at, és így tovább**, egyébként a nagy mesélők közül nekem Benedek Elek volt a kedvencem, ő ennél százszor jobbakat írt. Na mindegy, nézzük a regisztrációs űrlapot!

Van itt sponzor identifikáció, meg minden, mi szem-szájnak ingere, hogy nézni is tereh. Milyen személyes adatokat is kell ismeretlenül megadni? Várják tehát nagy tisztelettel:
- teljes nevünket
- pontos lakcímünket
- telefonszámunkat
- emailcím is kell nekik (**Itt Péterfalvi Attila már biztosan csuklik és jeges borogatást helyez a halántékára...**)
- és választhatunk saját előtagot a domainhez, amin majd saját üzletmentünket intézhetjük Armani öltönyben, csillogó Rolex órában, Mercedessel a rózsadombi villa garázsában - **"köszönhetően a jólelkű és adakozó arab olaj-mágnásoknak és üzletembereknek"**, egyszerűen nem hiszem el, hogy ezt ennyien beveszik... Azért rendesek és kíméletesek a fiúk, mert a kutya oltási bizonyítványának számát be sem kérték.

Már blogokban is terjed az ige, az erő meg az elsöprő lendület legyen velünk :-)

Azt, hogy mennyi hiszékeny ember van - aki munka nélkül fog sok pénzt keresni, az is mutatja, hogy a Googleban rákeresve a dologra, már temérdek **ingyenes hirdetési újságban toborozzák maguk alá az újabb balekokat**.

Ingyen pénzt ingyen hirdetésben, nomen est omen!

Azt hiszem most már **ideje mindenkinek felébredni**, aki pedig ezt az egészet elhiszi, annak őszinte részvétem. Mert ha senki nem dolgozik, mindenki csak ügynök, és csak emailt írogat, akkor miből lenne pénz?

Abba meg belegondolni is szörnyű, ha egyszer csak a fődomainre feltennének egy új kártevőt, és akkor az egy gombnyomásra a hiszekenyhugo.dubaimlm.com oldaltól kezdve a naivnora.dubaimlm.com oldalig egyszerre, Magyarországon és külföldön egyaránt - egy szinte StormWorm-szerű hadseregként - ontaná a látogatókra a kódot világszerte.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/298712

Kommentek:

huszár 2008.01.16. 16:01:48

Ez jól hangzik amit írsz!Biztos utánna is jártál a tényeknek amiből ez a "jópofa"kis cikk kikerekedett!Szellemes,de tényleg!Az igaz,hogy sok ember akar meggazdagodni munka nélkül,ez tény.
Az is tény,hogy ez a lehetőség ingyenes,tehát kockázatmentes!
Áttverés?Lehet!De ha valaki egy erre a célra létrehozott email cimmel regisztrál akkor mi baja lehet belőlle?(majd te elmondod,mi baja lehet gondolom).Ezek az emberek legalább próbálnak valamit tenni magukért!Ők legalább nem csak panaszkodnak,de tesznek is valamit!Kíváncsi lennék ha a jövőben kiderülne,hogy még is komoly a dolog akkor irnál-e egy kiigazító cikket,hogy bocsánatot kérj a sok általad "baleknak"nevezett embertől?

huszár 2008.01.16. 16:13:41

Egyébbként február elején kiderül mi a helyzet..Kérlek olvasd el az
egész oldalt tüzetesen és a regisztrációkor kapott üdvözlő emailt is (kérd el valakitől).Kívánom mindenkinek,hogy sosem veszítsen több pénzt mint amit ezen veszíthet!Szerintem profi az oldal és ha utánna olvasnál akkor azt is tudnád,hogy senkinek nem igérnek pénzt munka nélkül!Dubai dollár nincs is!Ez egy pontrendszer amivel az aktív tagtoborzók munkáját ismeri el a cég!Ezt lehet majd a jövőben beváltani illetve levásárolni (persze csak állítólag!!),Biztos akkor lessz ha elköltötted!De ahoz előbb meg kell
keresni..Mondom:Soha senki életében ne veszítsen többet senki mint amit ezen fog,ha kiderül,hogy kamu a dolog!De egyenlőre erről szó sincs!Semmi nem bizonyítja!A vélemény pedig olcsó dolog,az mindenkinek van és kéretlenül osztogatják

az emberek..De a rossz hírek mindíg érdekesebbek mint a jók!
Egy csomó "balek"egy rakáson!Ráadásul egyre több!Ez aztán a hír!!Egy jó lehetőség,ami ráadásul kockázatmentes is?Kit érdekel!Unalmas..

huszár 2008.01.16. 16:21:05

A spam gyűjtés mint végcél elképzelhető!Bár még senki nem kapott a regisztráltak közül,de lehet (jelenleg nem zárható ki!).
Na de piramis játék???Kedves Rambo!Úgy gondolom nem vagy teljesen tisztába a fogalommal!Itt ugyan nincs termék és szolgáltatás sem (jelenleg)de pénzt sem szednek be!!Márpedig a nélkül sajnos nem lehet piramisról beszélni!
Bocsánat ha "sok"voltam..

buherator · http://buhera.blog.hu 2008.01.16. 16:23:15

Hogy valaki ennyire ostoba legyen... Ugye ha megpróbálunk regisztrálni, máris megjelenik, hogy kinek a holdudvarába fogunk tartozni:

Buzdogány Andrea
30/2509060

Google persze ismer mindenkit:
ppl.hu/inside.ppl?page=view&id=nfvi7

Úgyhogy ha valaki szeretne Andinak eladni pár doboz viagrát, némi nyugtatót, vagy egy raklap trágyát, annak itt a remek lehetőség!

buherator · http://buhera.blog.hu 2008.01.16. 16:30:01

Huszárnak egyébként igaza van abban, hogy addig nem piramisjáték, amíg nem fizetsz. Ettől függetlenül undorító ilynnel spammelni, splogolni.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.16. 16:35:36

Kedves Huszár!
Gondolom, te a barrikád másik oldaláról nézed és valódi üzleti lehetőségnek tekinted a dolgot. Nem akartam én megbántani senkit a "balek" szóval, ismerem a magyar valóságot, a munkanélküliségi adatokat, a negyven felettiek nehéz elhelyezkedését és azt is tudom, vannak olyan MLM cégek, amelyek működnek.
EZ VISZONT szerintem nem az, hanem hiszékeny emberek megtévesztése.
Azzal is egyetértek, hogy mindenki próbálkozzon kedve szerint. Azt viszont te nem látod, hogy:
1. Egy ilyen közös domain tényleg könnyen válhat kártékony kódót terjesztő hálózattá - elvi veszélye megvan
2. Nem tudod, fogalmad sincs, KIKNEK adod meg a személyes adataidat. A maffiának? John Doenak? Jurij Afanaszjevnek? csak beépeled, és reménykedsz, a személyes adataidat, emailcímedet IGENIS KOCKÁZTATOD.
Láttad, beírtam hogy ha működik, a sok dollárból hívjanak meg egy sörre, adtam ennek is - ha csekélyke - esélyt :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.16. 16:47:02

Kedves Huszár!
Na én is többlépcsőben válaszolok :-)
Szóval mindenkinek, aki ebben hisz, bátran lépjen be, keressen pénzt. Én a saját biztonsági szakértői szemszögemből írtam, nekem hiteltelenül hangzik, és én a személyes adataimat holmi névtelen cégnek, kilátásba helyezett nyereményekért sose adnám meg.
Sok sikert a belépőknek, és szívből kívánom, hogy neked, nektek legyen igazatok, ne nekem :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.16. 17:04:19

Tisztelt Olvasók!
Ezúton kérem, hogy akik majd sikeresen pénzt keresnek ezzel a Dubai MLM rendszerrel, osszák meg velünk kedvező

tapasztalataikat, hadd ismerjük meg a történet folytatását is, amit kíváncsian várunk.
Előre is köszönöm.

buherator · http://buhera.blog.hu 2008.01.16. 17:09:19

Na megnéztem jobban ezt az oldalt, meg elolvastam az üdvözlő levelüket is, a következőket szeretném a szíves figyelmetekbe ajánlani:
- Az oldalon nincs privacy policy vagy egyéb dokumentum, ami tisztázná, hogy mi is lesz a személyes adatokkal
- Arról sincs egy nyamvadt bekezdés, hogy mégis mivel lehet itt pénzt keresni (azon kívűl hogy berángatsz minél több embert)
- A személyes oldalon egyelőre nem működik semmi, a linkek "javascript:void(0)" eventekkel vannak felruházva. (persze lehet hogy csak azért, mert ff+noscript alatt nézem)
- A regisztrációs mailben azt írják, hogy "DubaiMLM has a ZERO TOLERANCE - STRICTLY ENFORCED - NO SPAM POLICY", szóval Andikát elvileg ki kéne vágniuk az oldalról, ha tudomást szereznek a módszereiről. Arról nem szól a fáma, hogy le van-e tiltva az új regisztrációról...
- Azt is írják, hogy egy ország pénzének azért van értéke, mert azt a pénzt az országban mindenki elfogadja. Na most ez baromság, a pénznek azért van értéke, mert az azt kibocsátó ország bír egy megfelelő gazdasági erővel. Ilyen erőt emögött a vállalkozás mögött nem mutatnak be.
- "DubaiMLM Dollar already has Thousands if not Tens Of Thousands of outlets willing to accept DubaiMLM Dollars" - lehet hogy az én angol tudásom korlátos, de ez sztem azt jelenti, hogy vannak cégek, akik _tervezik_ hogy elfogadják a DubaiMLM Dollart. Majd...talán..valamikor.
- És a kedvencem: "Your DubaiMLM back office will be able to receive DubaiMLM Dollars, __Euro Dollars__ and USA Dollars"
Gondolom jól utánajártak a dolgoknak, és mindent gondosan megterveztek :)

Azt igérik, hogy január 30-án kiadják azoknak a cégeknek a listáját, akik hajlandóak elfogadni ezt a lovettát. Hiszem ha látom...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.16. 17:54:39

Szia Buherator :-)
Koszi az utananezest. Hazafele en is azon tunodtem, hogy nem normalis dolog az, hogy barki, aki akar a google alatt talal egy ilyen szponzori oldalt, látja a nevet és a mobilszámot. Az lenne a normális, hogy ha valaki névvel-jelszóval belép, akkor látja a csoportját vagy a felsőkapcsolatát. Így most mindenki nemcsak a cégnek, hanem BOLDOG-BOLDOGTALANNAK adja meg az elérhetőségeit, amit lehet, hogy még az IWIW-en sem tenne meg. Ezen is el lehet gondolkodni, ez is adalék vagy egy tégla a falban.

huszár 2008.01.16. 20:42:44

Kedves Rambo és buherator!Ahogy a fordítás is mondja:
Azt igérik, hogy január 30-án kiadják azoknak a cégeknek a listáját, akik hajlandóak elfogadni ezt a lovettát. Hiszem ha látom...Ez a lényeg!Mondok egy érdekes dolgot!Ismerek embereket akik fals adatokkal regisztrálnak..Egyszerüen belépnek egy erre a célra létrehozott e-mail címmel és kitalált adatokkal regiznek!Igy tagok lesznek akik foglalkozhatnak a lehetőséggel.. Ezek az emberek úgy gondolkodnak (miközben épül alájuk a hálózat),hogy ha majd kiderült,honnan is fúj a szél akkor majd megadják a valós adataikat,ha akarják!!Ha így nézzük a dolgot akkor már nem is olyan vészes igaz?Sok vélemény elhangzik ezen a fórumon.Hiszem,hogy a legtöbbet a jóakarat szüli!Nem gondolom,hogy valaki irigységből beszélne le bárkit is erről! De a tények makacs dolgok..Jelenleg arra nézve,hogy ez áttverés lenne semmi nem utal!!

freya-spamblog · http://spamblog.hu 2008.01.18. 10:19:50

Azt hogy valójában ki van a háttérben, meg mire használja a címeket, csak több utánajárással lehetne eldönteni, de szerintem ez lényegtelen. Az is egyértelműen látszik, hogy átverés és komolytalan, ezer sebből vérzik a történet.

Szerintem egyszerűen valódi email címeket gyűjtenek, végülis mennyivel egyszerűbb lánclevéllel, mint egyéb módokon. Egy nagy címlistának mindig van értéke, egy kipróbáltnak főleg (hiszen mindenki kap egy válaszlevelet, tudják, hogy mi a valódi). Ha jól csinálják, összehoznak egy pár millió címes listát amit például január 30-án (mintha említettétek volna :) eladnak néhány száz dollárért néhány száz vevőnek... biztos megtérül a befektetett idő ezzel.

Károkozókat (még) nem raknak az oldalakra, ezért is egyértelműen az email cím gyűjtés a cél.

buherator · http://buhera.blog.hu 2008.01.18. 15:24:49

És az vajon mennyit ér, ha az email címek mellé jelszót is adsz? Tapasztalataim szerint jelentős mennyiségű felhasználó

használja az e-mail címéhez tartozó passt ilyen alkalmakkor is. Egy olyan scriptet pedig semmiből nem áll írni, ami végigpróbálgatja a mail - jelszó párokat, meg esetleg pár egyszű variánst, aztán kimazsolázza a kontaktlistákat meg a facebook/myspace infókat... Innentől kezdve pedig már milliós listákról beszélünk marketing profile mellékelve...

[off]
Ákos, ha esetleg lemardtál volna róla:
www.theregister.co.uk/2008/01/17/anti_spam_activist_lawsuit/
[/off]

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.18. 20:02:31

Egy kis olvasnivaló a témában:
internetscamphishing.blogspot.com/2008/01/is-dubaimlm-scam.html

Szaros gerle / Lighting Enchanted Multiple Shots · http://gerlefeszek.blog.hu/ 2008.01.19. 04:12:25

huszár, te egy szerencsétlen balek vagy aki szeretné hogyha igaz lenne

buherator · http://buhera.blog.hu 2008.01.19. 10:58:27

Ha valaki enm szeretne angolul olvasgatni:

A DubaiMLM.com-ot is ugyanaz a Phil Piccolo

www.worldwidescam.info/ppstory.htm
www.transgallaxys.com/~kanzlerzwo/showtopic.php?threadid=3131

akinek már több hasonló átveréshez is köze volt. Ezek egyike volt a BankMLM

www.scam.com/showthread.php?t=3544

aminek a domainje a bankmlmofdubai.com-ra mutat (bár ez a host nem aktív), és megtévesztésig hasonló kampányt használt a különböző személyes adatok begyűjtésére.

A Rambo által belinkelt blogger tanácsa: változtasd meg a rendszerben tárolt személyes adataidat amilyen hamar csak tudod, bár lehet hogy már késő...

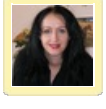
nevetőharmadik 2008.01.23. 16:22:23

Nos, a helyzetem a következő: egy nagyon kedves, üzletileg alulképzett, naív. lelkes rokonom a napokban elkezdte nyomatni rám ezt a DubaiMLM-et, hogy ő belépett mert érti meg miegymás, és regisztráljak én is azonnal. Nos azonnal megállapítottam, hoyg ez gyanús, és amikor a honlapjukat megnéztem (Untitled page !), biztos voltam benne, hogy ez egy kamu.

De hálistennek megnyugtattatok, hogy ezzel nem fogják kisemmizni ezt a nagyon kedves, üzletileg alulképzett, naív, lelkes rokonomat.

És mivel meggyőzni úgysem tudom arról, hogy ez egy baromi nagy kamu, azt teszem, amit huszár mond: regisztrálok egy új e-mail címmel, kamu adatokkal, és hadd szóljon. Kecske is jóllakik, káposzta is megmarad. Remélem. Az e-mail fiókot meg megszüntetem majd.

Azért mégis megpróbálom lebeszélni az egészről, és arra meg rá, hogy gyorsan változtassa meg az adatait.



Vidi Rita · http://www.hosnok.hu 2008.01.26. 21:32:00

nekem azon megy fel a cukrom (csak nehogy a kávém is felmenjen), hogy ezt komolyan lehet büntetlenül csinálni?
hát ilyenkor nincs sehol egy rendőr?

komolyan kiakadtam ezen, nem hittem, hogy ennyire buták az emberek...:(

sztem össze kéne fognunk... és turnézni, a legkisebb faluba is elmenni, és elmondani, mekkora veszélynek vannak kitéve... hát, cirka 150 év alatt 3 embert meg is lehetne győzni, nem?...
és még optimista voltam...

az tuti, hogy minden kezdő netezőnek át kell mennie egy saját ütemű fejlődési folyamaton, amit kicsit sem szabad siettetni, és speckó állomások kellenek hozzá, ugyebár személyre szabottan..

ezt még alá is írom, de esküszöm megtiltanám mindnek, hogy egymással beszéljenek! :D

Vidi Rita · http://www.hosnok.hu 2008.01.26. 21:36:09

na, én is több lépcsőben: az meg a másik, hogy nem favorizálom kóka jánost, de igaza volt bakker, hogy a többség pénzügyi analfabéta...

legutóbb, mikor jól "működő", netes mlm-be akartak beszervezni, akkor volt ám mindenről szó, de arra a kérdésemre, hogy "oké, de hol termelődik a profit????" soha, senki nem tudott válaszolni.

könyörgöm, munka nélkül nincs pénz...
regisztrációból nincs pénz...
előállított termék, akár szellemi, akár fizikai, nélkül, nincs pénz...

kamatból van pénz, de ahhoz előbb kéne egy kis tőke... az e-mail cím nem a tulajdonosa számára tőke....

na, most megnézek valami gyilkolós filmet:)

buherator · http://buhera.blog.hu 2008.01.31. 11:12:46

Tisztelettel jelentem, január 31. a dátum (Dubaiban, és az Államok mindkét partán is), de valahogy nem látom a Dubai Dollar-ral foglalkozó cégek listáját sehol sem... Valahogy nem lepődtem meg.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.31. 16:57:11

Sziasztok!
Köszi, hogy szétnéztél, és valahogy én sem lepődtem meg...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.03. 22:15:55

Egy újabb adalék:
forum.index.hu/Article/viewArticle?a=75347638&t=9123617

Mericles 2008.02.06. 22:27:47

Én hálózati marketinggel foglalkozom, de ez a Dubai MLM szerintem is címlista építés.

"legutóbb, mikor jól "működő", netes mlm-be akartak beszervezni, akkor volt ám mindenről szó, de arra a kérdésemre, hogy "oké, de hol termelődik a profit????" soha, senki nem tudott válaszolni."
Hol, hol? Hát a termék árában, amennyiért azt a rendszerből meg tudod venni! Pl. az Amway-nél nem (lényegesen) olcsóbb, a termék, mintha a boltba vennéd, viszont nincs benne egy csomó tétel, ami a kiskereskedelemben forgalmazott termékekben benne van. Mivel az ára viszont kb. ugyanannyi, az árrés a hierarchiában feletted álló partnerek számára (és a tiédre is részben) visszaforgatódik.

Ezt a beszervezés szöveget gyakran hallom, hála Istennek, aránylag kevesen szállnak be (megkeresett emberek 5-20%-a), ezért ez még 100 évig jó buli lesz. Beszervezni akarata ellenére nem lehet senkit, és iszonyú nagy szívás vank vele. Ugyanis csak az idődet nyomod bele (mondjuk melód után), de az égvilágon semmit nem csinál, csinálhatsz egy ideig helyette is mindent. Egyszerűbb olyat keresni, aki jön magától is, abból kb. 5-10 megfelelő ember kell, és 5 év alatt meg vagy mentve a munkahelyedtől.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.20. 11:05:50

Lassan vége a márciusnak, és még egy Dubai MLM-es se hívott meg a keresetéből egy pofa sörre ;-)

zvaragabor 2008.03.25. 17:16:29

Itt egy hasonló témájú oldal, ez vajon átverés?
www.dubai-ingatlanbefektetes.hu/index.php?p=uzleti-infok

prosz 2008.03.26. 19:54:09

Sziasztok,

Sajnos a mai világban teljesen jogos zvaragabor kérdése, hogy vajon átverés -e a www.dubai-ingatlanbefektetes.hu oldal tartalma is.

Én is mindig kétkedéssel fogadtam és fogadom a hasonló témájú, nagy hozamú befektetésekről szóló híreket, főleg ha munkabefektetés nélkül vagy nulla kockázatvállalással ígérik mindezt.

Ez esetben azonban, mivel a fenti oldalt én üzemeltetem, és saját bőrömön tapasztaltam meg 100% feletti hozamok valóságát, mindenkit arra bátorítanék, hogy egy személyes találkozó keretei között tájékozódjon maga az off plan típusú dubai ingatlanpiaci helyzetről, pénzügyi konstrukciókról, a gazdasági számításokról, és az ezek hitelességét alátámasztó dokumentumokról. Nem befektetni szándékozó, csupán érdeklődőket is szívesen beavatok a részletekbe és eloszlatom a kételyeiket.
Hadd legyen végre a sok dubai MLM átverései között egy legális és pozitív példa is :)
elérhetőségeim a fenti weblapon

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.14. 14:31:38

Már szinte elfáradtam, annyit járok vissza a dubaimlm oldalra, és mindig az az érzésem, itt állandó visszaszámlálás van. A mostani final-final dátum ezúttal április 20, utána jön majd a Kánaán ;-) Mindenesetre jó látni, ahogy utólag meghamisították a célkitűzéseket, és pótlólag beszúrták a 240 nap alatt elérendő 500 ezer tagot :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 12:08:56

Ma ismét ellátogattam kíváncsiságból, vajon lejárt-e már a határidő, hát meglepődtem, újabb időpont vírit:Starts JUNE 1, 2008 International.
Egy biztos, nem ilyen türelmetlen népeknek való ez, mint amilyen én vagyok ;-) (Mindent akarok, de azt most rögtön, mindent akarok azonnal... köszönjük Ferókám)

ideals 2008.06.23. 20:05:39

Kedves Prosz!
Megnéztem az oldaladat.. - van egy Bp-től 50 km-re lévő - dicséretére legyen mondva, a falu központjában - egy 100 nm-es komoly jelzáloggal kb. 5 millióval, terhelt öreg parasztházam. Nem akarod megvenni???
Na, nem gúnyolódni akarok, félreértés ne essék! Láttam a lapodat, nagyon komoly - tényleg.. - csak ki hiszi el, hogy 5 millió Ft-ért bárki bármit meg tud venni Dubaiban?? A múltkor megnéztem az ingatlanpiaci körképet itt Európában, és mondjuk egy pici, de 2 szolbás lakás kb. minimum 50 milla körül van! Szerintem Dubaiban egy kutyaólat lehet venni 5 milláért, vagy egy 2x3-as szobácskát - lehet, hogy "biztonsági őrökkel"?? - ha az összeg nem lenne "komolytalan", még talán komolyan is lehetne venni!
Spanyolországban egy tanya, az Isten háta mögött 3 lépéssel, minimum 30-40 millió (forintban), hogy lehetne már bármit kapni 5 millióért Dubaiban???

ideals 2008.06.23. 20:12:31

Utóirat a beszélgetéshez:
Ami a cím-gyűjtést illeti, ha arra használják, egy ilyen weblap megszerkesztése még dicséretes is, mert legalább melózott vele a tulaj!
Annál "szebbek" és tisztességtelenebbek, mikor a barátaim által küldött kör-emilek arról szólnak, hogy segítséget kér valaki, mert beteg ő vagy akárkije - és mikor ráklikkelsz, hogy ki küldte, valami kávézó, vagy más MLM-lap jön be rajta! Na, ez a tisztességtelen! - a többi mindenkinek szíve joga.. - ki hova mikor és miért iratkozik fel.
Egyébként szerintem teljesen mindegy, hova regisztrálsz, mert egy idő után úgyis eladják az adataidat. Pont úgy adják-veszik a címlistákat, mint a piacon a nem tudom mit.. - még alkusznak is rá.
Ennyit a "személyiségi jogokról", megy a Privacy Policy-ről vagy minek hívják, az csak oda van biggyesztve és kész!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.06. 15:01:57

Alighanem minden gazdasági dolog megtorpant a válság miatt kissé:
www.penzcentrum.hu/cikk/1015849/1/ezerszamra_hagyjak_magukra_a_hitellel_megterhelt_autokat

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.14. 13:19:56

Egy kis csillogó felszín alá való tanulságos bekukkantás:
hvg.hu/vilag/20090414_karen_andrews_dubaj.aspx

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.15. 14:12:01

Nekik sem fognak szobrot állítani tisztességes hozzáállásért:
www.origo.hu/techbazis/internet/20090710-adatlopassal-vadoljak-a-taggedcom-kozossegi-portalt.html

Yann Le Pentrec · http://lnk.bz/t7c 2009.11.05. 20:25:31

Aszondja a szöveg: "Jelenleg az INGYENES előregisztrációk folynak, ennek keretében a közös ágra lehet regisztrálni a tagokat. Ebből adódóan a közös ág fantasztikusan gyorsan épül."

Ez a közös ág csakis a szopóág lehet. :)

No komment

2008.01.17. 08:52 | Csizmazia István [Rambo] | 4 komment

Címkék: spam komment no regyisztráljon

Mai **No komment rovatunkban** egy **minőségi spamet** mutatunk be, lehetne a címe akár **helyesírás rulez!** is. Ha esetleg valaki érti, hogy miért, hogyan és egyáltalán, az ne kíméljen bennünket, jelentkezzen és ossza meg velünk, miről szól ez a "linkehagyott" kéretlen levél.

A HELO rekord szerint valóban Freemailes címről érkezett, a többi rejtély...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/300488

Kommentek:

ihatethisindapassthingy 2008.01.17. 12:00:24

HELO rekord? :)

Egyébként ez tuti csak poén. Ugye az? Nem hiszem el, hogy ilyen létezik :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.17. 15:54:48

Szia!
Egy csali, honeypotos címemre jött, ezért azt mondhatjuk, "ilyen nincs, de mégis van..." :-D

Hegylako 66 2008.09.28. 22:46:45

Szerintem is csak egy vicc az egész. Ilyen helyesírási hibákat csak akarattal lehet "véteni"!

chromeshelter · http://halfps.blog.hu/ 2008.09.30. 15:57:27

hát ez már tényleg merész :D

Szeretettel... vagy mégsem?

2008.01.17. 09:01 | Csizmazia István [Rambo] | 5 komment

Címkék: noscript withlove szeretettel stormworm irfanview heurisztika

Alig másfél nap telt csak el, hogy az F-Secure blogban írtak a StormWorm újabb felbukkanásáról, mi is megkaptuk, több példányban is. Az angol nyelvű levél "Dance of Love" tárgysorral és egy IP címet tartalmazó linkkel érkezik, és rákattintani nem javasolt.

Az eredeti hír olvasásakor először a szokásos grafikai buherálás, kísérletezés következett: **kíváncsiság, Irfanview a neved ;-)** Ha nem is elsőre, de végül sikerült a bemutatott címről is letölteni a kártevőt. Fránya egy dolog ez a satírozás, mi magunk részéről inkább a Pixelize függvényre esküszünk.

Az F-Secure oldalon bemutatott **IP cím egyébként teljesen különbözött** az általunk kapott levéltől, sőt a későbbi példányok is **mind más helyre mutattak**.

Jópofa a szöveg, miszerint ha esetleg nem indul el a letöltés 10-20 másodperc után, akkor nyomjunk kézzel a linkre. Nos erre ugyan várhatnánk ítéletnapig, jó szokás szerint itt is **a felhasználónak magának kell kattintania** ahhoz, hogy bambán megfertőzhesse a saját gépét, és ezt sokan kíváncsiságból meg is teszik. **NoScriptes FireFox mellett a letöltési link meg sem jelenik!** Próbaképpen engedélyezzük ideiglenesen a helyszínt. Az is szépen látszik, hogy a ShowIP plugin is mutatja alul pirossal a weboldal IP címét.

Oppá, meg is jött a linkünk, de kattintás előtt - fokozzuk a feszültséget - **nézzünk bele az oldal forrásába!**

Vajon az fck2008 milyen angol szónak lehet a rövidítése? ;-)

Jól látható, hogy **sok jóindulat nem tételezhető fel arról, aki a linkjeit Unescape függvénnyel próbálja elrejteni a nagyérdemű fürkész pillantásai elől.** Kódoljuk hát vissza láthatóra ezt a zagyvalékot.

Aham, szoval kétféle exe töltödik a gépünkre, próba indul, kattintsuk hát arra a linkre, és már jön is a "withlove.exe".

Bekapcsolt NOD32-vel semmi az ég világon nem történik, a figyelmezető ablakok felbukkanásán kívül. Matamatika órákról kölcsönözve az "**és most vegyük észre**" szófordulatot érdemes megfigyelni, hogy **az ingyenes vírusirtók közül sem az Avast, sem a Clamav nem detektálta a kártevőt**, a nagy nevek szinte mind észlelték - talán a Panda a kivétel.

Bármilyen antivírust is válasszunk, **érdemes erős heurisztikus képességgel felvértezett darabot** kiszemelni, a Viharféreg variánsokkal - sajnos - biztosan nem most találkoztunk utoljára.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/300433

Kommentek:

titan 2010.04.27. 12:15:49

Izé, csak én nem vettem észre, hogy a ClamAV nem ismerte fel? Legalábbis ha a nevével egy sorban levő másik cellát nézem, ott vörösen világít a Trojan:Peed-89

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.04.27. 12:38:12

Szia Titan!

De-de-de, pontosan az a jó, ha szerepel ott valamilyen név, akkor van felismerés. Aki nem ne detektálja, annak csak egy - jel jut.

titan 2010.04.28. 14:51:17

@Csizmazia István [Rambo]: akkor szerintem picit írd át ezt a mondatot:
"és most vegyük észre" szófordulatot érdemes megfigyelni, hogy az ingyenes vírusirtók közül sem az Avast, sem a Clamav nem detektálta a kártevőt
Talán elnézted egy sorral annó :) megesik...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.04.28. 18:44:53

@Titan: Jogos, tényleg mellénéztem, elnézést.

titan 2010.04.29. 12:51:18

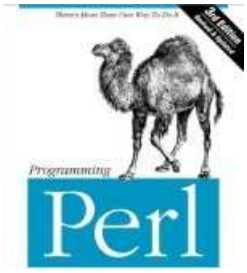
Semmi gond, nem a ClamAV ügynöke vagyok :D

A Perl, a pornó és két füstölgő puskacső

2008.01.21. 14:59 | Csizmazia István [Rambo] | 6 komment

Címkék: perl pornó adserver perl.com

Több alkalommal is beszámoltunk már feltört, **eltérített weboldalakról, amelyek máshova irányítottak, vagy kártevőket töltöttek le** a felhasználók gépeire. A nagyobb látogatottságú oldalak is egyre jobban felkeltik a rossz oldal érdeklődését, a MySpace, a FaceBook közösségi portálok, a baseball és hoki liga weboldalai után most egy **furcsa technikai malőr következtében az O'Reilly Media** által birtokolt Perl oldalra járt rá a rúd.



Ez a nagyhírű weboldal esett most áldozatul, a jelenség pedig az volt, hogy **aki csütörtökön eredetileg a Perl.com-ot szeretette volna meglátogatni, az váratlanul egy online pornó webkamerás oldalon találta magát**. Az átirányítás egy a grepblogs.net DNS-név tulajdonjogában bekövetkező változás eredménye, ami a nyíltforráskodú hirdetési szerverrükkel volt kapcsolatos (http://grepblogs.net/adx.js). 2006 óta a JavaScriptes kódok a grepblogs oldalról futottak. Akik kikapcsolt JavaScripttel látogatták az oldalt (pl. NoScript), azok megúszták a galibát. A hibát péntek reggelre már elhárították.

A **Perl egy programozási nyelv, melyet Larry Wall tett közzé 1987-ben**. Különösen a rendszergazdák kedvelték-kedvelik, sok elemet olvasztott magába a C, az AWK és a ShellScriptes elemekből.

Talán abból a szempontból új korszakot élünk, hogy **egy kattintás után lassan már sosem lehetünk benne biztosak, hova is jutunk el végül**. Még az is lehet, hogy egyszer egy pornó oldalra látogatva a végén egy scriptnyelvet népszerűsítő weboldalra érkezünk - de erre azért senki ne vegyen mérget ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/305923

Kommentek:

Szokol 2008.01.21. 23:43:32

2 napja a feleségem egy bababolt honlapján ütközött vírusba. Szegény tisztára kétségbeesett, mit csinált rosszul.

Manyizga (törölt) 2008.01.22. 08:10:24

Nem kéne weben venni babacuccot... :)

Meg persze nem IE-t kell használni böngészésre, de az alap, ugye.

Szokol 2008.01.22. 08:27:56

Miért ne kéne? sok mindent vettünk már. És persze nem IE-t használunk.

Nite · http://animecomment.blog.hu 2008.01.22. 08:42:45

nekem a múltkor firefox alá is lemászott egy vírus, még az antivírusom se ismerte fel (persze nem is az a szép hőskori vírus volt, csak valami kis hülye script-kiddie ténykedése) mindenesetre legközelebb ha warez oldalakat nézek, linux alól teszem :D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 09:05:17

Szia Szokol!
A weblapok eltérítése nem védhető ki százszázalékosan - CrossSite Scriptin, DNS manipulációk, a fenti eset meg egy fatális véletlen - és gyanítható, ez a módszer sajnos az idén egyre jobban fel fog erősödni :-(

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 09:08:07

Hello Nite!
A Linux alól való ténykedés jó ötlet :-) Lehet hogy egyedül vagyok ilyen paranoiás, de én még ott is nyomatom az FF plugineket (NoScript, stb.)

Ha annak idején a szüleid inkább moziba mennek...

2008.01.22. 13:58 | Csizmazia István [Rambo] | 37 komment

Címkék: spam iwiw viewbug nikkki tolvajp

Úgy tűnik, egyre sűrűbb szárnypróbálgatásokkal kísérleteznek a spamküldők az IWIW-en is ontani a felesleges, idegesítő és főleg KÉRETLEN leveleiket. Az elkövetők nyilván számolnak vele, hogy **egy nick csak egy ilyen akcióra elég**, de valószínűleg gondoskodnak egyre újabb és újabb profilokról, **az üzemeltetők pedig a kitiltáson kívül látszólag nem tesznek semmit**. Írtunk ugyan levelet az adminnak, de egyelőre nem reagáltak, ha esetleg később mégis lesz válasz, betesszük majd egy kommentbe.

Pedig lehetne, nyilván **szolgálhatna információval az admin, illetve aki az illetőnek a meghívót annak idején küldte**. Kaphatna helyet **egy "Jelentem" gomb** is az üzenetolvasásnál és a spamtörvény megsértése miatt indulhatna is az NHH eljárás.

Ehelyett mi a helyzet most? Megnyomhatom magamnak a "Feladó kizárása" gombot, amivel ugyan a mi problémánk **erre az egyetlen agyatlan levélíró esetére megoldódik**, de a következő törölt nickre már nem, és persze a többi felhasználó úgyanúgy megkapja ezeket, **amíg csak egyesével nem kattint mindenki** az ilyen arghhhh!%!++% által küldött levélre.

Na neee már, hogy **ilyen fatengelyesen kelljen ezt kezelni 39 évvel a Holdra szállás után**.

Nikolett - **ha tényleg ő az, és nem egy gerillamarketinges reklámcsapat** - ma is korán kelt, sőt elképzelhető, hogy le sem feküdt, ne is firtassuk, sikerült neki hajnali 4 óra 1 perckor 4 azaz négy példányban is - egy spam nem spam - elküldeni értékes üzenetét.

Maga a levél itt van, ha **esetleg van olyan Guiness rekord, hogy a legtöbb címzettnek küldött IWIW körlevél**, bátran indulhatna, a képet csak fekve tudtuk így is betenni.

A post címét **tolvajp** nevű kommentelőtől kölcsönöztük, (eredeti copyright szerint: "Hát, jobban járt volna a világ ha annak idején a szüleid inkább moziba mennek...") **ezúton köszönet neki** a frappáns, szalonképes és lényegretörő fogalmazásért :-D A többi hozzászólás sem kevésbbé offtopik, de érthető módon indulatosabbak és a vélelmezhető levélíró szüleit, rokonságát, azok nemi életét említik meghökkentő és roppant részletességgel, különös tekintettel a felmenők között egy bárgyúképű puputevébe oltott rinocérosznak egy varangyosbékával történt nászára. Szóval **e kommenteket csak erős idegzetűek olvassák**, illetve ajánlónak lehetne még a South Park féle felvezetés is: **Vigyázat durva nyelvezet, megtekintését semmilyen korosztálynak sem ajánljuk :-)**

Közben egy Beatrice nóta jár az eszünkben, a Minek él az olyan... kezdetű dal, nem is értjük, miről jutott ez most eszünkbe, na mindegy... ;-) **Jó lenne, ha az üzemeltetők megelőznék a hasonló eseteket**, mielőtt valaki nem egy ilyen ártalmatlan oldalra, hanem **egy kártevőket letöltő oldalra irányít ilyen módszerrel** embereket. Mindenesetre **most már a ViewBug látogatottságát sikeresen fellendítettük, lehet hogy éppen ez volt az eredeti cél** :-)

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/307126

Kommentek:

buherator · http://buhera.blog.hu 2008.01.22. 14:55:11

if ([van olyan címzett aki nem ismerős] && [címzettek száma]>5){
[user figyelmeztetése]
}

if([figyelmeztetések száma]>2){
[user törlése]

[a meghívó küldőjének figyelmeztetése]
}

Nem igaz, hogy ennyit nem képesek lekódolni, inkább veszik a drága vasakat...
Facebookra, MySpace-re nem kell meghívó, mégsincs ekkora spamprobléma. Őrület, komolyan...

OkoskaTo:rp 2008.01.22. 15:18:25

És ami még szebb: A villámgyors rendszerük képes arra, hogy már a spammelő feladó kizárása UTÁN küldje el nekem az üzenetről az értesítő e-mailt. Jönnek a levelek egymás után, hogy "-/- üzenetet küldött neked". Granulálok.

nade 2008.01.22. 15:21:47

Én ma ötöt kaptam ebből a cuccból egyetlen címre.

movhu 2008.01.22. 15:24:56

Szerintem(v0.2beta):
if ([user regisztrációjának időpontja-mai nap]1){
[user törlése]
[az ő meghívója küldőjének figyelmeztetése]
}

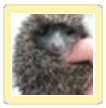
movhu 2008.01.22. 15:26:46

Na ezt jól összekócolta a blog.hu :)

Szóval:
if ([user regisztrációjának időpontja-mai nap]

movhu 2008.01.22. 15:28:24

Feladom a programozós beírást, mert nem úgy jelenik meg, ahogy akarom :)
Szóval a lényeg, hogy friss regisztrációval ne lehessen küldeni üzenetet legalább 1 hétig. A régebbieknél pedig a meghívó kizárása 1 hétre, 1 hónapra, örökre...



Los Alamuszi 2008.01.22. 15:39:27

Amit én nem értek, hogy, ha már kizárják az illetőt, aki spamekkel tömött tele (gondolom, megfelelően megvizsgálják előtte, tehát BIZTOS, hogy az illető elkövette, amiért törölték a regjét), akkor miért nem törlik az összes szemét szétküldött levelét a postaládámból? Mire gondolnak, mit akarok vele csinálni?
Ez szerintem kimondottan támogatja a spamelőket, hiszen, nem a regisztrációja számít neki, hanem, hogy a levele ott legyen a postaládánkban...

Bit Rot 2008.01.22. 15:48:17

Szerintem is - aki meghívta, azt elsőre 30 napra kizárni, utána örökre.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 15:49:25

Sziasztok!
Uff, Buherátor és Movhu is jó helyen keresi a megoldást, szerintem ennyit alaphangon minimum meg kellene végre tenniük.
@OkoskaTo:rp:
Érdekes a felvetés, de valószínűleg programozástechnikailag addigra (kizárás) már egy spoolban csücsülnek a levelek.
@Nade:
Szia, nekem is négy jött egyszerre, pedig egy is sok belőle ;-)
@Los Alamuszi:

Van ráció az ötletben, ha valaki magát törli vagy őt törlik, akkor üzenetei is úgyszintén feleslegesek lesznek a mátrixban, hiszen csak zavart okoznak az erőtérben...

Gery Greyhound · http://www.bestofgyurcsany.hu/news.php 2008.01.22. 15:51:39

Egyszerű lenne megoldani: mondjuk lehetne egy limit, hogy 5-nél több nem ismerős usernek nem lehet egyszerre levelet küldeni.

movhu 2008.01.22. 15:59:23

Lehetne még fokozni, és viszonylag egyszerűen:
-Beállíthatnám, hogy ismeretlentől nem fogadok levelet. Mivel lehet, hogy még is van olyan, aki írna, ezért lenne havonta 5 "joker" küldés mindekinek, ha mégis szerenénk ismeretlennek írni
-Régen értékesebb volt a meghívó, ma már mindenki osztja az üzenőfalon is. Új meghívó szabályzat, mely rögzíti, hogy amennyiben a meghívott spammel, akkor az acc AUTOMATIKUSAN 1 hétre locked
-Általános szabály lenne, hogy egyszerre csak x számú usernek küldhető levél, ezzel ki lenne szűrve a sok értelmetlen és személytelen karácsonyi/újévi kívánság is

yanchi 2008.01.22. 15:59:57

Az a gáz, hogy a nem ismerősök számának ellenőrzése plusz egy szög az amúgy is agyonhajszolt adatbázis koporsójába.
Jónak tűnik hasonló esetben a meghívó személy likvidálása, bár ezzel valószínűleg csak azt lehetne elérni, hogy egy kamureggel távolabb legyen Hajnali Nikolett valódi, hús-vér megbízója.
Esetleg kiváló megoldás lenne a hotdog.hu-n (is) alkalmazott módszer, hogy bejelölhessem, hogy csak kölcsönös ismerőstől akarok üzenetet kapni.

movhu 2008.01.22. 16:05:29

Akkor nagyon egyszerű:
Egyszerre egy személynek. A többire ott az üzenőfal, ha valakinek még is tutira kell szólnom, akkor egyesével.

Etalon 2008.01.22. 16:18:41

Movhu: ezt egy ügyes script-el gyorsan megoldanák a spam-erek. A meghívó kizárása sem rossz ötlet, de akkor meg egymásba ágyaznának egy csomó acc-ot. Mondjuk ez kiküszöbölhető azzal, hogy új acc csak egy hónap múlva hívhat meg bárkit is (a fő gond, hogy a spam-ereknek általában van idejük előkészíteni a dolgot, ráérnek ügyködni hetekig is ha kell)

Én a küldhető levelek számát havi szinten a visszaigazolt ismerősök számában állapítanám meg. Egy friss regnek lenne mondjuk 10-20, hogy tudjon írni azért pár embernek, a következő hónaptól meg már élne a normál limit.

movhu 2008.01.22. 16:33:13

Úgy látom abban egyetértünk, hogy megoldás ezért volna bőven...

la hermandad 2008.01.22. 16:49:42

Elépzelhető, hogy az oldal üzemeltetője profitál ebből a tevékenységből.

perecember 2008.01.22. 17:05:01

Az biztos hogy profitál, egy kattintás az oldalon, egy adag reklámbevétel a magenta szütyőbe. Nem hinném hogy a "-/- üzenetet küldött neked" üzenetek - jön egy jó adag belőle - törölt felhasználótól jön, ez kőkemény rendszerüzenet, és azért nincs feladó, hogy ne tudd kizárni. Mögé pedig büntetlenül el tud bújni a tékom, hiszen nincs kit feljelentened a spam miatt.

gibson 2008.01.22. 17:13:32

a baj az, hogy a cél szerintem is ennek a szemét oldalnak a látogatottságát növelni, ez pedig nyilvánvalóan sikerült az alkotóknak. ráadásul rengetegen regisztráltak is, hogy elküldjék őket a jó büdös kurva anyjukba. én biztos ami ziher feljelentettem ezt a bali "szerepjáték-szex-nagyköcsög" norbertet is, meg írtam neki egy kultúrált levelet is, hogy hova takarodjon. ha esetleg nem tudta volna, kinek / mire küldi a meghívót, ezentúl jobban nézzen utána a célszemélynek :)

la hermandad 2008.01.22. 17:15:02

Ismerősnek jelölt Vera. az Aloe.

bög 2008.01.22. 17:49:36

az még nem jutott eszetekbe hogy ne iwiwezzetek? én pl soha nem voltam tagja (nem csatlakozom olyan közösségekhez, melyeknek nagyanyám is tagja:)), és igen jól megvagyok nélküle.

◄ViZion 2008.01.22. 17:55:46

megoldási lehetősé sok van, de tudás az iwiw-es programozókba...
bár az sem kellene sok...
max 1-3 címzettet lehessen megadni, és ne legyen ctrl+v...
nos ha minden spamet gépelni kell...
oda miért nem raknak catchpa-t?

a szomorú az, hogy leszarják, a másik, hogy sok béna user psw-t feltörnek, és onnan küldik (múlt héten ezért töröltek egy lányt, ő meg nem is tudta...)
Szal a jelszavaknál is fejlődnie kellene...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 18:11:56

Mondjuk ahhoz az is kellene, hogy ne csak maximum nyolc karakter hosszú jelszót engedjenek használni.
A jelszó választás csődje

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 18:12:40

na a link meg lemaradt:
antivirus.blog.hu/2007/12/11/a_jelszovalasztas_csodje

Los Alamuszi 2008.01.22. 18:32:10

Az szerintem az iwiw (valódi) értelmével ellenkezik, hogy ne tudjak levelet írni ismeretlennek, vagy olyan ismeretlennek, akivel még közös ismerősünk sincs.
Mert, mi van, ha bejelölöm a régi szomszédomat, aki épp nem emlékszik rám, ezért rákérdezne, hogy honnan ismerjük egymást (de, természetesen, azért nem jelöl vissza, hogy ezt megtehesse, és, mondjuk a többi hajdani szomszéd nem iwiw tag, tehát nincs közös ismerősünk?)
Tudom, gyakoribb, hogy Kovács Ivettke 1,5 éves kislány jelölget végig ismeretlenül, de én (régi beidegződés) még mindig szarul érzem magam, ha valaki jelöl, és nem tudom elsőre kizárni, hogy csak ilyen ismerős szám növelő jelölés, és még nekem van lelkiismeret furdalásom, hogy nem emlékszem rá, pedig kellene.
Ja, és persze, biztos én vagyok túl jólnevelt, de, ha nagyon régi ismerősre bukkanok, akinél nem is várom el, hogy kapásból emlékezzen rám, hát, én biza a jelölés mellé mindig dobok egy levelet is (ugye, természetesen, ismeretlenül), hogy én vagyok én, és, hogy innen ismerjük egymást...

Jack__Bauer 2008.01.22. 18:54:21

Javaslom, hogy aki úgy érzi, hogy zavarja a kapott spam, az írjon vmi kedveset a meghívó küldőjének. Hátha elgondolkozik a

3000. levél után a felelőtlen meghívóküldözgetés veszélyein...

Jack__Bauer 2008.01.22. 18:55:53

Los Alamuszi: a megoldás egyszerű - visszajelöl, ír\válaszol, aztán eldönti, hogy tényleg ismer-e. Ha nem, és zavarja, akkor töröl az ismerősök közül. Ennyi.

buherator · http://buhera.blog.hu 2008.01.22. 19:31:48

@bög
Sajnos az iwiw az egység sugarú júzer számára A Közösségi Hálózat, és az emberek ismerőseinek többsége egység sugarú júzer... Arra azért kíváncsi leszek hogy mi lesz ha magyarítják a Facebookot (ha már meg nem történt)

A legjobb szerintem az lenne, ha a spammerektől felgyűrűzne a kizárási/figyelmeztetési hullám egészen azokig, akiknek már semmi közük a spamhez, csak ismerik a spammert, mert így talán IRL kapnának az ismerőseiktől a pofájukba. Bár ki tudja, hogy már milyen szövevényes csatornákon jut el egy-egy meghívó a kis köcsögökhöz...

tolvajp 2008.01.23. 05:32:11

Örülök, hogy tetszett.
Tényleg nem lenne egy nagy bonyolultságú dolog ezt kiküszöbölni, de még a mostani rendszer is romokban hever. Amíg az nincs meg, ne várjunk csodákat.

Conquistatore 2008.01.23. 07:08:51

Sziasztok,
Tetszett a szöveged Tolvajp:)
Igaz ismerlek nah de mind1
Nagyon jó lett:)

cso zsi · http://www.ingyen-jatekok.com/ http://www.demonoid.me/ 2008.01.23. 07:42:30

Egy "spammer" meghívójának üzenete:
Hát muszáj volt elköltöztetnem magam egy szebb helyre, mert már fél M.o. utál! Köszönet annak a féregnek aki ezt tette! Akkor sem törlöm magam -ről (mert néhányan ezért lobbiznak) bízom a gépházban, csak megoldják valahogy!

Idő közben kiderült, hogy a meghívottamnak sincs semmi köze az egészhez, ugyanis 6 napja nem járt netközelben (2008.01.12.-től visszaszámolva!!!). Ez úton szeretnék megkérni minden kedves felháborodott egyedet, hogy ne írjon, kiderítjük mi folyik itt, de már nem kérek több fenyegetős, anyázós üzit.
Töröld ki, amit a nevemmel fémjelezve kapsz, aztán jól van, nem kell megnyitni, nem én küldöm!

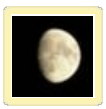
Ja, meg egy kérdés! Mindenki a potencianövelő cég reklámját kapja? Mert fel lesznek lassan jelentve! És akkor kiderül, hogy mi folyik itt!

További szép napot mindenkinek!

Van olyan spamom, ahol három lépcsőben törölték a meghívókat, de a kapcsolatok megmaradtak így visszafejthető egy még nem kizárt meghívóig.

ReWriter · http://miazhogy.blog.hu 2008.01.23. 09:49:09

Én azt vettem észre, hogy mindig 4 embernek küldik el a spam-et. És milyen érdekes, a négy ember regisztrációs száma egymás melletti számok. Ez is ki lehetne szűrni. Ha n levelet küldenek, akkor a regisztrációs számok max és min közötti különbsége n-1.



movhu 2008.01.23. 11:06:46

Ma betette a kaput egy másik barom, írtam is róla:
mover.blog.hu/2008/01/23/niki_noemi_es_a_tobbi_iwiw_kreten

Jack__Bauer 2008.01.23. 12:56:59

A legviccesebb, hogy az iwiwen csak akkor tudod törölni a levelet, ha már megnyitottad... Akkor is, ha ordít róla, hogy spam (mert mondjuk 3 példányban is megkaptad, ugyanazzal a tárggyal, ugyanattól az ismeretlen - törölt - személytől. Ez is milyen már?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.23. 13:47:06

Egy kis olvasnivaló hasonló nyűgökről:
gery.blog.hu/2008/01/23/torold_a_myspace_regisztraciod

zlad (törölt) 2008.01.23. 18:32:31

Sziasztok!

Nem pont iwiw téma, de meg tudja nekem mondani valaki, hogy az ESS tűzfala automatikus módban mennyire hatásos? Azt látom, hogy sok eseményhez nincs szabály, de nem igazán szeretnék a tanításával bíbelődni, mert nem értek annyira hozzá. Előre is kösz az infót!

(z)

Conquistatore 2008.01.25. 12:20:22

NAh Tolvajp-miért nem írsz?:O:P:P:P:P

Vidi Rita · http://www.hosnok.hu 2008.01.26. 09:23:23

Szia István!

Csináltam Neked egy kis munkát;) Tudom, hogy szeretsz olvasni:)))

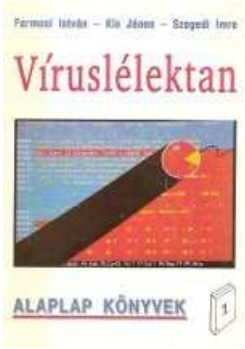
Várom az izgi bejegyzést!

Automatizálás, heurisztika, múltba révedés...

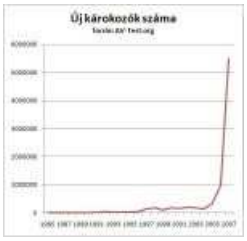
2008.02.01. 11:37 | Csizmazia István [Rambo] | 3 komment

Címkék: windows statisztika vírus féreg heurisztika darabszám

Szinte idilli állapotot mutat, **ha kicsit visszaevezünk a múltba**, és a Magyar Elektronikus Könyvtárból is elérhető "Víruslélektan" című könyvben lapozgatunk. Az **1990-ben kiadott írásban "mindössze" 5-6 ezer** közé eső vírus mennyiségből kimazsolázott érdekességekből kapunk ízelítőt, leírásokat, háttérinformációkat.



Manapság viszont egyre sokasodnak a beszámolók arról, hogy a megjelenő kártevők száma hihetetlen mértékben emelkedik. Íme egy riasztó kép az AV-Test.org oldal adataiból.



Az explonenciális növekedésről több antivírus cégnél is beszámolnak, a Sunbelt szerint a kisebb AV vállalatok nem is fogják bírni a versenyt, az F-Secure jelentése pedig napi 17 ezer! kártevő megjelenéséről számol be, amit nyilvánvalóan hagyományos, kizárólag **kézi elemzéssel - adatbázisalapú bővítéssel - képtelenség feldolgozni**.

Minden nagyobb víruslaboratóriumban bevezettek már valamilyen megoldást, amellyel a kevésbé kiemelt variánsok automatizált elemzése és vírusadatbázis bővítése történik, és így a szűk keresztmetszetet jelentő magasan képzett emberi erőforrást a kiemelt esetekre tudják fordítani.

A felismeréseknél eddig is komoly erőfeszítések történtek a generikus, egész családokat azonosító jellemzők meghatározására, de kétségkívül ésszerű megoldás emellett a proaktív technikák használata, így korábban a virtuális kódemuláció, mostanában a heurisztikus

felismerés kerül egyre jobban előtérbe. Az ESET programjai rendkívül erős heurisztikai képességekkel rendelkeznek, ez pedig nem csak hatékonyan ismeri fel az új kártevőket, hanem kevés esetben hibázik, azaz riaszt tévesen nem vírusos állományokra. Az itt használt úgynevezett Kiterjesztett heurisztikának (Advanced Heuristics) éppen az a feladata, hogy **proaktívan ismerjen fel vadonatúj, korábban még ismeretlen kórokozókat**.

Érdemes még az alábbbi táblázatra is rápillantani: nem minden operációs rendszerre jellemző ez az elképesztő növekedés, a leginkább támadott Windows platformmal szemben a MacIntosh és a Linux már évek óta tudja tartani a száz alatti darabszámot.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/320731

Kommentek:

BenkoG 2008.02.05. 14:27:28

Nemrégiben Mac felhasználók egy csoportjával volt némi "afférom" azon okból, hogy megjelent a képviselt vírusirtónk Mac Editionja. Ők akkor sem hitték el nekem, hogy nem a mostani "status quo" számít, hanem az, hogy mi lesz holnap, mire kell számítani és mi lesz akkor a megoldás. Mert akkor biza lesz nagy kapkodás, hogy mit is tegyek, meg a fejeknek falakba való ütögetése, hogy "bárcsak akkor..."
Nem vagyok próféta,a szemüvegemen nem tükröződnek vissza zöld terminál-karakterek a félhomályban, nem irányítom billentyűzetről a grafikus felületet (ahogy a filmipar ezt próbálja bizonygatni) - kényelmes vagyok és "egerészek".
Mindazonáltal most is igazolva látom: lesz még fogaknak csikorgattatása... napi 17ezer új vírus... ajjaj. Hámmég a Windows.
Ajjajaj!

BenkoG

BenkoG 2008.02.05. 14:29:51

P.S.: A minap került a kezembe a fentebb említett könyv (ugyan nem dedikált, de SAJÁT példány), anno mint a Bibliát, olyan áhítattal vettem a kezembe... kicsit még most is.

BenkoG

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.05. 15:50:22

Szia BenkoG!
Igazából egyrészt ezek az alternatív platformok valóban sokkal biztonságosabbak - hogy csak annyit mondjak, a programok nem a rendszer könyvtárba szemetelnek, hanem a /home-ba, userként csak akkor kell begépelni a root jelszót, ha olyan műveletet végzel, amihez tényleg kell, stb., stb. - de azért a megtévesztés itt is meg fog majd jelenni, én is attól tartok. Ha divat

lesz áttérni, akkor sok olyan képzetlen ember is ül majd a gépek előtt, aki eddig bambán kattintgatott az Outlook Express levél mellékletekre, itt pedig a "kodekcsomagokra", ingyen játékokra, hamis ellenőrizetlen forrásból származó programokra fog kattintgatni. Ha elér egy elég jelentős számot a Mac és Linux felhasználók tábora, én is attól félek, hogy eleinte virtusból, később pedig kőkemény üzleti okokból ráindulnak a kártevő készítők. Több mint tíz éve Linuxozom, szerencsére egyelőre valóban nagyságrendekkel biztonságosabb.

Háztűznézőben

2008.02.04. 14:13 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google maps dubai cím

Tegnap találtam egy zseniális kommentet az Index fórum MLM tapasztalatok című szobájában, és mivel volt némi kapcsolat a korábbi Dubai MLM cikkel, beírtam oda hozzászólásként. Éjszaka azonban revideáltam a nézeteimet, és rájöttem, megér egy önálló cikket is.

Miről is volt szó a Pillangom 17864-es sorszámúpostjában? Ő, illetve a hivatkozott angol fórumozó szépen begépelte a címet a Google Maps-be, és bár lehet, hogy olajkutakat és felhőkarcolós irodákat vártak, egy szimpla családi ház bukkant fel a képernyőn. Előtte nem sokkal ugyanazon a címen a **"AATurboCharge Marketing Inc."** szerepelt, most viszont már a **"DubaiMLM"** - igaz a változatlan címen megadott telefonszám is megváltozott. Jó emlékeink szerint Bill Gates is egy garázsban kezdte, szóval ez még önmagában nem biztos, hogy minősít egy vállalkozást. Ennek ellenére az email cím gyűjtéssel kapcsolatos aggodalmaimat fenntartom, nekem nem tűnik valóságosnak a dolog, és ezt korábban sem rejtettem véka alá.

Ha tévedek, és áramlanak majd a dubai dollárok, akkor remélem megkapom a sörömet a sikeres MLM tagoktól, és titkon remélem, hogy majd a Dubai MLM csúcsra jutott vezérkara Billt és Melindát megszégyenítő módon még többet fognak zsíros profitjukból nemes célokra való adakozásra, adományozásra fordítani.

A képen a Skála áruház és az autókkal zsúfolt parkoló: a valóságban már rég nem így van

Ha domain bejegyzők címeire keresünk, akkor egyébként már nem ilyen könnyű a térképészkedés. Ha eleve .**info csoportba tartozik a oldal**, ott csak pénzért tekinthetünk be az adatokba, ezért is választják egyre inkább a kártevő terjesztők az ilyen címeket. Másfelől a bejegyző és az az üzemeltető gyakran nem azonos, és ha nem amerikai címről van szó, a térkép **adatbázis felbontása és naprakészsége** csapnivaló módon régi állapotot mutat. Ennek ellenére tetszett az ötlet, földig emelem a kalapom.

Kár, hogy nem tudunk így segíteni a StormWormos vírusírókat üldöző szentpétervári hatóságoknak...

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/324786

Kommentek:

Nincsenek hozzászólások.

Keress minden e-mailel(sic!) akár 700 Forintot!!

2008.02.05. 16:12 | Csizmazia István [Rambo] | 18 komment

Címkék: spam üzlet email becsapás

Akár, na persze! Ha bankban járunk, jól ismerjük már ezt: a THM **akár** - és itt a plakáton, vagy prospektusban egy hihetetlenül és valószínűtlenül alacsony értékű százalék következik. Persze igazából nem is a nyelvészkedés okán jön a képbe a dolog, hanem hogy ekkora ostobaság is elhangozhat, és szintén nem kevésbbé szomorú, hogy valószínűleg olyan is **akad, aki mindezt el is hiszi**. Persze, ha már nyelvészkedés, akkor az **"e-maillel"** szót két l-lel illett volna írni...

Íme a levél:

> " Keress minden e-mailel akár 700 Forintot!!
>
> Találtam egy weboldalt, amivel pénzt lehet keresni az Interneten. Én fél órája regisztráltam, de máris kerestem ezer forintot, és a határ a csillagos ég! Nézd meg! Nem bánod meg.
> Klikk ide: http://wmpartner.try.hu/?pid=katang "

Számoljunk csak: nem akarunk sztahanovisták lenni, küldjünk ki "csak" **napi száz e-mailt**, az akkor napi 70 ezer, 20 munkanappal (na nehogy má' hétvégén is robotoljunk ;-) számolva is **havi 1,400,000.- HUF**, persze nem csúnya szám így leírva, ~~a papír~~ a képernyő mindent kibír, csak hát kissé érthetetlen, hogy **vajon a buszsofőrök, vasutasok, szívsebészek, áruházi eladók miért dolgoznak rengeteget ennek az összegnek a töredékéért?** Biztos, mert nem ismerik a varázsmódszert ;-) Csak elküldenék az e-maileket, aztán mindenki menne Spanyol honba, meg Görögországba nyaralni, és a hazai GDP is rekordokat dönthetne.

Na mindegy, ne mérgeskedjünk, még mielőtt megint kritikus megjegyzésekkel illetnek minket, mint a korábbi Dubai MLM kapcsán. A "Siker, nők, pénz, csillogás" jegyében azt azért érdemes megfigyelni, hogy **a kedvcsináló felső kép itt is hasonló impozáns felhőkarcolókat mutat**. Talán ez a záloga, hogy elhiggyük...

Remélem, sokan látták annak idején a remek Ösztön (Instinct) című filmet, szóval **a mit veszíthetünk kérdésre jobb esetben itt is a naívságunkat lehet a jó válasz**.

· 1 trackback

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/326507

Trackbackek, pingbackek:

Trackback: BuheraBlog 2008.02.05. 18:52:03

Az agyam eldobom!Ilyen nincs!Fullstart.hu. További info itt.

Kommentek:

buherator • http://buhera.blog.hu 2008.02.05. 18:41:44

Uhh, ez fájt!
"Valamint ellentétbe például a Google AdSense programmal"

Mondjuk aki ilyen URL-ekben megbízik:
server10.megacp.com/~fullthu1/part/reg.htm

az meg is érdemli...

Gondoltam megnézem a Page Infot:

keywords: animal,bugyi,bula,cici,csöcs...
description: sex full love girl youngest teen fucking

A regisztrációs form pedig a fullstart.hu-hoz megy el (whoist nézni érdemes).

W Joe 2008.02.05. 19:38:19

Kemény :)

0xFFFF 2008.02.05. 21:34:26

Ezz kamú ! Ne higyjetek ezekknek ! Aki sokk pénszt akar keresni az kűdjön nekem 2000 forintot és egy órán belül viszakűdök 4000 forintott ! És ez IGAZ !

Gabo58 2008.02.06. 08:16:40

Ezz kamú a javából a cikket már tegnap olvastam.Gondoltam kicsi utána járok a dolognak.az origo munka otthon na vagy 20cinre írtam kapptam is tömkelegével még most se értem a végére a jobbnál jobb lehetőséggeket kinálók között.Na 1-ső kategória akinek veb árúház van lépj-be vegyél valamit szervez be 3 embert!Na persze rozsaszín csekken 600-700 add fel.M azután az anyag.A m2.az a csúúúcs figyú ki küld egy sima e -mailt mert ő takarékos nagyon röviden ,hogy regisztrálj 600 ft boritékba tedd a lét mert igy olcsobb küld el neki .Az utobbinak utána eredtem mert ez a bíztít ki verte a megadott cím a tudakozónál nincs semilyen telefon be jelentve Horváth néven. Nagyon jól mehet neki!!Szóval nagyon jó ,hogy ezt a téma emmelted mert az emberek szemét nyitni kék .Mert igy könnyen lehet ,hogy amit állit igaz csak számold ki 700x XY azazér

nem semmi ugye. Mert sok a naiv ember,és munkát keresők száma és ez csak nő ni fog .Hiszen a nyugdíj rendszert át alakitották rendessen. A leszázalékoltak felét siman kivágják ,erröl is tunák odákat zengeni .Tehát az a sok ember mind probálkozik ugye beteg gonja van tehát otthoni meló kéne na itt a csapda.

0□FFF 2008.02.06. 08:23:48

Gabo58 !!!

Az ember roszul van irva !!! Hejessen ENBER !!!

insert_click · http://www.kutyapoint.hu/ 2008.02.06. 08:38:58

off: 0xFFFF: neked is b..sza a szemed?! ;) egyébként pedig helyesen: enyber off
on: aki bedől ennek az megérdemli, de el kellene tiltani őket a nettől, ezek miatt meg a barom körlevél és spamek tömkelege.

movhu 2008.02.06. 08:51:37

Sokat segítene a dolgon, ha valamilyen törvény születne erről, vagy legalább a szolgáltatók ASZF-je tartalmazna olyan kitételt a webhostingoklók felé, hogy letiltanak minden olyan elérést, akinek ilyen baromság van az oldalán.
Illetve a másik oldalról is meg lehetnem fogni, azaz a spam-ek mintájára lehetne egy online adatbázis, ami alapján a szolgáltató a hálózati eszközeiben letilthatná az ilyen irányba menő forgalmat.
Nem is oly rég pont ezeknek a barmoknak írtam nyílt levelet a blogomban, de tudom, mindig is lesznek olyanok, akik benyelik azt, hogy munka nélkül is lehet pénzt keresni.

sklaudia 2008.02.06. 09:08:10

Mi vaaan? Mi a csuda ez itt? Kik írják a kommenteket? vagy ez most itt vicces? vagy mi vaan? Tényleg nem értem, magyarázza már meg valaki pls! Pontosabban: magyrázza mán meg vakali !

Gabo58 2008.02.06. 09:35:42

Bocsi OxFFFf !!! Tudom igazad van .De siettem az irással,be kellet érnem a melóba.Ahogy jött irtam. DE tudom ENBER. De nem ez a lényeg.Az én szememet is sok minden b...!!
movhu én nem olvastam,de jók a meglátásaid és nagyon egyetértek veled!!! Az a lényeg,hogy valaki legalább próbál valamit tenni.

◄ViZion 2008.02.06. 11:12:05

És a legrosszabb, hogy vadidegeneknek kiadnak még 500 mail címet, amivel ugye újabb mongoloididiótabarmoktól kapok levelet.
Belezőkarmolóval megvakítani mindet, a végbelén át!!!
:)

insert_click · http://www.kutyapoint.hu/ 2008.02.06. 11:24:17

Gabo58: szerintem csak vitz volt ;)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.06. 14:16:25

Hello Gabo58!
Maximálisan egyetértek, hogy a nehéz gazdasági helyzet és a munkaerőpiaci problémák miatt sok rászoruló úgy kapaszkodna ezekbe a lehetőségekbe, mint egy utolsó szalmaszálba. Én nagyon sajnálom ezeket a reménykedő embereket, amit kihangsúlyoznék, hogy ma már nélkülözhetetlen, hogy valaki jól végiggondolja, mikor lehet hinni egy ajánlatnak, és mikor

nem.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.06. 14:30:55

@Movhu!
Minden törvény annyit ér, amennyit betartatnak belőle. Itt van például a "ne lopj nevű" tétel a tízparancsolatból, ami csöppet sem idejétmúlt. Ha például valaki 34.5 milliárd HUF-ot "hűtlenül kezel", szabadlábon védekezhet és a végén esetleg kap 3 milla büntetést. De ha valaki a Nyugati postán behajon a pult mögé, és ellop, kiránt 500 forintot, azt már biztos bilincsbeverve viszik el a rendőrök.
Amiben én reménykedem, hogy az ilyen blog, a sok cikk, újság, tv-műsor előbb-utóbb felhívja a kevésbbé figyelmes, de nagyon is érintett többség figyelmét a veszélyekre.
Ami még fontos: a Qui prodest, vagyis kinek az érdeke kérdés. Egy ISP-t baromira nem érdekli, hogy vírusos levelek mennek, spamek küldődnek a hálózatából, amíg a havidíjat fizetik. Inkább ezen kellene változtatni, hogy érdekük legyen tisztántartani a hálózatukat.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.06. 14:46:22

@Sklaudia!
A világért nem akarnék itt CovBoy (Commodre Világ) babérjaira törni, de ha hiszed, ha nem a kommenteket az olvasók írják :-)
Az írás egyébként egy kéretlen e-mailekben terjedő csalásról szólt - sok ilyen van sajnos mostanában - ezen a blogon is igyekszünk ezekről beszámolni, gyere máskor is olvasni!

Moonline 2008.02.06. 17:29:01

Nem ehhez a cikkhez tartozik de megkérdezem megint, hogy hogy áll már a magyar verziójú nod32, és az eset smart security? Elvileg december közepén ki kellett már volna jönnie a magyar verzió(k)nak most meg már február van, elég elszomorító h ennyi időbe telik lefordítani, akkor legalább ne ígérték volna decemberre.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.08. 12:43:16

Szia Dante01!
Sajnos csúszás van valóban. Annyit tudok a dologról, hogy állítólag már tényleg a küszöbön (1-2 hét) van, a francia és holland honosítás már végre megjelent, tűkön ülve várjuk a magyart.
www.wilderssecurity.com/showthread.php?p=1178559

SPY89 2008.02.19. 21:37:21

Vannak elviekben olyanok amik ténylegesen fizetnek de azoknak a feltételei olyanok, hogy ember legyen a talpán aki azt teljesíteni tudja pl csak 20000 eurónként szedhetet ki és akkor 1cent/mail és mondjuk napi 5mailt kap az illető és azokat meg 20percig kell nézni szóval meg őszül mire lesz 20000 eurója :D.. Én most találtam erre a blogra nagyon jó cikkek vannak (üdv az írónak és mindenkinek :))

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.19. 22:16:23

Hello Spy89!
Üdv a klubban :-) Hát mondhatnám nagy slengesen azt is, hogy aki egy e-mailt 20 percig nézeget, sikeres ember nem lehet. De inkább azt mondom, én még nem láttam olyan embert, aki látott olyan embert, aki így keresett volna rendes pénzt. Inkább urban legendsnek vagy átverésnek tűnik...

A probléma a billentyűzet és a szék között van

2008.02.07. 16:16 | Csizmazia István [Rambo] | 4 komment

Címkék: windows linux jövő biztonság social macintosh múlt c64 jelen engineering

Kicsit ünnepi, kicsit emlékező, de jelent és a jövőt sem elfelejtő post gépelődik ezekben a pillanatokban. 47 éves lettem én, meglepetés e ~~költemény~~ blogbejegyzés. Kicsit olyan **visszagondolni erre a nem is oly távoli múltra**, mint mikor Al Bundy azt mondja: "Gondolj bele fiam, mi annak idején még óvszer nélkül szeretkeztünk!".

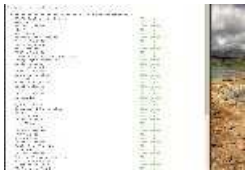
Furcsán hangozhat a mai fiatalok számára - **akik talán nem is láttak már CD/DVD nélküli számítógépet** - hogy a számítógéppel való kapcsolatom 1979-ben indult, egy évig nagygépes operátorként dolgoztam egy FÜTI (Fővárosi ÜgyvitelTechnika Iroda) nevű cégnél. Ízelítő volt ez **a szobányi központi egységek, a kétméteres bolgár lemezegységek és a lyukkártya-olvasók** hősi világából.

Akkor biztonsági szempontból még "csak" az volt **az ember legnagyobb gondja, hogy hibátlanul lefusson a programja egy hétvége alatt, vagy hogy az operátor ne essen orra a küszöbben a lyukkártyás dobozzal a kezében**, mert akkor több napig lehet újra rendezni azokat. És milyen Murphy, az adatkártyáknál mindegy volt a sorrend, a "//EXEC JOB"-bal kezdődő program kártyáknál viszont fontos volt a sorrend, és hogy-hogy nem, éppen mindig ez utóbbiaknál remegett meg a lábunk ;-)

Szóval az akkori **biztonság** még jobbára kimerült abban, hogy **idegenek ne jöjjenek a gépterembe**, továbbá **épeszű ember a kódjában ne osszon nullával**. Na ez az, ami mára gyökeresen megváltozott, a programok fő funkciója mellett ugyanolyan fontos, hogy biztonságosan működjenek. Nagyon keserű volt a számíze, mikor az alap C64-es trükk (a programvédelem kivezeti a 1541-es olvasófejét egy extrém szélső pozícióba, ahonnan csak szétszedéssel és kézzel lehet csak visszahozni) után **elkezdtek megjelenni az igazi Commodore gépeken terjedő vírusok is**, amelyek a nem leragasztott floppy lemezeken egy DIR parancs útján is tudtak már vándorolni. Ezek után már semmi nem volt olyan, mint korábban :-(

Hiába ül valaki Mac előtt, ha óvatlanul kártékony kodekcsomagra kattint

A harc azóta is zajlik, de nem elég, bár **nagyon fontos a jó védelmi program, kell mellé megfelelő hozzáállás, óvatosság is**, és itt jön a képbe egy mai cikk, amely nagy pesszimistán a Mac-es gépek veszélyeztettségét jósolja.



Az RKHunter egy színvonalak rootkit kereső Linuxra

Belegondolva inkább realista, mint pesszimista, és itt jön a félelem: **régebben akár igaz is lehetett a mondás**: "Félsz a vírusoktól? Használj MacIntosht és élj nyugodtan!" vagy "Biztonságra vágysz? Válts Linuxra, és többé nem lehet semmi bajod!"

A CHKRootkit segítségével ismert linuxos rootkitekre vadászhatunk, valamint a fájlrendszerünk épségét ellenőrizhetjük

A váltást persze megértem, sőt én is részese vagyok, de úgy érzem, hogy egy időzített bombán ülünk, egyszer el fog indulni itt is a Windowson "megszokott" invázió, és akkor már csak az fog számítani, hogy a felhasználó ért-e a saját rendszeréhez vagy sem? Az fog számítani, hogy ha aláíratlan webhelyről, frissítési forrásból származó kodeket, Windows emulátort, programcsomagot vagy 3D-s játékot kínálnak a kéretlen e-mailek vagy webes linkek, **akkor hányan kattintanak majd erre**, hányan használnak majd biztonsági programokat az alternatív rendszereken, hányan tudják egyáltalán értelmezni majd a rendszer logállományait vagy **hányan veszik egyáltalán észre, hogy a rendszerüket megpiszkálták**?

Fájlkiszolgáló és levelezőszerver védelmére számos Linux platformra évek óta van jó vírusvédelmi megoldás

Mindenesetre a helyzet adott, **minden OS felhasználó emberből van, megtéveszthető, és a gyengepont keresése a jövőben ezeket a helyszíneket sem fogja elkerülni** - Fülig Jimmy őszinte sajnálatára.

Ubuntu Linux teljes harci (Compiz Fusion) díszben

És bár egyelőre kétségtelenül **a Windows világ a legnagyobb célpontja, azért az alternatív rendszereken is tűzre-vízre (Windows emulációra) vigyázni kell**, és ezután (is) tartsuk szárazon azt a bizonyos puskaport.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/329404

Kommentek:

□enkoG 2008.02.08. 12:57:47

Jajj, István, az istenke áldjon meg, a szívemből szólasz, hát végre máshonnét is olvashatom ezt... remélem, a beszeljukmac.com olvasói is olvassák ezt a blogot, mert igencsak rájuk fér.
Bocs, de ezt nem lehetett kihagyni.

Vidi Rita · http://www.hosnok.hu 2008.02.08. 14:14:35

Boldog Szülinapooooooot, istenke éltessen sokáig!:))

Na, mostmár normálisan írok:)

Nem szeretek ördögöt a falra festeni, de azért befizetnék arra a pillanatra, mikor elkezdenek majd aggódni egy cseppet azok, akik most túlságosan nagy biztonságban érzik magukat.

Ne legyen úgy!
Maradjon védett legalább a Mac és a Linux!
Maradjon számunkra valami menekülési útvonal féle!
De nem marad:(

Bár, én nem értek sem a Mac-hez, sem a Linuxhoz, de ezeknél a felhasználónak kimondottan butának kell lennie, nem?

Oké, hogy az ember a leggyengébb láncszem, és amikor csak egy kattintásra van a totális összeomlástól, akkor biza kattint.
De a Mac-en meg a Linuxon nem bonyolultabb ez egy hangyányit?
Mert, ha már két kattintás, akkor a fele buta kihullik... És így tovább:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.11. 14:56:36

Szia Rita!
Koszi a jokinvansagokat :-)
A cím egyébként Hancu mestertől (CoV) származik, szerintem nagyon kifejezo...
A remenykedesre visszateve, szerintem biztonsagos rendszer NINCS. Mindenhol muszaj kuzdeni, folyamatosan figyelni, naplozni, biztonsagi programokat futtatni, frissiteni es sajat munkat menteni. Itt egy jo pelda, hogy Linux eseten is vannak sajnos problemak:
hup.hu/node/50696#comments

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.18. 10:22:39

Egy érdekes felmérés:
Mire számítanak egy felmérés alapján a Mac felhasználók:
www.sophos.com/pressoffice/news/articles/2008/02/mac-poll.html

Csak ennyi kellene a csalások ellen

2008.02.11. 16:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac windows linux figyelem csalás truecrypt feltételek kódolás alap óvatosság

Sokszor és sokat vétkeznek ellenünk a számítógépes bűnözők gondolattal, szóval és cselekedettel, nekünk viszont a "mulasztással" szóval kapcsolatban akadhatnak restanciáink, pedig **többnyire elegendő lenne néhány ökölszabályt betartani**, és jelentősen minimalizálhatnánk a károkat. Vajon miért nem tesszük? Ez egyelőre rejtély.

Mik is ezek? Rendszeresen **ellenőrizzük banki számlánkat**, nincsenek-e rajta gyanús tételek. Ez vonatkozik a napi SMS egyenlegekre, de ugyanúgy a havi postai levélben érkező záró értesítőkre és az esetlegesen igényelt hitelek évvégi összesítésére is. Azt már nem is kell mondani, hogy **bizalmas információt ne küldjünk el csak úgy e-mailben**, hiszen sima szövegként utazik, és óvakodjunk ezeket telefonba bemondani, mielőtt százszázalékosan **meggyőződtünk volna a hívó személye felől**.

Sokan **őriznek bizalmas adatokat, jelszavakat, leveleket, dokumentumokat a számítógépükön**, azt gondolva, ott biztos helyen vannak. Érdemes lenne minden ilyen kényes személyes adatot valamilyen titkosítással ellátni, és mondjuk egy titkosított meghajtón vagy partición tárolni. Jó hír, hogy ennek megvalósítása sosem volt még egyszerűbb: például az ingyenes TrueCrypt segítségével ezt most játszi könnyedséggel megtehetjünk mind Windows vagy Linux, mind pedig MacIntosh platformon. A kezelése pofonegyszerű, egy átlagfelhasználó is könnyen elboldogul vele. A létrehozott partíciók készítésekor pedig válasszunk erős jelszót, sok kis- és nagybetűvel, számmal valamint különleges karakterrel; ja igen, és lehetőleg ne veszítsük el, mert úgy magunkat is kizárjuk.

Közösségi oldalon gmail jelszót kérnek - ejej...

Ha emellett rendszeresen frissítjük operációs rendszerünket és egyéb programjainkat, jó minőségű és **naprakész vírus- és kémprogramirtót használunk**, valamint tűzfallal is védjük magunkat, WiFi kapcsolatunkat legalább Mac címszűréssel és WPA2 kódolással látjuk el, úgy mindent megtettünk, amit technikailag csak megtehettünk. Ha pedig kedvünk van hozzá, már csak óvatosnak kellene lenni és máris jófelé ülünk a lovon.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/335119

Kommentek:

Nincsenek hozzászólások.

Kizökkent világ

2008.02.12. 17:16 | Csizmazia István [Rambo] | 1 komment

Címkék: gép csalás hamis használt fertőzött fabillentyűzet

Koyaanisqatsi - ha mond ez valakinek valamit, jó régen láttuk már a mozifilmet. Sok mindenre fel vagyunk készülve, úgy érezzük, minket már nem érhet meglepetés, ám végül kiderül, van lejjebb. A mai hírben azt olvashatjuk, (tisztára mint hogy a suszter cipője lukas) hogy az AVSoft Technologies **antivírus letöltő oldalát is megfertőzték kártékony IFRAME kóddal**, és ettől kezdve kártevőket töltöttek le a látogatók - igaz, ez az eset Indiában történt.

Hogy már minden megtörténthet, és nyugalmas hétköznapi emberek helyett a végletekig gyanakvó, paranoiás elmebetegnek kellene lennünk, az a másik storyból világlik ki: hogyan aknázzák ki a csalók az internet világát zseniális trükkjeikkel. Szó van itt a Fából faragott királyfi helyett fából faragott számítógép billentyűzetről (ezt egy igazi számítógép helyett kapta a pénzéért az áldozat), de úgy tűnik, az oly **régi 419-es nigériai csalás is képes újabbnál újabb köntösbe bújva**, turbosított extra változatokkal színre lépni. Nekünk a nigériai lelkipásztor tetoválási trükkje tetszett a legjobban, de úgy látszik tényleg a balek a legelterjedtebb árucikk a Földön. Aki szereti a cirkalmas urbanlegends típusú történeteket, vagy csak képbe akar kerülni a csalási módszerekkel és a csalókra vadászókkal kapcsolatban, ne hagyja ki. Nálunk is jelent meg érdekes olvasni való, igaz ez nem kifejezetten a csalásokkal, hanem a hoaxok és lánclevelek útján terjedő igaz vagy igaznak látszó történeteket öleli fel Legendavadászat címmel.

Mi pedig talán azzal egészíthetnénk ki korábbi intelmeinket, melyeket a vadonatúj, de vírusfertőzött készülékekről írtunk, hogy az árverési portálokon vagy **használtan vett készülékek esetén is legyünk elővigyázatosak**, particionáljuk újra a merevlemezt, vagy **kezdjük a birtokbavételt egy alapos vírus- és kémprogram ellenőrzéssel**. Ja és Commodore 64-et csak megbízható forrásból szerezzünk be ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/336535

Kommentek:

SPY89 2008.02.19. 23:00:32

lol még anno volt ilyenem megbízható forrásból nem fa :P

A Mindentudás Egyeteme

2008.02.13. 12:40 | Csizmazia István [Rambo] | 12 komment

Címkék: gpl veszély tudás nyílt antivírus forráskód hibajavítás clamav

Mai hírként olvasom, hogy megjelentek a január eleje óta várt hibafrissítések a ClamAV víruskeresőhöz. A kártevőkészítők számos esetben **előszeretettel intéznek támadást, keresnek gyenge pontot a védelmi eszközökben**, szinte minden vírusvédelmi szoftvernél kellett már rendkivüli programfrissítés keretében - **zömmel puffertúlcsordulási hibák miatt** - javítást kibocsátani.

Szóval nem csak a kártevőkészítés, hanem **a kihasználható hibák keresése** is gőzerővel zajlik, legyen az operációs rendszer, elterjedt alkalmazás vagy akár éppen vírusvédelmi alkalmazás. A ClamAV - mint az közismert - egy **ingyenes és nyíltforráskódú csomag**, amit nem csak mindenki használhat, hanem még a forráskódját is letöltheti.

Azt maximálisan méltányolom, hogy ingyenesen (az AVAST és az AVG mellett) adják a programjukat. De itt jönne a logikus kérdés: bár tisztelem és földig emelem a kalapom a GPL előtt, sőt valamilyen szinten híve is vagyok (még Windowsos koromban is igyekeztem kizárólag legális vagy ingyenes programokat használni): jó dolog-e, hogy egy ilyen forráskód mindenkihez eljut?

Ha valaki ilyen módon **részleteiben közzéteszi a munkáját**, azért sok minden történhet. Ha valaki éppen egyetemista és vírusirtóprogramot szeretne készíteni, annak egy nagy lehetőség és remek adalék, tanulási lehetőség, ez kétségtelenül mellette szól. De nézzük, mi szólhat ellene? Lehet, hogy könnyebb túlcsordulási hibát keresni benne, hiszen látni a belsejét. De jöhetnek a "keselyűk" is, vélt vagy valós szabadalombitorlással vádolják meg (persze közben saját zárt forráskódjukat hét lakat őrzik). Ilyen perrekkel - még ha esetleg teljesen alaptalanok is - gazdaságilag és erkölcsileg könnyen tönkre lehet tenni egy céget.

Állítólag ennek a szobornak az áthelyezésével kezdődött a konfliktus

Ha egy pillanatra visszaemlékszünk a tavalyi Hacktivity második napján szereplő Dr. Kovács László előadására, amikor az észt-orosz hacker konfrontáció kapcsán az derült ki, **nagyon is lehet élni (vagy visszaélni) ilyen jellegű magasan képzett tudással**, amit ebben a konkrét esetben hivatalos NATO körök óvakodtak hadviselésnek nevezni, hiszen ez esetben akár háborús konfliktus is könnyen kialakulhatott volna Oroszország, és a NATO tag Észtországot támadás esetén kötelezően megvédő többi tagállam között.

Az összeomlott infrastruktúra következtében az ATM bankautomaták sem működtek

Vagy gondoljunk Angela Merkel kínai látogatására, miközben éppen állítólag **kínai eredetű trójai kémprogramokat fedeztek fel több német minisztériumban**. Az üzemszerű és kiterjedt kínai kémkedést sokan gyanítják és sejtetik, igaz bizonyítani roppant nehéz dolog - sokféle értelemben is.

Akkor most ezek alapján képzeljük el, **milyen minőségi tudás gyűlhetett össze a nagy, komoly vírusvédelmi cégek fejlesztőinél**, hogy csak a heurisztika két nagyágyúját, az ESET-et és a Kaspersky-t említsem. Mi történne, ha az adatbázisszerkezettől kezdve, a felismerés, a munkamódszer, a gyors és hatékony működés minden elemét, részletét kitennék forráskódban a netre? A konkurrensek nyilván pillanatok alatt rácsapnának, az egy dolog. **De nyilvánvalóan a rosszfiúk is**. Eddig is úgy zajlottak az új kártevővariánsok fejlesztései, hogy szépen le lett töltve minden jelentős AV program, és addig faragták a biteket különféle (NOP, Morphine, stb.) segítségével, amíg egyik se, vagy a legkevesebb vírusvédelmi alkalmazás riasztott rá, akkor már útjára lehetett bocsátani a kártevőt. Igaz, később a fertőzés napvilágra kerülése után minden vírusirtó **igyekezett frissített adatbázis kibocsátani**, de addigra a vírusírók munkapadján **már rég a következő darabokon történtek a finomítások**.

Na most ennek fényében **vajon használna-e a védelmünknek, ha ilyen kódok közkézre kerülnének? Én úgy vélem, hogy nem**, ezért ezen a biztonsági területen nem tartom ezt jó ötletnek. A titkosszolgálatoknál is az a jó állapot, ha minél kevesebb cikk, műsor szól róluk, minél kevesebb direkt közfigyelem irányul rájuk, nem szükséges (sőt káros, és más konkurrens titkosszolgálatok malmára hajtja a vizet) minden módszerüket részletesen leírni, közszemlére tenni, mert azt a rossz oldal is olvashatja, láthatja, sőt egészen bizonyos hogy olvasni és nézni fogja. Henryt idézve a Csengetett Mylord-ból: "Hová vezetne ez?" ;-) **Vannak információk, amiknek csak a szakértők fejében és Pandora szelencéjében vannak a helyük** - szerintem.

A fenti írás a magánvéleményemet takarja, de ha akár pro, akár kontra szeretne érvelni valaki, szeretettel várom a kommenteket.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Tízből öt kártevő hátsóajtót nyit
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/337513

Kommentek:

Vidi Rita · http://www.hosnok.hu 2008.02.13. 18:01:17

Nemtom, hogy pro vagy kontra, de érvelek:)

Teljesen igazad van!
A nyílt forráskód (és annak közzététele) úgy hangzik, mint valami karitatív cselekedet.
Gondolom, lényegében az is.

De vírustéma esetében tényleg nincs ok jótékonykodni.

Már az is világosan látszik, hogy az úgynevezett: otthoni felhasználók számára ingyenes verziók közel sem érnek annyit, mint bármi más, ami fizetős. Sorry, de ez van! Ki nem mennék a netre ingyenes avg-vel!

Most meg már egyenesen az a helyzet, hogy 3 terméknél többet nem is mernék ajánlani senkinek! A háromból is inkább csak kettőt:D

Szóval cinkes a helyzet.
Ha belegondolok, mi volt tavaly ilyenkor, mikor kezdtem a cégalapozást...

(Bár itt jegyezném meg, hogy ha én valamibe belekezdek, azon a területen hirtelen felpezsdülés tapasztalható. Ha céget alapítok, épp változik a cégalapítási törvény. Ha boltot nyitok, éppen változik a kereskedelmi törvény, de legalábbis kijön 8 kormányrendelet, ami összekutyul mindent. Ha tanfolyamra járok, minden változik a felnőttoktatással kapcsolatban. Szóval várható volt, hogy a vírusok terén is történik valami:D)

Tavaly még minden olyan kellemesen izgalmasnak tűnt vírustémában (így tél végén), most meg már néha olyan kellemetlenül nyomasztónak tűnik...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.13. 19:58:52

Szia Rita!
Üdv a fedélzeten. A nyílt forráskód jó dolog, szeretem, sokkal inkább jó, mint a 10,000 EUR-ért nézhető Windows kód ;-)
Amiben picit vitatkoznék, az az ingyenes AV progikkal kapcsolatos. Abban egyetértünk, hogy a komolyabb és fizetős programok jobban teljesítenek, de a semminél még mindig jobb, ha valaki AVG vagy AVAST-ot használ. Az észrevett fertőzésekkel legalább így is kevésbbé terheli a környezetet, és bár a reakcióidejük sokszor lassabb, mindenkinek ajánlani szoktam, aki nem akar, vagy nincs pénze másra.
Remélem a pechszériádnak vége szakad, végülis ez itt a Patkány éve :-)

zvaragabor 2008.02.13. 20:27:45

Én ki mernék menni a netre avg/avast/avira ingyenes veriójával minden további nélkül, de csak Firefox+NoScript és AdBlock Plus addonokkal. Na jó, azok nélkül is, de akkor csak tényleg azt a pár megbízható, minden nap látogatott oldalt nézném meg. Azért nincs a feature set annyira megtépázva az ingyenes verzióknál, hogy annyira megbízhatatlanok legyenek. Azért CLamAV-val más a helyzet, azzal már lehet, hogy nem kísérleteznék. Bár ez így értelmetlen vona, mert a ClamAv-nak(parancssoros), de még a ClamWin-nek(grafikus felület) sincs on-access scannerja a wines verziónál, így nincs is hol megállnia a helyét, legalábbis valós időben nem tudna nevezni(habár van olyan opensource antivir, amiben clamav motor van, és hozzáheggesztettek még egy realtime scannert is. meg aztán sourceforge.net-en is akad néhány hozzá.). Heurisztikával nem tudom hogy állnak(szerintem nem túl jól) az is lehet, hogy nincs is. Az adatbázis 210ezres, ez heurisztika/viselkedés elemző nélkül nem ér sokat pc-re. De ha mail szervereknél bávált...franc tudja.
Szerencsére tűzfalaknál nem így van, ott ott van pl a Comodo. Erős csomagszűrő megspékelve egy masszív HIPS-szel. matousec féle teszten ugyan még a 2.4-es volt tesztelve (ami még így is top helyezést ért el), de a 3.0 a hivatalos fórum lakói szerint alap beállítások mellett is átmegy minden teszten.

Biztonsági rések, exploitok mindig is lesznek, open source-nál talán hamarabb találnának, de talán hamarabb is reagálnak rá a fejlesztők. Vagy nem. :) Nem tudom. Nem láttam még ilyen közösséget, nem tudnám megbecsülni, hogy kb mekkora lehet pl a clamav fejleszőgárda, és hogy mennyire aktívan fejlesztik, eddig nem kísértem figyelemmel a ClamAv changelogját, meg a vele kapcsolatos híreket. :) Talán azért én se bíznám a rendszert egy nyílt forráskódú biztonsági programra.

Ui.:István megkaptam a pm-et a fórumon, köszi szépen a választ. Nem gond, hogy "késtél", nem volt sietős, még aktuális volt a kérdés.

zvaragabor 2008.02.13. 20:31:04

Lemaradt, ingyenes és jó tűzfalnak még ott van a Jetico, Online Armor is.

ragazzo 2008.02.14. 12:04:17

Sziasztok!

Ha már az ingyenes víruskeresőknél tartunk. Valaki megtudja nekem mondani, hogy miért nem csinál senki egy jó kis összefoglaló tesztet ezekről.Már írtam a PC World-be is, de ott is azt írták nem foglalkoznak vele. Most valami pénzügyi lobbi van amögött, hogy mindenki csak a fizetőset teszteli? Vagy félnek hogy kiderülne az igazság? Arra gondolok amit Rita is írt. Szóval mennyit ér a kereső ha ingyenes?
István! Te nem tudnál csinálni valami tesztet? Belevennéd a Clamavot,Comodo-t, AVG és Avast Free-t.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.14. 16:47:35

@Zvaragabor!
Az AVG szerintem sem rossz, gyujtott mar nehány VB100-at is, van heurisztikaja, stb.
A tűzfalaknál az ingyenes Comodo tavaly egy nagyon alapos tűzfal tesztben elverte a teljes mezőnyt, benne több fizetős progit is.

zvaragabor 2008.02.14. 16:57:26

István:

Hát már egy ideje ott tart szerintem az antivírus piac, hogy heurisztika nélkül bizony nem élet az élet. :)

Igen, a matousec.com teszter cég az, amiről beszéltem, ahol a Comodo(v2.4) állva hagyta a mezőnyt. Tavaly február óta a Comodo-t használom, tavaly november óta már a v3.0-t. Bivaly egy szerkentyű, a hips modulja még ráadásul kapott egy heurisztikát is, érdekes volt látni, ahogy egy kártevő.exe elindításakor riasztott, hogy a heurisztika szerint veszélyes.

Én a matousec féle leak testing mellett szívesen látnék még egy DoS attack tesztet. Cégeknek, akiknek van web szerverük, bizonyára szívesen látnának egy átfogó képet, hiszen számukra a dosolás is egy potenciális veszélyforrás.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.14. 16:58:25

Szia Ragazzo!
Ha megnézed, bármilyen magazin is maximum a személyes benyomásait, ergonómiát, sebességet tud tesztelni. A komoly teszteléshez nem csak géppark, hanem alapos és aprólékosan megtervezett környezet, vírusgyűjtemény, megfelelő szaktudás és RENGETEG MUNKA ÉS IDŐ szükséges. Ezek szerintem maximálisan megvannak az alábbi helyeken:
www.av-comparatives.org/
www.av-test.org/
www.virusbtn.com/vb100/index
checkvir.hu/
Az ilyen teszteken azoknak az eredményeit látjuk, aki résztvesznek. Ha valaki nem indul el ezeken, akkor maximum a magazinok tesztjeiben kaphat "szép pasztell színű a doboza" jó pontot.

senkisee 2008.02.15. 11:39:56

milyen baj tud érni tűzfal nélkül? vagy mit kell nézni a neten, hogy valami baj érjen? :)
mióta XP létezik azóta csak a beépített tűzfal van.
no persze felraknék egyet, ha tudnám miért kell, mitől kell félni.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.15. 13:10:21

Szia Senkisee!
Az XP tűzfalal CSAK a befelé irányuló forgalmat szűri, és ennek hatásosságát is jócskán megkérdőjelezik. Leghelyesebb egy

kétirányú, öntanuló szabályrendszerrel illetve policy-val irányítható tűzfalat használni, ami naplózni is tud. Az úgynevezett Internet security komplett biztonsági csomagokban rendre szerepel már a tűzfal is, próbáld ki pl. az ESET Smart 30 napos csomagját.
És hogy mik történhetnek, abból itt egy kis izelítő:
www.virushirado.hu/oldal.php?aid=273&hid=49&print=1

senkisee 2008.02.16. 10:26:31

kipróbálom, csak nem tudom mire kellene nekem? :)
az elmúlt 7 évben miért nem szedtem össze semmit?
jó a cikk, de engem ezek szerint kihagytak ezek a férgek is, vagy itt vannak és velem élnek a gépemen csak nem tudok róluk :)
de kizártnak tartom

buherator · http://buhera.blog.hu 2008.02.16. 13:08:51

@senkisee

Ne aggódj, ott vannak a kis okosok, csak nem verik nagy dobra a dolgot ;)
Rendszergazdáknál bevált mondás, hogy ha megkérdezik, hányszor törték fel a rednszeredet az utóbbi egy évben, feleld azt hogy egyszer! Ha azt mondod, egyszer sem, akkor nyilvánvalóvá válik, hogy még a betörés tényét is képtelen vagy észlelni.

"kipróbálom, csak nem tudom mire kellene nekem? :)
az elmúlt 7 évben miért nem szedtem össze semmit?"

Tanúlj egy kis valószínűségszámítást, ha igazad lenne, ez akkor sem jelentene semmit.

Vírusstatisztika magyarországi adatokkal

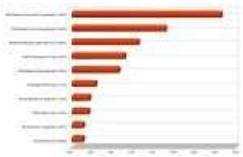
2008.02.15. 12:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: magyar adat nod32 eset vírusstitisztika threatsense

Terveink szerint egy igazi különlegességgel jelentkezünk mostantól, minden hónapban közreadjuk az előző időszak tíz legelterjedtebb kártevőinek listáját. De hiszen ez eddig is így történt, akkor hol itt a különlegesség?

A NOD32 antivírus rendszer gyártója, az ESET havonta elkészíti a legelterjedtebb internetes kórokozók top tízes listáját. A vírusstatisztika alapját a vállalat ThreatSense.Net vírusfigyelő rendszere képezi, amely a NOD32 felhasználók önkéntes adatszolgáltatásának köszönhetően az e-mailekben terjedő vírusok mellett a böngészés közben a számítógépekre került kórokozókat is listázza és mostantól ezt országokra lebontva is le tudjuk kérni, így végre arra is mód nyílik, hogy **a havi toplista teljes egészében a magyarországi észlelésekre alapozva jelenhessen meg**.

A **listán szereplő tételek minden esetben konkrét károkozókat jelölnek**, az eredeti listában található csak gyanítható, de egyértelmű azonosításra nem alkalmas észlelési adatokat nem vettük figyelembe. **Igyekeztünk a legtöbb kártevő mellett feltüntetni a weboldalunkon található részletes vírusleírásra mutató linkeket is**.



Az ESET programjai rendkívül **erős heurisztikai képességekkel rendelkeznek,** ez pedig nem csak hatékonyan ismeri fel az új kártevőket, hanem kevés esetben hibázik, azaz riaszt tévesen nem vírusos állományokra. A Kiterjesztett heurisztikának (Advanced Heuristics) az a feladata, hogy **proaktívan ismerjen fel vadonatúj, addig még ismeretlen kórokozókat**. A ThreatSense adatok között nagyszámban találhatóak olyan kártevők, melyeket éppen a NOD32 proaktív védelme fog meg. Nézzük hát akkor, **milyen hónapot is zártunk januárban Magyarországon**!

1. Win32/Adware.Virtumonde.FP alkalmazás (14.55%)
Ez a kártevő szintén a Kéretlen alkalmazások táborába tartozik az ESET kategorizálása szerint. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában (alapértelmezés szerint C:\ Windows\ System32) véletlenszerűen generált névvel fájl(oka)t hoz létre, melyeknek kiterjesztése .dll. A trójai megkísérel egy távoli szerverhez csatlakozni, és onnan további komponenseket letölteni.

2. Win32/Adware.Virtumonde alkalmazás (9.06%)
A Virtumonde (Vundo) program a Kéretlen alkalmazások (Potentially Unwanted) kategóriába esik, készítői arra használják, hogy segítségével kéretlen reklámokat másoljanak a felhasználó PC-jére.

3. Win32/TrojanDropper.Agent.DGO virus (6.39%)
Harmadik helyen egy trójai alkalmazást találunk, illetve egész pontosan annak már egy sokadik változatát.

4. Win32/Obfuscated.A1 trójai (5.04%)
Az Obfuscated (összezavart kódú) elnevezés egy olyan általános kategória, amellyel számos fájl már proaktívan felismerésre és eltávolításra kerül, amelyek gyanús technikákat használva igyekeznek kibújni az antivírus vizsgálat elől. Az ilyen állományok többsége reklámprogramokkal (Adware) ellátott alkalmazások telepítő csomagjaiból származnak, mint amilyen például a korábban is említett Virtumonde. Futása közben kéretlen reklám ablakokat jelenít meg.

5. Win32/Adware.Ezula alkalmazás (4.48%)
Ez a program egy hagyományos telepítőprogram ikonjával érkezik, de ha a felhasználó rákattint, semmilyen párbeszédablak nem jelenik meg. Ez a szintén a Kéretlen alkalmazások közé tartozó program semmilyen visszajelzést vagy tájékoztatást nem ad a telepítése során, csendesen, elbújva zajlik az installálási folyamat. Ha sikeresen feltelepült, onnantól kezdve további szoftverkomponenseket igyekszik letölteni és lefuttatni az áldozat gépén, a letöltések jelenleg egy Fülöp-Szigeteken található szerverről történnek.
Ezen túlmenően kémkedik a felhasználó szokásai után is, ehhez egy előre definiált listából ellenőrzi és figyeli a begépelt keresőszavakat. Internetezés közben pedig alkalmanként kéretlen reklámokat is megjelenít.

6. Win32/Agent.NOP trojan (2.17%)
A hatodik helyen az Agent-NOP trójait találjuk. A féreg különféle kártékony állományokat helyez el a Windows/System32 mappában, illetve további kódokat is igyekszik letölteni.

7. Win32/CMDOW.143 alkalmazás (1.58%)
A cmdow.exe állományra sok antivírus program nem jelez, hiszen nem vírusról, hanem egy hacker eszközről van szó. A cmdow egy olyan parancssori segédprogram, melynek segítségével Windows NT4/2K/XP/2003 rendszereken kilistázhatjuk, átmozgathatjuk, átméretezhetjük, átnevezhetük, illetve elrejthetjük vagy ismét láthatóvá tehetjük, minimalizálhatjuk vagy kinagyíthatjuk, helyreállíthatjuk, aktiválhatjuk illetve inaktiválhatjuk, továbbá bezárhatjuk, leállíthatjuk az ablakokat. Az eredeti cdow alkalmazás egy 31 KB-os végrehajtható fájl, amely nem ír a Registrybe, nem igényel külön telepítést, elég lefuttatni. Eltávolításához elegendő ezt az állományt törölni.

8. Win32/Jeefo.A virus (1.49%)
Ezt a vírust 2003 nyarán észlelték először. Megtévesztésül egy svchost.exe állományt hoz létre a Windows könyvtárában, míg az eredeti és hasznos svchost.exe alkalmazás a Windows/System32 mappában található. A fertőzés alkalmával elkódolja az állományokat, illetve egyes esetekben a fertőzött fájlban felülír hasznos területeket is, így az működésképtelenné is válhat.

9. Win32/HackAV.G alkalmazás (0.97%)
A HackAV csoportba azok a kártevők tartoznak, melyek a NOD32 hitelesítési eljárásait próbálja meg feltörni, illetve eltéríteni. Ezeket az alkalmazások a NOD32 illegális, jogosulatlan másolatait próbálják működőképes állapotba hozni.

10. Win32/VB.EL féreg (0.96%)
A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adathordozókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is.

Ezek tizen adják az összes észlelés 46.69 százalékát, vagyis a további megközelítőleg 53 százalékon már sok, kisebb arányban előforduló kártevő osztozik.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/339083

Kommentek:

Nincsenek hozzászólások.

A kártevők nyomában

2008.02.18. 12:02 | Csizmazia István [Rambo] | Szólj hozzá!

Az ESET ThreatSense szolgáltatása a felhasználó beleegyezése esetén **folyamatosan adatokat gyűjt arról, hogy mely országokban milyen kártevők jelentek meg**. Az adatok elemzése alapján képet alkothatunk arról, hogy hol és milyen kártevők keserítik meg mindennapi életünket. Nézzük, milyen következtetéseket vonhatunk le, mit olvashatunk ki a számok közül!

A legszembetűnőbb észrevételünk az, hogy világviszonylatban **az első száz kártevő csupán az összes fertőzés 57,5 %-át fedte le**. Ez azt jelenti, hogy nagyon sok, **több ezer kártevő jelenik meg, ami ténylegesen fertőzést is okoz**. Manapság már nem jellemzőek az olyan járványok, melyek a fertőzések nagy részét kitennék.

A kontinensek adatait vizsgálva, mindössze 29,45 % azon fertőzések aránya, melyek minden régióban (kontinensen) megjelentek. Ez azt mutatja, hogy a kontinenseken belül is eltérő a fertőzések összetétele. Az alábbi ábra három kontinens (Észak-Amerika, Európa és Ázsia) adatai alapján mutatja, hogy mely fertőzések jelentek meg a másik régió(k)ban. Az adatok az első 100 kártevőre vonatkoznak, így régiónként 56-61%-ot jelentenek.

Az adatokból kitűnik, hogy **Ázsia esetén mind Európához, mind pedig Észak-Amerikához viszonyítva nagyon kevés az olyan kártevő, ami nem vált világméretűvé**, ugyanakkor mind a két kontinensen elterjedt. **Ázsiában a fertőzések kb. fele egyedi, azaz csak itt fordult elő**, másik fele pedig Európában és Észak-Amerikában is megjelent.

Európa és Észak-Amerika esetén viszont csak a fertőzések negyede-ötöde olyan, ami a másik két kontinens valamelyikén nem jelent nem. Ebből azt szűrhetjük le, hogy **ezen két kontinens esetén a fertőzések sokkal könnyebben terjednek** az egyik kontinensről a másikra.

Magyarország és két szomszédunk (Ausztria és Szlovákia) adatai alapján szintén megállapíthatjuk, hogy az országok esetén is hasonlóan igaz a **kártevők kis része jelenik meg mindegyik országban**. A vizsgált 3 ország esetében kb. a kártevők harmada-negyede. A fertőzések zömét pedig az adott területen terjedő kártevők teszik ki, melyek megmaradnak az országhatáron belül.

A fenti jelenségek oka a jelenleg terjedő kártevők összetételében keresendő. A kártevők **túlnyomó többsége manapság internetezés közben** kerül a számítógépekre, és e-mail üzenetekben is terjed. A felhasználók e-mail/internet használati (böngészési, levelezési, csevegési) szokásai **nagyban befolyásolják a kártevők terjedését**. Magyarországon például nagyrészt hazai oldalakat látogatunk, hazai címzettnek küldünk e-mail üzenetet, itthoni ismerőseinkkel csevegünk, és ennél átlagosan sokkal ritkábban fordul elő, hogy határokon túlra küldünk üzenetet. Ez igaz mind az országok, mind pedig a kontinensek szintjén is.

A cikkben szereplő számértékek az ESET ThreatSense által gyűjtött adatokon alapulnak, melyek természetesen nem lehetnek valamennyi számítógép felhasználóra vonatkozóak, pusztán a felhasználók egy részhalmazát jelentik. A regisztrált jelentések nagy száma azonban mindenképpen a hűen tükrözi a kártevők elterjedtségének az arányait.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/339220

Kommentek:

Nincsenek hozzászólások.

Lehallgatják-e a Skype-ot?

2008.02.19. 16:51 | Csizmazia István [Rambo] | 30 komment

Címkék: skype bundes trojaner wikileak

A stílszerűen szomorkás - és kissé az "Egy óra múlva itt vagyok" Láng Vincéjét idéző válasz az lehetne: és **mit nem hallgatnak le** manapság? **Érdekes dokumentumok** kerültek ki, majd tűntek el, és jelentek meg ismét.

Van egy ősi dakota mondás, miszerint: **ha valami egyszer felkerül az Internetre**, azt onnan leszedni már nem lehetséges. Egy kaliforniai bíróság ugyan letiltotta a Wikileaks oldalt, de az ott közölt információk már különféle tükrök segítségével, sőt **torrent fájlok formájában** is olvashatóak.

Egy korábbi Bundes Trojaner témájú cikkünkhöz **jó illusztráció** lehet ez a Skype lehallgatásáról szóló oldal, ezt jó érzékkel mi is csak linkeljük, és nem tároljuk ;-) Németül tudóknak pedig ajánljuk a Heise.de cikkét.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/345874

Kommentek:

satie • http://321.hu/sas 2008.02.19. 19:03:55

azt nem hallgatják le, amit megbízhatóan titkosítasz, nem ilyen programmal, nem értem, miért kell az embereknek ilyen szarokkal mérgezni magukat és környezetüket

f renc 2008.02.19. 19:30:11

Mármint a skype mérgezi az embert? Nem mérgez jobban, mint maga a számítógép...

grigorij (törölt) 2008.02.19. 20:20:29

Először is éppeszű ember nem megy az iwiw-re, nem szkájpol...
Másodszor, pont tegnap mesélte egy rendőr barátom (nem posztos), hogy addig nincs baj, amíg nem kerülsz a "fényre"...
Onnan viszont...
Jó megoldás az egyéni cryptelés, de ezzel szinte az összes "illetékes" szerv figyelmét magadra irányítod!

Dextro (törölt) 2008.02.19. 21:26:13

Ki tudja ezt követni? Egyszer arról cikkeznek ,hogy a német zsaruk, meg az oroszok durrognak mert ,nem tudják lehallgatni a skype-ot.Hát bakker most akkor most valaki "vetít".

-Oiler- (törölt) · http://varhegyi.myminicity.com/ 2008.02.19. 21:56:36

Aki skyp-on beszél nem lehet sikeres ember.
Mondjuk annak meg lehallgatják a mobilját:)
varhegyi.myminicity.com/tra

pistibacsi · http://henkajpan.blog.hu 2008.02.19. 22:03:31

Hát én szkájpon szoktam beszélni, de aki arra kíváncsi, az nem lehet sikeres ember. Nem irigylem, ha valaki a saját magánélete helyett másokéval foglalkozik.

SPY89 2008.02.19. 22:06:22

Spec mai világban csak egy dolgot mondjon valaki amit nem hackelhet meg valaki valami valamiért?:D Most néztem pont Prison Bréket szóval bennem van egy bizonyos üldözési mánia, de szóval mobilt minden szart lehalgatnak akkor már pont skypot ne.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.19. 22:13:10

További olvasnivaló:
mover.blog.hu/2008/02/13/sokmillio_parazo_orszaga_vagyunk?fullcommentlist

markusbenjamin 2008.02.19. 22:14:05

najó, sztem ez k*vaegyszerű: ha vaj van a fejeden, akkor tényleg nem kell iwiwelni, meg skype-olni, de amúgy mi a haragért ne? tőlem aztán tudhatja a rendőrség, hogy kivel vagyok jóban, le se szarom

TBC 2008.02.19. 22:15:06

Hmm, lehallgatnak Skype-on?... Tegyék csak, ha nekik ez akkora élvezetet jelent. :-D A telefonokat ezerszer könnyebb lehallgatni, gyakorlatilag semmi titkosítás nem védi, mégis fenntartások nélkül használjuk évek óta. Különben sincsenek olyan titkos dolgaim, amik hétpecsétes titkok lennének. Akinek meg mégis, az írja meg emailben, és titkosítsa PGP-vel. :-)
Amúgy meg jó dolog a Skype, még akkor is, ha nem szabványos protokollt használ, illetve ő maga nem szabadszoftver.
Különben meg: egész véletlenül nem azt hangoztatták egész eddig a Skype-ról, hogy titkosítást alkalmaz? Vagy netán valami hátsókapu mégis van benne?...

koimbra · http://filmdroid.blog.hu/ 2008.02.19. 22:18:43

Manapság már mindenbe betekintenek, ha úgy akarják. Legalábbis ez hírlik, hogy ebből mi az igaz.

Ismerősöm ismerősének (stb) mesélte, hogy neki a mobilját kapcsolták be (ugyanis belehet ha úgy akarják), így megtudják merre is jársz, sőt erről mutatott is pár dolgot bizonyításképpen.

TBC 2008.02.19. 22:49:48

A mobilos dologról én is hallottam; és annak tekintetében, hogy kikapcsolt állapotban is működik a kijelző, tud hangot kiadni, stb, nem annyira meglepő. Sőt, valahol azt is olvastam, hogy a letörölt sms-eket is jórészt vissza tudják olvasni.
Igazából én azon lepődnék meg, ha lenne olyan, amit nem tudnak lehallgatni. :-D
De ez nem újkeletű, hisz leveleket is el tudnak olvasni, csak egy megfelelő fényerejű lámpa kell. :-D Ahhoz képest egy titkosított beszélgetés nagyságrendekkel biztonságosabb...

Joaquin 2008.02.19. 23:24:10

Akkor megleplek TBC, a titkosított internetkapcsolatba nem lehetséges beleolvasni. Amikor ezeket kitalálták még nem az internet-felhasználó volt a közellenség...

Lesza 2008.02.19. 23:34:52

Aki skyp-on beszél nem lehet sikeres ember.

Akkor én nagyon nem vagyok sikeres ember, mert mivel nem Magyarországon lakom, így naponta ezt a programot használom, hogy a családommal beszéhessek.

Na és ha lehallgatják, legyen jó nekik, ha őket az érdekli, hogy én Anyukámmal a külsőféle vadas receptekről, meg működöm építésről beszélgetek :)

Perillustris 2008.02.19. 23:39:30

Én úgy előzöm meg a lehallgatást, hogy kihangosítom minden beszélgetésem. A buszon persze furán néznek, de nekem csak az számít, hogy ne tudjanak lehallgatni.

TBC 2008.02.20. 05:09:02

Joaquin: tudom, hogy titkosított kapcsolatot nem lehet lehallgatni, vagy legalábbis a titkosítás miatt nem kevés ideig tartana azt visszafejteni. Csak én konkrétasn valami hátsókapura gondoltam, pont ilyen esetekre, hogy netán jelen esetben a skype mégis vagy "megfeledkezik" a titkosításról, vagy a használt kulcsot elküldi bizonyos szerveknek, ha épp az adott beszélgetést le tudják hallgatni... Persze ez már eléggé összeesküvés-elmélet-szagú teória, de nem lehet 100%-ig kizárni.
Többiek: ez a "aki XY programot használ, az sikeres ember nem lehet" duma nagyon csak óvodás szintre vall. Alaptalan piszkálódás, semmi más, arról meg jobb esetben leszokik az ember alsó tagozatban. Persze, viccnek jó, de egy idő után már unalmas, amikor minden poszt után hárman ezt elsütik... Amúgy meg ha komolyra venném a szót, nem ettől függ valakinek a sikeressége, sőt, pont az nem lesz sikeres, aki csak azért nem használ jelen esetben Skype-ot, mert ő pl. elszánt SIP-használó, és elvből nem hajland Skype-ot használni. Miközben a barátai, ismerősei mind ezt használják, és csak az ő kedvéért nem fognak más szoftverre áttérni.
Visszatérve a lehallgatásra: hallgassák le nyugodtan, amikor épp a múlt heti focimeccsről, vagy a legutóbbi biciklitúrámról beszélek a haverokkal, ki a fenét izgat? Sőt, még azt is hallgassák le, amikor a legutóbbi bulin megesett csajozásról dicsekszünk el egymásnak, ki a fenét érdekel? Egyrészt nem olyan személy hallgatja le, aki bármi kárt tudna okozni azzal az információval, másrészt meg aki nem készül államellenes cselekedetre, aki nem foglalkozik pénzmosással, embercsempészettel, stb, annak nincs félnivalója egy esetleges lehallgatás miatt.

washabi 2008.02.20. 08:02:23

Minden titkosszolgálat él a lehalgatással, csak aztán mire használják az infót az a kérdés. Mondjuk jól jöhet, ha tudja a hatóság, hogy ki szőkíti az olajat. Ott is voltak lehallgatások meg információszerzés. Csak hát aki felhasználhatta volna, mégsem használta.

atleta.hu · http://www.atleta.hu 2008.02.20. 16:02:07

Sracok, to olvastatok a belinkelt doksit, vagy az nagyon zavarna a nyugodt parazgatasban?

Akkor bezavarnek egy kicsit - a kiszivarogtatott doksiban szo nincs arrol, hogy feltortek volna a Skype titkositasat. Sot, azt irjak, hogy ez baromira nem opcio a 256 bites AES es a 2048 bites RSA miatt. Egyszeruen egy kemprogramot telepitenek a lehalgatando szemely gepere, es az tovabbitja az informaciokat. Kar feleslegesen kattogni.

Jo, OK, zart forraskodu szoftverben sosem bizhatsz meg igazan, vagyis ha komoly titkokat szeretnel attolni az interneten, akkor hasznalj valami olyan szoftvert, amit te irtal, irattal, vagy atnezettel az embereddel (esetleg ha csoringer vagy, es nincs ra tobb millad, akkor az open source kozosseggel).

Amugy a kemprogramoktol ez sem ved meg...

TBC: ez a lehallgathato kikapcsolt mobil temat ne szedjuk mar elo sokadszor is. [Rambo] belinkelte a legutobbi vitat rola, ott el lehet olvasni, hogy miert nem valos a felelmetek.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.29. 14:21:03

Egy kis érdekesség: Alkotmányellenes az internet ellenőrzése:
hirek.prim.hu/cikk/66001/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.22. 09:01:40

Ez is elég durván hangzik:
Oroszországban új hivatalt hoztak létre a wifizők monitorozására.
www.infoworld.com/article/08/04/18/Wi-Fi-users-to-be-monitored-in-Russia_1.html?
source=rss&url=http://www.infoworld.com/article/08/04/18/Wi-Fi-users-to-be-monitored-in-Russia_1.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.09. 11:38:42

Itt az új durva fejlemény: eredetileg a rendőrség megfigyelő trójait telepíthet a célszemélyek gépeire, de csak online módszerekkel, távolról. Bajorországban már azt is engedélyezik, hogy a rendőrprogram telepítéséhez titokban behatoljanak a megfigyeltek házába.
www.heise.de/newsticker/Bayerischer-Landtag-setzt-den-Bayerntrojaner-frei--/meldung/110426

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.09. 11:41:09

De ez se piskóta, remélem jól leszavazzák:
itcafe.hu/hir/torvenytelen_lehet_a_firefox_es_a_skype_is.html

Szabad Internet rulez ;-) Kik azok az idióták, akik ilyen tervezeteket találnak ki?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.13. 16:27:34

A svédek is nyomulnak:
itcafe.hu/hir/svedorszag_fra_lehallgatas_tiltakozas.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.18. 21:13:36

Újabb fejlemény, nem az eredeti alkotmánysértés a fő bajuk, hanem a kisziváragtatónál tartanak házkutatást. Értik a dolgukat...
itcafe.hu/hir/bajororszag_kalozpart_skype_lehallgatas.html

pongyolapitypang 2008.09.19. 23:55:53

Nahat! Akkor megiscsak van megoldas arra a kerdesre, hogy hova tunnek azok az sms-ek, amiket kitorlunk??? Evek ota torom a fejem ezen. Persze ebbol is latszik, hogy nem itt a helyem, semmi egyebhez nem tudok hozzaszolni :))

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.01. 12:15:05

Van aki önként jelentkentkezik:
www.sg.hu/cikkek/63034

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.03. 08:55:38

Kínában is naplóznak központilag:
www.fn.hu/tech/20081003/kina_skype_ot_is/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.05. 13:29:52

Azt hiszem, abbahagyom a kommenteket, és legközelebb már csak azt szúrom be érdekes hírnek, ha valahol NEM hallgatják le alapból ;-)
Nah szóval a britek is elfogadták a terrorveszélyre hivatkozva:
itcafe.hu/hir/nagy-britannia_totalis_lehallgatas.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.23. 10:29:17

Az olaszok is készülnek a lehallgatásra.
www.vnunet.com/vnunet/news/2236939/eu-looks-voip-tapping

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.26. 12:35:27

Azért nem lehet majd egy rossz munka ez sem, ülni a kis állami hivatalban és naphosszat MySpace/Facebook forgalmat nézegetni jó pénzért. Gondolom, maltert keverni vagy utat építeni már nem lenne ennyire népszerű...
hirek.prim.hu/cikk/72184/

A Myvip.com tagsága szőrös mellű?

2008.02.20. 15:38 | Csizmazia István [Rambo] | 2 komment

Címkék: spam szőrös myvip mell

Sokféle kéretlen reklámlevél hullott már be a postaládánkba, de ez a mostani igazi unikum. Egyedülálló alkalom kínálkozik, hogy **végleg megszabaduljunk a zavaró mellszőrtől, bolond, aki könnyelműen visszautasítja ;-)**

Ha eddigi életünk sivár volt, mert **grizzly medvére hajazó mellszőrzetünk megkeserítette mindennapjainkat, sőt maszk nélkül mehettünk a búsójárásra**, de ennek vége, itt a megoldás. Abba már bele sem merünk menni, mi legyen **az ajándék testrész**, bár annak a neve a levélküldő felmenőivel kapcsolatosan gyakran szóbakerül az ehhez hasonló spam levelek érkezése során ;-)

Mindenesetre a kép alatti szöveg a legaranyosabb:
"**Ezt a levelet azért kaptad, mert a myvip.com tagja vagy.**" Hát ez világos beszéd, nemde?!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/347264

Kommentek:

W Joe 2008.02.20. 16:41:13

Visszautasíthatatlan ajánlat!

SPY89 2008.02.20. 19:24:44

Hümm elgondolkodtató :D SPAM mert megérdemled :P egyébként meg nagyon idehesítő jelenség mindenféle fajta formájában! :/

Harc a botnetek ellen

2008.02.20. 14:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: microsoft biztonság harc zombi botnet botsniffer

Harcolni sokféleképpen lehet - mondta Obi-Wan Kenobi és ebben egy csöpp okunk sincs kételkedni. Eddig csak azt tudtuk, frissítsük használt programjainkat valamint operációs rendszerünket, és **hogy kell-e vírusirtó, az egy percig nem volt kérdés**.

De meg lehet fogni **a dolgot a másik végéről is**, és pontosan erre tesznek kísérletet a School of Computer Science, College of Computing Georgia Institute of Technology munkatársai. A beszámoló szerint az új csapásirány egy olyan BotSniffer megalkotása lehet, amely **a hálózati forgalom elemzése alapján képes észlelni** a botnet pásztor aktivitását. A végső cél pedig a távvezérelt zombi gépek elszigetelése a parancsokat IRC vagy HTTP alatt kiadó rosszfiúktól. Az elv igéretesen hangzik, a kérdés az, hogy mennyire fog beválni a gyakorlatban.

A felvetés mindenesetre logikus, **olyan mennyiségű elhanyagolt frissítésű és védelem nélkül használt gépmennyiség csüng az interneten**, hogy pusztán ideológiai felvilágosítással nem érhető el érdemi eredemény. Ha sikerül legyőzni, vagy legalább kordába szorítani őket, az csakis egy többfrontos küzdelem eredménye lehet - talán, hiszen a csata a spamek ellen például ha nem is elbukott, mindenesetre nem állunk túl fényesen, és **ez pontosan a botnetek miatt alakult így**.

Drukkolunk a sikerért, valamint reménykedünk, hogy Microsoft mégsem fog majd frissítést végző vírust írni, és **mindent mégsem tanulnak el a vírusíróktól**. De az biztos, tenni kéne már végre valamit a hatalmas káosz ellen...

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/347188

Kommentek:

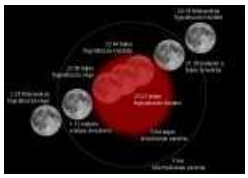
Nincsenek hozzászólások.

Holdfogyatkozás videó - na persze...

2008.02.22. 15:29 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: e mail hold trójai kártevő holdfogyatkozás

Szinte meg is lepődnénk, ha a holdfogyatkozás kimaradt volna a kártevő terjesztők repertoárjából. Az **eseményről készült videófilmet ígértek** a gyanútlan olvasóknak, ám minő meglepetés, mégsem ilyesmit rejtett a levél. Vajon miért van az, hogy ezen meg sem lepődünk?



'Lunar Eclipse Video, Your guide to the total lunar eclipse'
'Shocking video with Total moon eclipse'
'Total Moon Eclipse Video on NASA TV'
'Moon Eclipse is visible today'

És ehhez hasonló tárgysorral érkeztek e-mailek, ám azokban nem videofilm, vagy ezekre mutató link volt, hanem **egy adattolvaj trójai érkezik**. Ez a forgatókönyv sajnos már az unalomig ismert, minden ünnepi eseményt (**Valentin nap, Karácsony, Húsvét, Mikulás**, stb.), minden jelentős világpolitikai eseményt vagy természeti katasztrófát (**Burmai zavargások, Bhutto halála**, stb.) felhasználnak a rosszfiúk, és bizonyára mindig van, aki be is dől nekik.

Továbbra se fogadjunk el édességet idegentől, sőt a levélben ajánlgatott videó linkjére se nagyon kattintsunk - kivéve persze, ha szeretjük az izgalmakat és a kihívásokat ;-) Nemrég valamelyik fórumban láttam az alábbi idézetet, szerintem jópofaság:

"Firefoxot csak a gyávák használnak, az Internet Explorer az igazi férfi böngészője: kaland, veszély, nyitottság." :-D

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/349987

Kommentek:

Nincsenek hozzászólások.

Amikor a nigériai csaló tényleg nigériai...

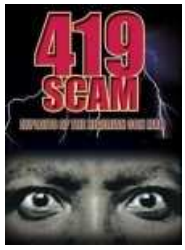
2008.02.25. 11:24 | Csizmazia István [Rambo] | 6 komment

Címkék: csalás nigéria 419

Vannak időnként furcsa események életünkben: néha a fekete 7-es busz megelőzi a piros 7-est, álmodunk valakiről, akivel aztán másnap valóban találkozunk és sorolhatnánk. Persze **az események bekövetkezésének valószínűsége sem egyforma**.

A. eset. Kő leesik és felmelegszik.
B. eset. Kő lehül és felemelkedik.

Ez utóbbi eset a természetben elég ritkán fordul elő ;-) Sokszor adtunk már hírt különféle csalásokról, és a tanulság leszűrési részben bár meg volt említve, hogy **nem érdemes e-mailben ígért örökségünkért** vagy holmi uralkodók vagyonának kimentésének céljából a valóságban is a veszélyekkel teli Nigériába utaznunk, azt többnyire mindig megállapíthattuk, **csak a csalás neve, illetve típusa (419-es) nigériai**, az elkövetők rendre inkább az USA-ból, Kinából és más országokból próbálkoznak a megtévesztéssel.



Volt már egyébként halálos áldozata is az ilyen jellegű esetnek, a félreértés folytán 2003-ban egy 419-es csalás kapcsán egy cseh nyugdíjas végső elkeseredésében igaziból agyonlőtte a nigériai nagykövetség ártatlan – pénze visszaszerzésében egyre csak tehetetlenségét hajtogató – konzulját. A mostani story **érdekessége, hogy a gyanusított valóban Nigériából való**.

Az ausztráliai Perthben fogták el azt a 29 éves férfit, akit nagy értékű, interneten elkövetett csalásokkal valamint pénzmosással vádolnak. Az elkövető **online toborozta az áldozatokat - magát diplomatának kiadva - és váratlan nyereményekről illetve örökségekről szóltak a megtévesztő üzenetei**. Tavaly augusztusban akadt olyan ausztrál károsult is, akit 1.8 millió dollárral könnyítettek meg a csalók.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/353537

Kommentek:

hoster 2008.02.25. 20:15:45

Azért vicc, hogy még mindig akad naiv ember bőven. Régi trükkök új köntösben. Nekem a szomszédomat vették palira egy felújított 419-es csalással, pedig figyelmeztettem.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.25. 21:06:19

Szia Xfaktor!
Egy egész kreatív iparág lett már ez a becsapósdi sajnos :-(

hoster 2008.02.26. 08:32:30

Ahogy mondod! Lehet, hogy az internet használatát, valamiféle vizsga sikeres abszolválása után kéne engedélyezni. :-)

Cseber Lajos 2008.06.06. 00:18:57

Ha tud valaki angolul, akkor jól elszórakozhat ezeken az eseteken:
www.geocities.com/scamjokepage
...amikor akasztják a hóhért...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.24. 17:16:36

Egy jó kis összefoglaló:
techline.hu/it_vilag/20090223_nigerian_scam_419_nigeriai_csalok.aspx?s=rss

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.18. 11:30:28

Ezek tök profik voltak:
www.origo.hu/techbazis/internet/20090318-nigeriai-csalokat-fogtak-spanyolorszagban.html

Az tetszett a legjobban, hogy egy saját "banknak, benne széfnek látszó" irodában fogadták a kuncsaftokat.

Pár hónapja volt egy TV műsorban, hogyan gyűjtik be az angolok a börtönbüntetésre nem bevonulókat. Megkeresik, hol

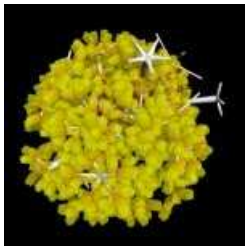
laknak, majd egy ügyvédi papírt küldenek nekik, hogy x csillió fontot örököltek, jöjjenek be az ügyvédi irodába. Az ál ügyvédi irodában végig kamerával figyelik az embert, a yard egy hátsó szobában áll készen, közben precizzen beazonosítják, végigellenőrzik a papírjaikat, és amikor az ember már a pénzt várná a markába, akkor kattan a bilincs a kezén.

Kártevők, ahogy még sosem láttuk őket

2008.02.26. 13:02 | Csizmazia István [Rambo] | Szólj hozzá!

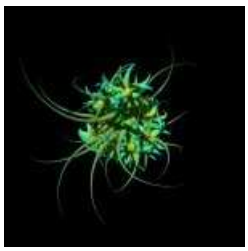
Címkék: vírus kód grafika 3d alex féreg dragulescu

A jó szakembert az jellemzi, hogy **nem szakbarbár, hanem nyitott más területekre, művészetekre is, verset olvas, sportol, moziba és színházba jár, például Einstein szépen hegedült is**. Most mi is kiszakadunk kicsit "az ismét megmutatjuk milyen veszély fenyeget éppen..." (**Ki fertőz ma?**) típusú sablonkalodánkból, és olyasmit mutatunk, ami szép, érdekes, sőt meghökkentő.

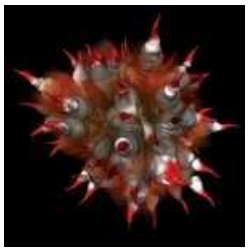


A Message Labs biztonsági cég megbízta **Alex Dragulescut, hogy alkossa még 15 híres vírus, illetve károkozó képzeletbeli háromdimenziós képét**. Dragulescu elismert művész - aki mind a hagyományos technikákban, mind pedig az új médiákban és technikákban gyakorlattal rendelkezik - elkészíttete ezeket a képeket. **Az alkotási folyamatban felhasználta a kártevőkből kapott konkrét kódrészleteket és mintákat is**. Aki Hieronymus Bosch alapján félig állati, de félig sem emberi szörnyeket várt, az talán csalódott, egyes kreatúrák talán még szépnek is nevezhetők (halálosan szépnek a Gizmodo szerint). A korrektség kedvéért meg kell említeni, hogy a cikk legfelső képén nem karfiolt látunk, hanem a művész elképzelése szerint egy IRCBOT-ot ;-)

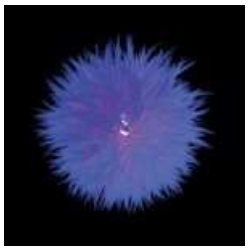
Ízelítőül pár kép, akinek pedig felkeltette az érdeklődését az alkotó, **személyes weblapján még több művet** megtekinthet.



A Win32/Mydoom féreg

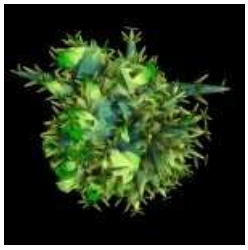


Ilyen lehet a spam közelről



Phishing 3 diemenzióban

Win32/Netsky2 féreg premierplánban



A Vyrutmytob művészi személyigazolvány képe

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/355075

Kommentek:

Nincsenek hozzászólások.

Fortélyos félelem igazgat

2008.02.27. 13:21 | Csizmazia István [Rambo] | Szólj hozzá!

Lassan úgy vélhetjük, hogy aki bagóért kéretlenül ránktukmálja **Rolex karóra hasonmását, Viagra tablettáit, férfiasság növelő piruálit, trójai kémprogramokat és vírusokat küldözget a levélmellékletben**, az egy gáláns grállovag, és a jobb későn mint soha elv alapján akár meg is invitálhatjuk (akarsz a világ egyik leggazdagabb emberénél ebédelni?) egy dupla BigMac-re. Mert ugye mi ez ahhoz a levélhez képest, amiben **bérgyilkosként kifejezetten az életünket fenyegetik**?

Sajnos nem teljesen újdonság, a váltságdíj szedéssel próbálkozó úgynevezett ransomware kártevők elő-előfordultak már korábban is: kezdve egészen az első fecskeként felbukkanó a merevlemezt elkódoló OneHalf-tól egészen **a levelezést eltüntető, és azt csak egy csinos összegért visszaszolgáltató postafiók kalózig** sok mindent láthattunk már.

Elképzelhető, hogy **egy ilyen fenyegető levéltől sokan komolyan megijedjenek**, különösen ha egy kis Google és MySpace nyomozással könnyedén beszerzett személyes információval is megspékelik. Mondjuk **az egyetlen furcsaság számomra** az volt benne, amikor az áldozat e-mail címét is a megbízótól kellett külön elkérni, amikor egy Mitnick típusú valakinek semmiből nem állna a többi adat birtokában azt kinyerni, megszerezni (megtévesztéssel, kukabúvárkodással, közösségi oldalakról, keresőkből, stb.). Reméljük, a magyar változatot sosem lesz szerencsénk egy külön postban itt köszönteni, és megmarad ez a dolog a hanyatló nyugat ópiumának ;-)

S hogy érdekesebb legyen a dolog, **nem csak a virtuális életben növekszik** szédítően a rémisztő események és kártevők száma, a technikai vívmányok mindenkori élharcosa és próbaterepe, a katonai alkalmazások között is van már egy félelmetes alkotás, a harci robot. Egyes adatok szerint mintegy négyezer robotot foglalkoztatnak ma is az iraki háborúban, ami önmagában jó, hiszen a robot régóta hasznosan alkalmazható a tűzszerészeknél is az emberi életek védelmében.

Most viszont a gyors technikai fejlődés azonban elhozta azt a bizonyos mérföldkövet, amikor potom **500 dollárért már bárki megvehet** egy GPS navigációval ellátott robotot, és gyaníthatóan terroristák, és más földalatti csoportok is élénken érdeklődni fognak az új lehetőség iránt. Bármi is jelenik meg ezen a piacon, várhatóan elkészül majd **a negyedáron kapható kínai másolata is**, és Asimov bácsi három robotikai alaptörvényét abszolút figyelmen kívül hagyó, Terminátor korszakot idéző agresszív gépezetek szabadulhatnak rá a világra.

Ennyi sok negatív hír után már igencsak nehéz Domján Laci agykontrollos tanácsai szerint **napról napra egyre jobban és jobban** érezni magunkat...

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/356573

Kommentek:

Nincsenek hozzászólások.

Trójai a kéziszámítógépen

2008.02.28. 14:18 | Csizmazia István [Rambo] | 5 komment

Címkék: csaba biztonság magánélet trójai titkosítás varga kézi számtógép adatlopás guska fsf roadshow

Talán az lenne a meglepetés, ha ezeken az eszközökön nem lenne kártevő, de mégis van. Jóval kevesebben lehetnek, mint az asztali Windowst támadó társaik, de számuk felfutóban, és nem lehet őket a jövőben figyelmen kívül hagyni.

Az aktuális beszámolók szerint a Windows Mobile rendszerre íródott InfoHijack jól végezte a dolgát. A Kínában terjedő károkozó kikapcsolja a Windows CE telepítéssel kapcsolatos biztonsági beállítását, a megfertőzött készülék gyári sorozatszámát, a futó operációs rendszer adatait, és egyéb információkat elküldi a kártevő szerzőjének. Az ilyen manipulált eszközök a későbbiekben **védtelenek maradnak káros kódok letöltésénél**, hiszen a biztonsági figyelmeztetések már nem jelennek meg. Időközben a trójai letöltő weboldalát - vélhetően a nyomozás miatt - **szerencsére már lekapcsolták**.

Itt is meg kell(ene) vizsgálni, **milyen adatokat őrzünk a tenyérgépen**? Használunk-e valamiféle titkosítást bizalmas adataink tárolásánál? Van-e róla mentésünk, és mi történne a napi munkamenetünkkel, ha elveszne? Mi történne, ha nem csak simán elveszne, hanem tartalma kikerülne az internetre, vagy esetleg a konkurenciánál landolna? Sokan éppen ezeknél a feladatoknál lustábbak a kelleténél, és ezzel állandó bizonytalanságnak teszik ki magukat, adataikat.

Számos felhasználó az ilyen kézi eszközökön (de pendrive-on és noteszgépen is) nem csak a kapcsolati tőkéjüket (nevek, címek, Filofax) őrzik, hanem emellett **jelszavaikat, belépési és banki pinkódjaikat is ott tartják**, hiszen praktikusan mindig kéznél vannak. Eddig ez rendjén is van, de csakis akkor, ha ezek valamilyen titkosított formában szerepelnek.

Sajnos én sem lehetettem jelen Varga Csaba Sándor (Guska) FSF Roadshow-beli előadásán, amely **"A magánélet biztosítása szabad szoftverekkel"** címen futott, ahol ez a téma is terítékre került. Szerencsére az előadásokról készült video felvétel, így akit érdekel, még utólag is megnézheti.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/358096

Kommentek:

hoster 2008.02.28. 21:07:31

Az ESET fog fejleszteni biztonsági szoftvert tenyérgépekre?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.28. 22:12:04

Szia!
Konkrét tervről még nem tudok, de előbb-utóbb valamilyen mobilplatfromra lesz szerintem.

virkid 2008.04.01. 15:16:12

Nem tudom a NOD32 esetében hogy müködik, de McAfee esetében ha mobil vírusos fájl kerül egy védet gépre, akkor riaszt...
Nem azt mondom, hogy jobb, csak érdeklődnék a NOD vajon erre fel van e készítve?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.01. 16:34:24

Szia Virkid :-)
Természetesen a NOD32 is ismeri a mobil eszközök kártevőit, tehát ha mondjuk PC-re letöltünk egy ilyet (hogy utána rátöltsük majd a mobil eszközre), akkor riaszt rá a program.
antivirus.blog.hu/media/image/200804/ess_commw.png

antivirus.blog.hu/media/image/200804/ess_duts.png

virkid 2008.04.02. 08:39:09

Köszi a választ...
Ezzel is okosabb lettem... :-)))

Adatait megőrizzük...

2008.02.29. 10:40 | Csizmazia István [Rambo] | 1 komment

Amikor adatvédelemről beszélünk, mindig feltételezzük, hogy minden szereplő a tőle elvárható legnagyobb gondossággal jár el. De mi van, ha ez még sem így történik? Ez esetben vehetünk olyan kormányzati laptopot az E-Bayen, amelyen többmillió állampolgár személyes adatait találták meg.

Sajnos ez nem fikció, nem a képzelet szüleménye, hanem a valóság. **Az angliai esetben egy elrejtett (CD vagy DVD) lemez rejtőzött a billentyűzet alatt**, amelyet javítás során a Boltoni szervizben találtak meg. Pozitívum, hogy állítólag ebben az esetben legalább titkosítva volt az adathordozó. Külön szabályozás rendelkezik az adattitkosítás rendjéről, és arról, hogy a megsemmisítésre váró hardvereszközöknél pontosan milyen **eljárással kellene gondoskodni az adatok megsemmisítéséről**, amihez annyi tartozik, hogy **minden szabály annyit ér, amennyit be is tartanak/tartatna**k belőle.

Úgy tűnik, sorozatos incidensek történnek a szigetországban. Emlékezetes, hogy **tavaly novemberben 25 millió családi pótlékra jogosult adata** tűnt el, miután azt egy felelőtlen alkalmazott egyszerűen csak postára adta az adathordozót, **decemberben 3 millió tanulóvezető adata** tűnt el, de idén januárra is jutott esemény: akkor **600 ezer frissen besorozott királyi tengerészgyalogos adatát** tartalmazó laptopot loptak el.

Magyarországon sem jár élen az ilyen jellegű óvatosságban, egyik régebbi HP szervízes kalandom során, mikor az elromlott és az új darabért cserébe leadandó merevlemez sorsáról igyekeztem információt kapni, az ügyintéző zavarbajött, nem is értette a kérdést, ezért csak a szervízvezetővel lehetett érdemben tárgyalni. A garanciális cserénél azonban mindenképpen ott kellett volna hagyni az elromlott darabot, **aminek sorsáról nem tudtak megnyugtatólag nyilatkozni**. (Talán megpróbálják megjavítani, talán elszállítják valahova, talán el is adják valahova, talán esetleg megsemmisítik valahol egy központban). Mivel az ott nem hagyás plusz sokezer forint plusz javítási díjemelkedést jelentett volna, így azt nem kértem. Tudtommal a fegyveres testületek és az NBH dicséretesen alapos e tekintetben, ott **fúrógéppel átfúrják a leselejtezett merevlemezeket**, és ez így van jól.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/359168

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.09. 16:48:08

Szervizes háttérinfó:
appleblog.blog.hu/2009/03/09/megkeresi_a_hazipornonkat_a_szamitogep_szerelo

Kattintsunk-e tréfás kutyára?

2008.03.03. 10:14 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: letöltés kutya worm garfield storm virustotal kéretlen odie

Méltánytalan lenne, ha a korábbi macskás epizódokat (benne a felejthetetlen Psycho macskával) nem követné a kiegyensúlyozottság jegyében ;-) egy ebekkel kapcsolatos bejegyzés. Persze a dolog oka inkább, hogy némi nemű tacet után **ismét Storm aktivitást lehet érzékelni**, konkrétan a mi postaládában mára virradóra már kettő is várakozott belőle.

Nagyjából persze sejtettük, mi várhat ránk, amikor belenéztünk a levélbe, továbbá az **Itakami és Simpson Hughes nevű ismerősöknek is sajnálatos hiányában szendvedünk** - hiába, az élet kegyetlen, és ezen már talán az idő sem fog segíteni.

Hajrá irány a weboldal, és ami talán apró érdekesség, hogy az erőszakosan **felugró ecard.exe letöltés a NoScript ellenére megjelenik**. Persze a futtatás nem kötelező - népiesen nem erőszak a disznótor - aki pedig ilyet ismeretlenül elfogad, és kattint, az már csak a vírusirtójában bízhat, de erről majd később.

Letöltjük a mellékelt állományt, és veterán antivirus.blog olvasók már szinte felkiáltanak, úgy tudják mi következik: igen, természetesen egy VirusTotal vizsgálattal folytatjuk, hogy lássuk az állomány kiféle, miféle és itt most vége a mondatnak ;-)

A történet innentől már kis híján sablonszerű: a féreg egyértelműen a StormWorm (másnéven Nuwar, vagy Zhelatin) egy újabb darabja, és **szinte minden AV motor szépen felismeri**, ami talán meglepő, hogy az ingyenes Avast és a Panda itt és most a kivételeket erősíti.

Olybá tűnik, szegény rajzfilmhősökre ilyen sanyarú szerepeket osztanak, pedig az Odie-szerű kutyus itt ártatlan. Mindenesetre a **"jaj milyen édi-bédi cuki-muki, kattintsunk rá gyorsan"** effektust használó kártevőterjesztők alighanem jól számoltak, a gyerekek és a gyengébb nem képviselői közül valószínűleg számosan lesznek majd olyanok, akik mégis meg akarják nézni az állítólagos tréfás képeslapot. **Az IP cím időközben már nem is működik**, vagy a szolgáltatók lekapcsolták, vagy ami még valószínűbb: a botnet pásztor intézi úgy, hogy **egy adott cím mindig csak egy rövid időre éljen** a nehezebb felderíthetőség miatt.

Mindenesetre reménykedünk, hogy a felhasználó egy **rendszeresen frissített antivírus és operációs rendszer mögül nézik ezt az egészet**, és akkor a csalódás számukra maximum az lehet, hogy mégsincs ott egy vicces képeslap, és nem pedig az, hogy vicces módon újabb naív rekrutával bővült a botnetes zombi világhadsereg.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/363090

Kommentek:

Nincsenek hozzászólások.

ESET android a CeBIT-en

2008.03.04. 21:07 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: index cebit android nod32 eset

Örömmel konstatáltuk, hogy az Index címlapján a CeBIT kiállítást beharangozó cikkben teljesen véletlenül az ESET androidos képe jelent meg. A NOD32 vírusvédelmi program gyártója egy **gondolkodó androiddal** próbálja a termékeibe beépített, **a proaktív védelemhez szükséges mesterséges intelligencia fontosságára** felhívni a figyelmet.

Szintén a véletlennek köszönhető, hogy a Salzburger Nachrichten is az ESET standról ismert figurát használta a CeBIT-ről szóló írásában.

Az android sem akármilyen, ugyanis azt a magyar Digic Pictures tervezte, amely a magyar származású hollywoodi producer, Andy Vajna **tulajdonában lévő** Cinergi Interactive cégcsoport tagja és számítógép-animációs filmek, trükkök készítésével foglalkozik. A magas szintű, **igényes munkákra specializálódott műhely a Terminator 3 forgatásában** is résztvett.

A CeBIT kiállításon a **NOD32 antivírust és a Smart Security biztonsági programcsomagot** gyártó ESET is természetesen a kiállítók között szerepel, és **mindenkit szerettel várnak** a 6-os épület E16-os standján.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog

- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/365794

Kommentek:

Nincsenek hozzászólások.

Tini Botnet Művek

2008.03.05. 10:37 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: bank fiatal holland account letartóztatás új zéland botnet

Evidencia, hogy napjaink kártevői már semmi mást nem szolgálnak, mint **tisztán és hideg fejjel űzik a profitot**, amit a lopott adatokból, többek közt hitelkártyaszámokból lehet kinyerni. Ha valaki eddig aggódott volna az ifjúság töretlen szellemi fejlődése tekintetében, örömmel jelenthetjük, a jövő nemzedéke szürkeállomány tekintetében abszolút rendben van, sőt: erről meggyőzhet minket a hír is a minap letartóztatott mindössze 18 esztendős profi botnet főnökről.

(A "minden rendben van, sőt" szófordulatról jut eszembe, egyszer még a boldog emlékezetű Szabad Európa Rádióban volt egy adás, amelyben Brezsnyev elvtársat arról faggatták, hogy állnak az emberi jogok a Szovjetúnióban, és azt válaszolta: remekül, van elegendő jog, sőt több is mint kéne :-)
Az újzélandi illetőségű Owen Thorn Walker nem aprózta el, tásaival jelentős kárt okozott az általa működtetett **egy millió zombigépével**, az FBI jelentése szerint az Egyesült Államokban és Hollandiában 20 millió dolláros kárt tudtak okozni az áldozatok számláinak megcsapolásával. A cikk viccesen emlegeti az életkor kapcsán, hogy **a borotválkozáshoz még túl fiatal volt**, de a pénz motiválta szervezett bűnözéshez már nem annyira. Az AKILL becenevű Walkernek **most 10 éves börtönbüntetéssel** kell majd szembenéznie.

A mostani akciót megelőzte az észak-amerikai hackercsapat lefülelése, aminél szintén fiatal elkövetőket - **köztük számos fiatalkorút, sőt több kiskorút is** - tartóztattak le.

Ha valaki rendszeresen **frissíti operációs rendszerét, antivírus programot és kémirtót használ**, már több, mint sokat tett saját biztonsága érdekében. Másrészről megszívlelhetjük az **erős és gyakran változtatott jelszavak kontra lustaság** témakörében megjelenő problémát. Nagyon ajánlatos legalább negyedévenként vagy még sűrűbben változtatni, bár az alkalmazottak szokás szerint mindig is panaszkodnak a túl sok megjegyezni való jelszóra. Ennek ellenére senki nem szeretné egyszer csak viszontlátni hozzáférési adatait egy nyilvános weblapon, amint éppen eladásra kínálják...

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/366352

Kommentek:

Nincsenek hozzászólások.

Felelősség, odafigyelés? Jajj még mit nem...

2008.03.06. 10:03 | Csizmazia István [Rambo] | 1 komment

Címkék: fake hamis godaddy csaló virusirto furko unigray domaintools

Sokan nem hajlandóak megérteni, ahogy **egy pillangó szárnycsapásai egy másik kontinensen pusztító vihart is okozhatnak**, úgy **a leírt szavaknak is súlyuk, jelentőségük van**. Nem akarok most egy olyan szakmával példálózni, ahol a **keddi véleményüket az illetők szerdán már nem tudják vállalni**, de nekünk számítógépeseknek (is) alaposabbnak kell(ene) lennünk.

A Computerworld cikkében megjelentek persze riasztóak, de semmiképpen **nem mondhatjuk, hogy először esik meg ilyesmi** a világtörténelemben. Éppen Csiszér Béla kollégám volt az, aki egy hasonló magyar programot is leleplezett, akkor **az úgynevezett Furkó Antivírus** hirdette magát, és szintén hasonló szimptómákat produkált: tiszta gépen riasztást adott, és bőszen biztatott a termék fizetős változatának mielőbbi megvásárlására. Akkora átverés volt, hogy az adatbázisállománya sem volt igazi, az **a Moorhuhn nevű csirkelövöldözős játék egy átnevezett állományát töltötte le**. Itt a blogon is volt szó **hamis kémprogram irtókról**, többek közt még a nevet is lekoppintotta az a holland cég, amely a kártevőket terjesztő ál Spyware Terminatort forgalmazza.

Sajnos mindenben a **felhígulást és a spórolást** látjuk, **könyvek jelennek meg futószalagon szakmai lektor és nyelvi ellenőrzés nélkül**, de **mi azért mindig igyekezzünk kicsit oknyomozósdit játszani**, nézzünk picit utána, és csak utána csapjunk a billentyűzet közepébe. Biztosan **fárasztó, de megéri** azt a pár percet, amikor az ember utánanéz, létezik-e egyáltalán Alexey Tolstokozhev alávaló spamkirály, akit állítólag galádul meggyilkoltak és rákeres a SpamHaus-ban, vagy megnézi a Domaintoolsban, hogy aki írja ezt, az egyáltalán hihető forrás-e. Ez körülbelül olyan, mintha **lakást vagy kocsit vennénk, és nem kérjük ki a tulajdonlapot**, vagy nem vinnénk el egy szerelőhöz az autót, mert "csak nem csapnánank be éppen minket". De igen, és sajnos iparszerűen. A jobbik eset a médiahack, a rosszabb eset a csalás, és ez utóbbinál van kézzel fogható vesztenivalónk is.

Egy magára valamit is adó letöltő oldal hogyan mondhat olyat egy termékről, vagy másolja át bambán, hogy **"uses cutting edge technology to detect virus and remove them immediately"**? Ki sem próbálták, annyi szent, csak ment az iparszerű tartalom- és linkgyártás, kopi meg a paszta, amelyet egy megfelelően idomított pávián is megtehetne megfelelő mennyiségű banánnal dresszírozva. Ha csak ránézünk a regisztrátorra, a GODADDY.COM Inc. és a **friss 2008 február 20-i dátum már megadja az alaphangot, hogy esetleg egy szó se legyen igaz** a dologból. De a varázsprogram használatát is megelőzhetné egy kis Google keresgélés, hogy ott a mentesítési tanácsokat olvasva esetleg elgondolkozhassunk és észrevehessük, több kárt okoz, mint hasznot... Az Unigray oldalra visszatérve úgy látszik a nagy figyelem miatt időközben már le is kapcsolták. Furmányosabbak próbálkozhatnak a Google cacheben turkálni. És ha nem tetszik amit az UniGray nyújt, hát mehetünk panaszra az ENSz-hez, a Sóhivatalba, vagy esetleg írhatunk az üzemben tartó komoly és elmélyült bizalmat ébresztő rehanashraf1 gmailes pakisztáni e-mail címére.

Az rendben, hogy **a munka frontján harcolunk** (idézet Hofi Gézától), de inkább jelenjen meg az a cikk, hír, blogbejegyzés egy kicsit lassabban, de legyen alapos és később is vállalható a tartalma. Persze értem én, ez a munkásabb, az izzadtságszagúbb út, no meg sok időbe is telik, később kerül bele a hirkereső boxba, de **hiteles információt** szerintem csak így adhatunk. És persze a biztonságunkat **se vadonatúj ismeretlen csodaprogramokra bízzuk**, hiszen vannak itt a vírusvédelmi mezőnyben **erős, teszteken is jól szereplő**, közismert versenyzők

is, akik az ilyen csaló védelmi programok közül **úgy emelkednek ki, mint gladiátor az eunuchuk táborából.**

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/367932

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.27. 10:07:31

Perelik a csaló programok készítőit az USA-ban:
www.virushirado.hu/hirek_tart.php?id=1300&ref=hl

Casino Royale - Frissítve!

2008.03.10. 15:22 | Csizmazia István [Rambo] | 4 komment

Címkék: spam kína reklám adware levél kéretlen casion

Bár spam ügyben eddig mindig bosszankodtunk, az esetek többségében könnyű volt a búzát az ocsútól szétválasztania annak, aki csak magyarul beszél és sírva vígad: **ami e-mail külföldiül jött, az kuka** oszt vége. Ezen a falon ütött rést jó egy évvel ezelőtt a **magyar bankok elleni phishing támadás, ahol már magyar nyelvűek voltak** a megtévesztő levelek, és amelyben PIN kódjaink felől érdeklődtek nagy tisztelettel.

Mostanra úgy tűnik, ~~meg kell barátkozzunk~~ el kell viseljük az ilyen irányú "fejlődést", manapság ugyanis már **egy kínai kaszinóba invitáló levél is jöhet magyarul**, és a különféle bónusz ígéreteket sem méri szűkmarkúan - azt persze nem tudhatják, hogy a magyar emberek jelentős hányada a puszta ígéretekkel szemben már évek óta erősen flegmatikus és rezignált.

Indulunk a kaszinóba, és máris felugrik egy ablak, ami után l**e kíván töltődni a SetupCasino.exe** állomány.

Ha ezt bedobjuk a VirusTotalba, egy szép **adware** akad fent a hálónkon.

Ez persze jobb, mintha rögtön egy vírus vagy kémprogram érkezne, de sok ember a kéretlen reklámprogramokat sem kedveli.

Közben egy másik magyar nyelvű kaszinós levél is érkezett, de a link a vizsgálatkor már nem működött, mindössze az oldal oroszországi

regisztrálójának tudtunk utána nézni. Úgy tűnik, elindult a vadászidény...

- - - - - - Frissítve - - - - - -

Alig került ki a post, mintegy megerősítésként megérkezett egy harmadik fajta kaszinós levél.

Kapjunk 300% bónuszt, 300 EUR-ot, meg ilyesmi.

Ez most épp nem kínai, hanem amerikai szerveren van.

Amit viszont le akar tölteni, az hasonló a fentiekhez: itt is ugyanolyan kéretlen reklámprogram érkezhet a számítógépünkre.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/373927

Kommentek:

zvaragabor 2008.03.10. 16:34:00

Itt egy másik kaszinós oldal:
jeunescasino(pont)com/
Itt a DOWNLOAD NOW-ra kattintva jön csak le az exe fájl. VirusTotal-on eddig mindössze csak az Ikarus ismerte föl benne a kártevőt.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.10. 22:39:17

Szia!
Igen, látom, egyre újabbak és újabbak jönnek :-(

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.12. 07:14:48

Egy kis érdekesség online póker témában:
pokerhirek.hu/?hir=1370&rf=57

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.10. 08:55:52

Egy kis adalék a valódi nyerési/vesztési esélyekről:
www.penzcentrum.hu/cikkszp-1010515-1.html
Aki ennél is mélyebben szeretne belebonyolódni, annak pedig ajánljuk Prékopa András: Valószínűségszámítás című könyvét.

Nem lehet minden program mellé...

2008.03.12. 22:11 | Csizmazia István [Rambo] | 2 komment

Címkék: élet veszély számítógép eszközök hétköznapi threat

... **egy közlekedési rendőrt állítani**, ferdíthetjük el így a Fülig Jimmytől származó magvas tanulságot, és valóban. Ha Windowsunk van, legjobb ha futtatjuk a szentháromságot: vírusírtó, tűzfal, kémprogramirtó. MacIntosh és Linux esetében inkább csak a tűzfal, és rootkit ellenőrző látszik hasonlóan fontosnak - egyelőre. De vajon elég-e ez? Kevéssé meglepő módon úgy véljük, nem. Kell(ene) még emellé Józanész Kapitány és Óvatosságman is :-)

A rossz oldal állandó brainstormingban leledzik, **mintha egy elképesztő mértékű prémiumot tűztek volna ki egy kreatív csapat elé**: jönnek és jönnek elő az egyre furmányosabb és mindig **időszerű ötletekkel**.

Ez lehet olyan Microsoft Excel sebezhetőséget kihasználó levél, amely látszólag a **Pekingi Olimpiával kapcsolatos** részletes információkat ígér, de valójában kártevőt telepít a gépre.

Lehet vicces vagy ünnepi képeslap, amely látszólag ismerősünktől származó jó kívánságokat tolmácsol, de valójában kártevőt telepít a gépre. Újabban a kaszinók világa is képviselteti magát, és online szerencsejátékra buzdít, de ezt sem önzetlenül: **kéretlen reklámprogramot telepít gépünkre**, és akkor még ez egy szerencsés eset ahhoz képest, mint ha valaki egy láthatatlan kémprogramot kap, és a játékostársai ennek segítségével szó szerint kifosztják a valódi pénzben játszó áldozatot, miközben **nevetgélve át-átkapcsolnak a szerencsétlen balek képernyőjére**, ahol annak minden lapját láthatják.

Az állítólagos filmek megtekintéséhez letöltendő kodekcsomag trükk pedig már szinte szakállas, ennél inkább a Mac platformon való előfordulása jelentette az **újdonságot tavaly novemberben**. Aki nem egy tudatos felhasználó, hanem csak bambán kattint mindenre, ami mozog, annak ez is elég lehet egy trójai összeszedéséhez.

Benne van a pakliban az országok közötti hackerek útján vivott csata is, amelyben illegálisan, talán éppen a kormányok fizetnek a hackernek, hogy kémkedjen vagy indítson támadást ellenséges célpontok ellen.

És ami **talán kivédhetetlen, ha egy új program letöltést próbálunk ki**, egy kis gyanakvás, vagy Google keresgélés esetleg segíthet, ha már nem vadonatúj a csalás, de tegyük a kezünket a szívünkre: a paranoiásokat leszámítva ki szokta így intézni a dolgait? Pedig a veszély létezik, erről egy **Gmail mentést végző segédprogram kapcsán lehetett érdekeset olvasni** a HUP-on.

A történet lényege, a mentő program készítője hogy-hogynem minden felhasználói nevet és jelszót elküldött saját magának is, és ez csak teljesen véletlenül, egy hacker (jószándékú ügyes ember) révén derült ki. Egy ilyen ellen nem véd a víruskereső, maximum annak van esélye ezt észrevenni, aki agresszíven logolja a tűzfalat, és minden aktivitást alapból ellenőriz. **Az átlagembernek esélye sincs :-(**

Nem véletlen, hogy a vírusirtók már régen nem csak vírusokat kergetnek, hanem **mindenfajta számítógépes fenyegetettség ellen** védő komplex, integrált biztonsági csomagok felé fejlődik, amit nekünk, humanoidoknak ki kell egészítenünk egészséges gyanakvással és óvatossággal.

S hogy a végén legyen még egy kis borzongás is, a "szép új világban" már tényleg mindenben számítógép van-lesz, legyen az hűtőszekrény, médiacenter vagy mosógép: ezért új megközelítésre lesz szükség. Vagy pénzszerzés okán, vagy szándékos (bosszú vagy öncélú balhé) miatt a **közművek infrastruktúrái**, a gazdagok intelligens lakásaiban található számítógépek, de akár egy pacemaker is célpont lehet...

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/377812

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.24. 16:39:38

Feltörhető az amerikai áramellátó rendszer
index.hu/tech/biztonsag/2009/03/24/feltorheto_az_amerikai_aramellato_rendszer/

Yann Le Pentrec · http://lnk.bz/t7c 2010.04.27. 23:03:08

Avagy vannak olyan dolgok, amiknek nem kéne látszaniuk a külvilág felé. Ez is egy közülük...

A nagy Pa-pa-payPal csali

2008.03.13. 14:28 | Csizmazia István [Rambo] | 12 komment

Címkék: románia paypal bukarest phishing netcraft adathalászat csali

Egy érdekes dologra hívta fel a figyelmünket Subba Sógor - ezúton köszönjük neki, ez pedig nem más, mint egy újabb kísérlet **a PayPal fizetésközvetítő szolgálgatást** használók megkopasztására létrehozott **adathalász oldal**.

A levélből aztán jutott nekünk is, **minimális szövegeltéréssel megkaptuk ugyanazt** a csalárd, adathalászoldalra mutató oldalt. A **Spamatoval ékesített Thunderbird rögtön spamnek** minősítette, ezért már itt a nulladik percben gyanúval fogadtuk azt.

A link elrejtésével nem sokat pepecseltek, egyszerűen egy IP cím mögé másolt PayPalnak látszó;-) bukaresti linket helyeztek el a csali e-mailben.

Időközben annyian riportoltak már a bukaresti phishing weboldalról, hogy **a Netcraft már keresztnevén szólította** és azt javasolta neki, igyanak együtt valami édeset...

Érdekes elem a lap alján található **"VeriSign Identity Protection" logo is, egy kis bizalomébresztési trükk** a gonosz bácsiktól, mielőtt jól ellopják az accountunkat.

A Shazou plugin ezt mutatja az oldal hostjáról.

Amíg üzemel az oldal, **töltsük tele minél több hamis adattal**, hátha előbb-utóbb megér majd egypár törött kezet-lábat, mikor leszállítják a címeket.

Mindegy mit írunk be, érvényes a "Szép lehetsz, de okos nem" kitétel: **minden alkalommal a sajnáljuk... kezdetű ablak bukkan fel**.

Ha vetünk egy fürkész pillantást a **weboldal forráskódjába**, úgy máris nem meglepő, hogy a működésképtelenen az alsó sorban szereplő linkek.

Azon túlmenően, hogy ennél feltűnőbb, egy állatorvosi ló minden betegségével rendelkező adathalász oldalt már nem is lehetett volna csinálni, **biztos lesz, aki ennek ellenére bepötyögi az adatait**.

Addig is **nem butaság** a NetCraft Toolbar használata, ajánljuk mindenkinek jó szívvel.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Safe mód a Mechagodzilla ellen
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/379197

Kommentek:

yanchi 2008.03.13. 15:53:17

Régóta javaslom, hogy az ilyeneket a saját fegyvereikkel kell legyőzni: értékes adatnak látszó szeméttel megtömni az oldalt.

Brute 2008.03.13. 15:54:30

Már nem azért de jó láttam, hogy ipcím van a linkben nem?
Ez már elég levágós.

Körticsek · http://muranomanufaktura.blog.hu 2008.03.13. 16:25:20

Elküldtétek a paypalnak? Meg szokták köszönni.

movhu 2008.03.13. 16:26:22

Tudom sokkal ártatlanabb, de a kedvencem:

mover.blog.hu/2008/03/12/kutyaszar_fullversion

A fullreleases, ami bármilyen programhoz vagy filmhez ad neked azonnal linket, ha elég naiv vagy :)
Egyébként sokan benyelik az ilyet. A fenti írásomban is megemlített szlovák OTP-t is érintő trójait rengetegen beszedték, nem győzte a bank letiltani a grid kártyákat, amiken az egyedi azonosítók voltak, mert a usererek szépen begépelték az eredetileg egy megadandó szám helyett a kártya 10 mezőjét egyszerre a proginak. Igaz, ott a windosba épült a program, látszólag minden az OTP oldalán ment.

Bangkok Charlie · http://thai.blog.hu 2008.03.13. 16:43:11

Hát a post hatására gyorsan fel is dobtam a Netcraft toolbart, ennek az eredménye, hogy ezt a kommentet már Explorerből kell írnom. A Firefox azóta nem hajlandó belépni a blog.hu - inda azonosítóval.

DobayAdam · http://www.mitologia.hu 2008.03.13. 17:32:23

Én még nem hallottam a Netcraftról, de a képek alapján jó és profi, úgyhogy nekem ez nagyon hasznos cikk volt annak ellenére hogy mindig minden linket megnézek hogy hova is visz. (Az meg pláne hogy ilyet régen csak az Aliasban lehetett megcsinálni hogy megmutatja nekem a térképen hogy hol a szerver.)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.13. 18:04:02

@Yanchi:
Jaja, jó ötlet, én is egy fórumban láttam ezt a tippet korábban...

@Brute:
Hát igen IP cím lólába kilóg, semmi https, nem működő linkek, ennél több kellene egy ilyenhez.

@Körticsek:
Nem küldtem, de gondolom a NetCraftos fiúk szólnak nekik...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.13. 18:04:46

@Movhu
Hehe, ezt én is kiszúrtam már korábban:
antivirus.blog.hu/2007/11/09/balekvadaszat

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.13. 18:07:04

@Bangkok Charlie:
Szerintem a Toolbar nem okozhatna gondot, felül lehet bírálni a javaslatait. Próbáld meg, hogy az Eszközök - Kiegészítőknél kikapcsolod ideiglenesen. Még sosem hallottam egyébként olyat, hogy bajt okozott volna :-O

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.13. 18:08:57

@DobayAdam:
Szia :-)
Orulok, ha hasznonak találtad. Nagyon sok hasznos plugin létezik, pl. a ShowIP is egy ilyen jó kis okosság.

Bangkok Charlie · http://thai.blog.hu 2008.03.13. 20:46:59

Hmm, pedig sajnos úgy tűnik a toolbar volt a bűnös. Kikapcsoltam, FF újraindítás - és most már be tudtam lépni az Inda passommal.

FF: Mozilla/5.0 (Windows; U; Windows NT 5.1; hu; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12

Subba Sógor 2008.03.26. 12:09:19

jó a post! :)
nekem is tartogatott újdonságokat

És akkor a karakterek leestek...

2008.03.15. 22:01 | Csizmazia István [Rambo] | 4 komment

Címkék: mac joke virus newton intosh buherator pontscho harmless

... a képernyő alsó sorába. Mintha a híres Cascade (vagy Potyogós) vírus kelne új életre főnix madárként.

Szerencsére nem erről van szó. **Buherátor kollégának köszönjük** a linket, amely egy ártalmatlan, de módfelett érdekes **MacIntosh gépeken futó, úgynevezett Newton vírust** mutat.

Az inkább vicces programnál a fő kérdés inkább az, **honnan tudja a számítógép, illetve a monitor, hogy mikor tartják éppen ferdén?** Lehet, hogy esetleg csak trükk az egész? Emlékszem régen volt a traktorokban egy V alakú cső, benne higannyal, és ez figyelte, hogy a traktor ne dőljön be veszélyesen, illetve ne boruljon fel. Gondolom, ez nem alapfelszereltség az Apple gépeiben, de akkor ezt itt hogy ;-) Aki tud erre vonatkozóan érdemi részletekkel szolgálni, dobjon **egy kommentet**. Talán Pontscho is erre téved egyszer, akkor pedig üdv neki :-)

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/382548

Kommentek:

Én arra gyanakszom, hogy a merevlemezeknél szokott lenni egy rázkódásérzékelő, ami túlzott igénybevételnél olyan helyzetbe állítja a vinyót, hogy az író/olvasó fej ne tegyen kárt a lemezben. El tudom képzelni, hogy ezt az egységet kérdezgeti a program a dőlésről. Ha ciszont kamu a viedo, akkor elég jól van kivitelezve!

Subba Sógor 2008.03.26. 12:06:02

hogy mennyiben inkább trükk a videó azt nem tudom, de azt biztos, hogy a jobb mac laptopokban van mozgásérzékelő. kb. olyan mint ami a Wii kontrollerekben is van. mutatott pl. egy starwars fénykardozós effektet. a gép mozgatásával lehetett a fénykard hangját utánozni, tisztára mintha kezedben lenne a fénykard. már persze ha létezne fénykard ;)

Subba Sógor 2008.03.26. 12:07:16

kimaradt, hogy a kollégám, mert neki van ilyen laptopja.
de majd letöltetem vele ezt a "vírust" és kipróbáljuk :)

titan 2010.04.27. 14:19:23

Wiiccesen néz ki :) Egyébként én is láttam már oylan gépet, ami tudta figyelni a dőlését (bár korlátoottan)
És buherátornak is igaza lehet.

Vírusstatisztika magyarországi adatokkal

2008.03.17. 08:00 | Csizmazia István [Rambo] | 2 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

A NOD32 antivírus rendszer gyártója, az ESET havonta elkészíti a legelterjedtebb **internetes kórokozók top tízes** listáját. Nézzük akkor, milyen hónapot is zártunk **februárban Magyarországon**! Következzen a **NOD32 antivírus rendszert gyártó ESET ThreatSense.NET Center** felmérése.

A vírusstatisztika alapját a vállalat ThreatSense.Net vírusfigyelő rendszere képezi, amely a NOD32 felhasználók önkéntes adatszolgáltatásának köszönhetően az e-mailekben terjedő vírusok mellett a böngészés közben a számítógépekre került kórokozókat is listázza és mostantól ezt országokra lebontva is le tudjuk kérni, így végre arra is mód nyílik, hogy a havi toplista teljes egészében a magyarországi észlelésekre alapozva jelenhessen meg.

A listán szereplő tételek **minden esetben konkrét károkozókat jelölnek**, az eredeti listában található csak gyanítható, de egyértelmű azonosításra nem alkalmas észlelési adatokat nem vettük figyelembe. **Igyekeztünk a legtöbb kártevő mellett feltüntetni** a weboldalunkon található részletes vírusleírásra mutató linkeket is.

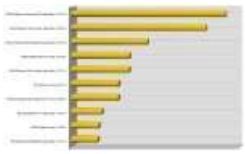
1. Win32/Adware.Virtumonde.FP application (7.34%)
Ez a kártevő a Kéretlen alkalmazások táborába tartozik az ESET kategorizálása szerint. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában (alapértelmezés szerint C:\ Windows\ System32) véletlenszerűen generált névvel fájl(oka)t hoz létre, melyeknek kiterjesztése .dll. A trójai megkísérel egy távoli szerverhez csatlakozni, és onnan további komponenseket letölteni.

2. Win32/Adware.Virtumonde application (6.39%)
A Virtumonde (Vundo) program a Kéretlen alkalmazások (Potentially Unwanted) kategóriába esik, készítői arra használják, hogy segítségével kéretlen reklámokat másoljanak a felhasználó PC-jére.

3. Win32/Toolbar.MyWebSearch application (3.59%)
Az Internet Explorer és Firefox alatt működő keresőszolgáltatás. Telepítésekor számtalan Registry kulcsot módosít, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kliens kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

4. Win32/Obfuscated.A1 trojan (2.73%)
Az Obfuscated (összezavart kódú) elnevezés egy olyan általános kategória, amellyel számos fájl már proaktívan felismerésre és eltávolításra kerül, amelyek gyanús technikákat használva igyekeznek kibújni az antivírus vizsgálat elől. Az ilyen állományok többsége reklámprogramokkal (Adware) ellátott alkalmazások telepítő csomagjaiból származnak, mint amilyen például a korábban is említett Virtumonde. Futása közben kéretlen reklám ablakokat jelenít meg.

5. Win32/Adware.SecToolbar application (2.71%)
Kéretlenül különféle állományokat tölt le a gépre, és ezek automatikus indításáról Registry bejegyzéssekkel gondoskodik. Igyekszik kapcsolatba lépni további weboldalakkal is, ahonnan további kártékony komponenseket tölt le és egy Install AVSystemCare alkalmazást is feltelepít a fertőzött gépre.



6. INF/Autorun virus (2.21%)
Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

7. Win32/TrojanDropper.Agent.DGO virus (2.20%)
Hetedik helyen egy trójai alkalmazást találunk, illetve egész pontosan annak már egy sokadik változatát. Ez a trójai fertőzéskor különféle kártékony állományokat hoz létre a Windows/System32 mappában, emellett Registry kulcsok létrehozásával gondoskodik arról, hogy a számítógép újraindítása után is automatikusan lefuthasson.

8. Win32/CMDOW.143 application (1.42%)
A cmdow.exe állományra sok antivírus program nem jelez, hiszen nem vírusról, hanem egy hacker eszközről van szó. A cmdow egy oly parancssori segédprogram, melynek segítségével Windows NT4/2K/XP/2003 rendszereken kilistázhatjuk, átmozgathatjuk, átméretezhet átnevezhetük, illetve elrejthetjük vagy ismét láthatóvá tehetjük, minimalizálhatjuk vagy kinagyíthatjuk, helyreállíthatjuk, aktiválhatjuk ill inaktiválhatjuk, továbbá bezárhatjuk, leállíthatjuk az ablakokat. Az eredeti cmdow alkalmazás egy 31 KB-os végrehajtható fájl, amely n ír a Registrybe, nem igényel külön telepítést, elég lefuttatni. Eltávolításához elegendő ezt az állományt törölni.

9. Win32/Jeefo.A virus (1.26%)
Ezt a vírust 2003 nyarán észlelték először. Megtévesztésül egy svchost.exe állományt hoz létre a Windows könyvtárában, míg az eredeti és hasznos svchost.exe alkalmazás a Windows/System32 mappában található. A fertőzés alkalmával elkódolja az állományokat, illetve egyes esetekben a fertőzött fájlban felülír hasznos területeket is, így az működésképtelenné is válhat.

10. Win32/Adware.PlayMP3Z application (1.21%)
Ez az alkalmazás a kéretlen és felesleges alkalmazások körébe tartozik. Kéretlenül reklámokat jelenít meg, MP3 tartalmakat és lejátszóprogram komponenseket tölt le. Automatikusan nem képes terjedni, ehhez szüksége van felhasználó közreműködésre is. Az elemzése alapján feltételezhetően Kínából származik.

Ezek tizen adják az összes észlelés 31.06 százalékát, vagyis a további megközelítőleg 69 százalékon már sok, kisebb arányban előforduló kártevő osztozik.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/381037

Kommentek:

Vidi Rita · http://www.hosnok.hu 2008.03.18. 19:29:03

ez a Jeefo micsoda egy kitartó kis mocsok:)

azt szeretném kérdezni, hogy a nod32.hu főoldal miért nem elérhető?

a vírusokról a linkek pedig igen.. mást nem próbáltam..

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.19. 08:12:46

Csak valami átmeneti zavar lehetett az Erőben :-)

Sebezhetőség a VLC-ben

2008.03.19. 09:20 | Csizmazia István [Rambo] | 6 komment

Címkék: kód felirat vlc sebezhetőség puffer videolan sérülékenység injcet túlcsordulás

Sokunknak egyik **kedvenc alkalmazása** a VideoLAN VLC player. Windows alatt egy **ingyenes DVD lejátszónak** örülhetünk neki (többek közt), míg Linux alatt a gyári DVD fájlok lejátszásánál jelentkező jogvédett kodek letöltési problémákat kerülhetjük meg vele sikeresen és **kapunk egy "mindenevő" univerzális médialejátszót**.

A Heise cikke adja hírül, hogy bár a 0.86e új verzió több korábbi hibára is megoldást nyújt, most a feliratfájlokkal kapcsolatban mégis találtak egy újabbat. A probléma gyökere **a feliratfájlok kezelésében rejlik**, mivel a VLC alapértelmezésben mindig megpróbálja betölteni az AVI nevével megegyező SSA felirat állományt. Ha ez **egy preparált, rosszindulatú kódot rejtő fájl, úgy puffertúlcsordulási hibát lehet okozni vele** és ezzel kártékony kód lefuttatására nyílik lehetőség.

Érdemes megjegyezni, hogy a számítógépes f**ertőzések jelentős részét különféle exploitokon keresztül** valósítják meg. Az exploit egy olyan kód, amelyet alkalmazva a támadók ki tudják használni bizonyos programozási hibával rendelkező programok sebezhetőségét. A **jó eset, ha a frissítés már hozzáférhető**, ekkor elegendő letölteni és futtatni azt, **a rosszabb eset, hogy vadonatúj hibáról van szó**, akkor a várkozás és az óvatosság kap nagyobb fontosságot.

A hiba javításáig **ajánlatos óvatosan kezelni a feliratfájlokat**, ismeretlen vagy megbízhatatlan forrásból származó feliratállományok esetén ellenőrizzük annak tartalmát, illetve inkább nevezzük át kézzel, hogy elkerüljük az automatikus betöltődést. Ez annál is inkább javasolt, mivel a sérülékenység kihasználására alkalmas kód máris elérhető az interneten.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/387262

Kommentek:

Vidi Rita · http://www.hosnok.hu 2008.03.19. 10:15:36

"ismeretlen vagy megbízhatatlan forrásból származó feliratállományok esetén"
Miért van olyan, hogy ismerős és megbízható forrás, feliratállományok esetén?

Van ezek mögött cég, vagy legalább egy lekövethető emberke, korrekt és valódi névvel, címmel, lekövethetőséggel?
Általában csak nicknév és egy free e-mail cím.

Úgyhogy MIND gyanús és veszélyes, punktum:)

Vidi Rita · http://www.hosnok.hu 2008.03.19. 10:16:20

pardon a szóismétlésért:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.19. 11:01:07

Azért ne feledjük: valóban _van_ megbízható feliratfájl is: például amit én magam készítettem :-)
Persze azért volt egy kis fricska is a megfogalmazásban, a Microsoft szokta mindig mondani: "és a Word sérülés miatt a javítás megérkeztéig (ajaj) csak MEGBÍZHATÓ forrásból származó dokumentumokat nyissunk meg, pamparam...". Mintha egy munkahelyen létezne egyáltalán ilyen kategória ;-)

Vidi Rita · http://www.hosnok.hu 2008.03.19. 17:38:17

hehe, ez jó! munkahelyi dokumentumok (bár az enyém most teljesen biztonságos, mivel egyedül gyártok dokumentumokat, azt is openoffice-szal:D) az egy külön álltafajta. Szerintem nem lenne hülyeség külön specializálódni rá;))

az is megbízható, amit én készítek (feliratfájl), mert olyan nincs is:))

amondó (törölt) 2008.03.20. 20:30:54

Az opensubtitles.org-ról leszedett .srt feliratok egyszerű szövegek. Elég vel/notepaddal belenézni, hogy tényleg filmszöveg-e és máris látható, hogy okés. Nem?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.29. 12:55:33

Ez is egy érdekes weboldal, tesztelhetjük biztonsággal kapcsolatos tudásunkat a programozói oldalról, milyen hibákat ne kövessünk el a puffertúlcsorduláshoz, etc:
msdn.microsoft.com/en-us/magazine/cc982154.aspx

Akit pedig mélyebben is érdekel a dolog, azoknak Andrew König: C csapdák és buktatók című könyvet ajánlom.

Kémprogramot vegyenek!

2008.03.20. 12:39 | Csizmazia István [Rambo] | 3 komment

Címkék: captcha spyware botnet iframe exploit kémprogram

Avagy telepítsünk készpénzt! Nem mindennapi üzleti érzékről tanúskodik az a vállalkozás, amely saját weboldalán hirdeti furcsa szolgáltatásait. **Pénzt kínál azoknak, akik az Iframe-be ágyazható kémprogramjukat hajlandó** a weboldalukra feltenni.

A ChannelRegister cikk számol be arról, hogy egy weboldal teljesen nyíltan kínálja fel ilyenirányú szolgáltatásait. Az InstallsCash.org oldallal szerződők elhelyezik weboldalukon a kapott, IFrame-be ágyazott kódot, és **az oldal üzemeltetői pedig fizetnek nekik a megfertőzött gépekért**.

Komplett tarifatáblázat mutatja, **melyik országbeli címek mennyit** kóstálnak. A jelenlegi árfolyam szerint **1000 ausztrál telepített kód száz dollárt** ért, ugyanennyi cím az USA-ban viszont már csak 50-et.

Ugyanez Franciországban vagy Németországban 25 dollárt ér, érdekes módon az olaszoknál 60-at, ám **az ázsiai címek mélyen leszállított összegen szerepelnek**: itt már csak 3 dollárt kereshetnek az ügyfelek.

Úgy tűnik, a dolog egy jól jövedelmező iparággá nőtte ki magát, az ügyfelek még valósidejű statisztikát és supportot is kapnak. Az eset sajnos egyáltalán nem egyedi, az iframedollars.biz ugyancsak orosz oldal hasonló szolgáltatásokat kínál.

S végezetül, hogy érdekes (bár inkább hajmeresztő) kezdeményezések és weblapok még ezenkívül is tucatszám lehetnek, arra csak egy példa: a VírusHíradó cikkében arról ír, hogy bérrabszolgákat toboznak az interneten a botnet pásztorok a Captcha törésre, és **darabszámra, teljesítménybérbe fizetnek nekik**.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/388993

Kommentek:

dupi 2008.03.20. 14:30:43

és a különböző árak szted miért vannak? a fertőzöttségi ráta vagy a felhasználói "színvonal" miatt?

Csizmazia István [Rambo] • http://antivirus.blog.hu 2008.03.20. 14:59:04

Szia Dupi!
Semmi biztosat nem tudok. Talán azzal lehet összefüggésben, milyen értékű adatot lehet így szerezni, mennyi hitelkártya és értékes info van közte, milyen könnyen és átlagosan milyen összeget lehet így egy adott országban ezzel megkaparintani, sőt akár a törvényi szigor és a hatékony bűnüldözés színvonala is szerepet játszhat benne.

dupi 2008.03.20. 18:21:38

na a hasznot kihagytam :), bár így második bikkre az UK/NL 60/25 érdekes, a hollandok nem kifejezetten csórik a britekhez képest sztem, átlagosan persze. mióta láttam a híredet, azóta gondolkodok rajta - és lehet, hogy nincs is benne logika nagyon :)

amúgy köszi a blogod, jó!

Az ön e-mailcíme nyert...

2008.03.25. 11:41 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam fake scam lottó csalás nyeremény identity phishing theft e mailcím

Így köszönt minket az az e-mail, amelyben megtudhatjuk, **nyertünk**. Ha így áll a dolog, az ember nem dobja ki a talált pénzt, hanem megpróbálhat örülni neki. **Gratulálnak nekünk**, és hogy meddig lehetünk boldogok, letörlik-e a mosolyt az orcánkról, az kiderül majd a továbbiakban.

Most éppen nem arról van szó, hogy nyertünk egy külföldi országban a lottón, pedig szelvényt sem vettünk - mert azért aki már ezt is elhiszi, annak részvételünk. Nem, finomítottak a részleteken, **az e-mail címünket húzták ki a sorsoláson**, ahhoz pedig nem kell szelvény, ki van ez találva kérem szépen. Tisztára, mint a vizum lottó. Talán még vicces is a "Security File Number" mezőjével :-)

Ha pusztán technikai szemszögből, és roppant gyanakvóan vizsgáljuk a levelet, akkor **örülhetünk, mert fertőzött melléklete nincs, sőt még gyanús weboldalra mutató linket sem tartalmaz**. Emiatt nem riaszt hát a víruskeresőnk és maradhatnak némák kedvenc webes tanácsadóink: NetCraft, Finjan, Phishtank és a többiek. Az ilyen helyzetekben a józan eszünknek kellene megvédenie minket.

Lássuk mit kell tenni a 700 ezer EUR összegért cserébe készpénzben - nagyjából 180 millió jó magyar forint - ezzel már kicsit túllőttek a célon a fiúk - sajnos ez már annyira hihetlennek hangzik, hogy itt már azonnal kipukkadnak az esetleges ábrándfelhők. Az orosz mondás szerint ingyen sajt csak az egérfogóban létezik.

> You are required to claim your winnings by 31th March 2008 otherwise it rolls over to the next draw.
>
> N.B: Procedures to claiming your prize:
> 1. Please quote your Reference number in all correspondence with the claims officer.
> 2. Indicate your Full Name, Address, Country, Telephone, Mobile, Fax Number, Occupation and Age.

Először is sürgetnek minket: 31-ig válaszoljunk, vagy visszaforgatják a pénzt. A sürgetés és/vagy fenyegetés ténye is igen jellemző a csalásoknál.

Aztán **adjuk meg: teljes nevünket, címünket az országgal együtt, vezetékes-, mobiltelefon- és faxszámunkat, foglalkozásunkat és életkorunkat**. Nem kevés bizalmas adatok kérnek így hirtelen, semmi udvarlás, semmi előjáték. Mindazonáltal komoly fegyverténynek könyvelhetjük el, hogy **cipőméretünket és a kutya oltási bizonyítvány számát nem is kérték** el.

Hogy mint az állatorvosi lónál, minden jellemző egyszerre szerepeljen a csaló levélben, a hemzsegő elírások, helyesírási hibák is figyelmeztető jelek lehetnek. **Válaszolni felesleges, személyes adatainkat ismeretleneknek "puszira" kiszolgáltatni bűn** lenne, már csak a szimbólikus **Delete gombra való spontán rákönyöklés** maradt hátra a processzusból, és hátradőlhetünk a székben. Ha nagyon kíváncsiak vagyunk, rákereshetünk az interneten, mennyire ismert az aktuális csalás. Ezzel a mostanival sem mi találkoztunk először.

Aminek ezek után örülni lehet, az már "csak" a szép tavaszi napsütés, na és persze a kellemes érzés: **adataink ezúttal** biztonságban nálunk maradtak.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/395708

Kommentek:

Nincsenek hozzászólások.

Itt a magyar verzió

2008.03.26. 16:23 | Csizmazia István [Rambo] | 16 komment

Címkék: magyar verzió 3.0 nod32 eset ess

Megérkezett végre a magyar ESET Smart Security és a NOD32 3.0 magyar változata.

Az új NOD32 3.0 verzió **jó pár újdonságot nyújt**, többek közt teljesen új, optimalizált program architektúrája, melynek köszönhetően **még kevésbé terheli le a számítógépeket**. Ezenkívül a vírusvédelmi rendszer **intelligens módon, felhasználói beavatkozás nélkül megtisztítja** a legtöbb fertőzött fájlt, és csak azokban az esetekben kéri a felhasználó beavatkozását, amikor az automatikus tisztítás nem lehetséges. Többek közt **bővült a támogatott levelező programok sora is** az Outlook Express és a Windows Mail rendszerekkel.

A komplett biztonsági csomag, **az ESET Smart Security is elérhető immár magyar nyelven**. Aki korábban az angolt használta, most váltani tud. A magyar nyelvű telepítési útmutatók és a telepítő csomagok megtalálhatóak a magyarországi weboldalon.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/397752

Kommentek:

zvaragabor 2008.03.26. 17:28:27

"intelligens módon, felhasználói beavatkozás nélkül megtisztítja"

Igen, amikor próbáltam, nekem is feltűnt ez az új feature. De azt még nem sikerült tisztáznom, hogy a (kiterjesztett) heurisztika által megjelölt fájlokkal mit kezd. Megpróbálja megtisztítani előbb, vagy a fájl kétességéből eredően eleve a felhasználóra bízza a döntés jogát.

narancsos (törölt) 2008.03.26. 18:41:12

Üdv, István!

Az utóbbi időben találkoztam 2 darab vírussal, amit a NOD32 nem ismert fel, de nagyrészt a többi neves gyártó vírusírtója sem. Viszont pár (számomra egy-kettő ismeretlen vírusírtó) felismerte.
Linkelem a Virustotal analízist:
www.virustotal.com/hu/analisis/90036a02f3a236234163848d8885e73b
www.virustotal.com/hu/analisis/378871187c1b9693d00a01dc589d90fb

narancsos (törölt) 2008.03.26. 18:45:54

Ui.: Elfelejtettem leírni, hogy tesóm gép fertőződött meg vele, mivel megnyitotta sajnos a fájlokat, és MSN-en kapta őket. Vírusírtás manuálisan történt, mivel NOD32 nem fogta meg és rendszerfolyamatként indult, ha jól emlékszem. A vírus, mint fájl, megvan, ha gondolod átküldhetem, hogy megvizsgáld.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.26. 19:56:23

Szia Narancsos :-)
Igen, érdekelne a két állomány, légyszíves küldd el, megnézném őket közelebbről. Ezen a weboldalon alul találsz hozzám e-mailcímet:
commodore64.hu/

narancsos (törölt) 2008.03.26. 20:31:53

Valami hibával tért vissza, ezért nem tudta, elvileg elküldeni. :S
else email address?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.26. 20:39:32

Adok egy másikat akkor:
lvoutgnz@no-spam.hu

narancsos (törölt) 2008.03.26. 20:48:11

Én vagyok szerencsétlen ? :S
Mindig Illegal Attachment -el tér vissza.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.26. 20:57:09

Jelszóval össze kéne tömöríteni ezt a két állományt kikapcsolt vírusirto mellett, aztan ugy kuldd el nekem ezt a zipet vagy rart es ird meg hozza a jelszot, pl. lehetne az hogy "infected". Így nem akad fenn a szűrésen.

narancsos (törölt) 2008.03.26. 21:01:45

rendben, megpróbálom.

narancsos (törölt) 2008.03.26. 21:06:53

elment a mail elvileg.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.26. 21:19:07

megjött a mail gyakorlatilag :-)

narancsos (törölt) 2008.03.26. 21:22:51

akkor minden rendben.
várom a reply-t amit lehet tudni rolla, avagy egy jó kis bejegyzést a blogban. :-)

smuzli 2008.05.16. 20:56:19

Halihó!Sajna amai nap szépen leszerepelt nálam az ESS.2 trojait és két spyt nem vett észre ráadásul mindegyik a program files mappában volt.Azaz én telepitettem fel őket vmi progival.A nodom fullra van állitva,minden a legmagasabb szintre van huzva.Hiába találta meg a két spyt,a 2trojait csak más virusirtó progival sikerült eltüntetnem.Szoltam pár ismnek akik szintén a nodot használják és meglepő eredményre jutottunk:az 1iknél 8virus,a másiknál 2virus.1 trojai.Meg mondom öszintén én eddig mindenkinek a nodot ajánlottam sőt miota itt a fullos nod azota azt és nem a sima virusirtot.De most elbizonytalanodtam...A régi sima nod ilyen hibákat nem vétett,többször teszteltem különbözö virusirtok felrakásával és nem volt semmi gond.A spy nevét meg tudom irni hátha vmit segit:Adware.win32.kitsune.b

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.18. 18:11:04

Szia Smuzli!
Sajnálom, hogy ezt a következtetést vontad le a történtekből, tutira állíthatom neked, hogy 100 százalékos védelem nem létezik. Eddig már sok száz, talán ezret is eléri, ami mintákat az évek során a VirusTotalra küldtem de ha egy-egy minta éppen nem lett detektálva, nekem nem az lett a véleményem, hogy el kell dobni az AV progit.
Az általad jelzett Adware.win32.kitsune.b egyébként egy Kasperskys elnevezés, és ők "not a virus" kategóriába sorolják.
www.virustotal.com/hu/analisis/cf06db93fd989b8032f9ea3047bb4ea1

Ez alapján valamilyen kéretlen reklámnak tűnik, és nem szaporódó vírusnak vagy kártevőnek.
Én mindenkinek azt szoktam javasolni, hogy használjanak még külön kémirtó programokat is, mert azok minden kéretlen, nem vírusnak besosorolt, csak "kellemetelen" programot is szűrnek és irtanak, a Spyware Terminatort és a SpyBot SD alkalmazésokat jó szívvel ajánlom, ingyenesek, jó minőségűek és gyakran frissülnek, valamint a NOD32-vel is tökéletesen megférnek egymás mellett.

smuzli 2008.05.19. 20:44:10

Halihó!Köszönöm a választ!Legalább vki foglalkozik is a problémával!Igazság szerint az elkeseredettség mondatta velem azt amit leírtam de tényleg nagyon sok embernek ajánlottam a nod sima és smart sec.es verzióját erre pont én szívtam vele.Nem akarok más írtot reklámozni de miután én kivégeztem a nodot megnéztem 1 ismerös gépét a kaspersky online scenerrel és 25! virust talált a nod mellett.Nem mondom h ez mind a nod hibája mert azt nem én állitottam be de azért szerintem kicsit sok.Szivesen visszarakom a nodot mert szeretem,de 1dolgot nem értek:ha átnézetem vele a gépet nagyon sok fájlra azt írja hogy nem tudta megnyitni és azokat kék szinnel írja ki.Általában a rendszervisszaállitás mappájában lévők ezek de vannak tömöritett fájlok is.Jó ez igy?KÖSZI!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.19. 21:00:23

Szia!
A végéről kezdem. Ha vírusos a gép, akkor érdemes kikapcsolni a rendszervisszaállítást, hiszen hiába mentesítesz, ha után ezzel egy korábbi fertőzött állapothoz térsz vissza.
A KAV-ra visszatérve én is nagyratartom őket, és évekig dolgoztam nekik, de ez a fajta összehasonlítás ennél lényegesen bonyolultabb dolog szerintem. Mivel volt már hasonló felvetés egy másik fórumban is korábban, egy kopi-pészttel idebiggyesztem az idevégó válaszomat:
A NOD32 alapbeállításban nem vizsgálja a tömörített fájlok belsejét kézi indítású víruskereséskor, tehát ha azokban van vírus, akkor nem jelez a program - ez végül is érthető, hiszen ezek a fájlok közvetlenül nem jelentenek veszélyt a gépre. Amint megpróbálja valaki kicsomagolni őket, az AMON rögtön megfogja a vírust. Van persze kivétel is: azokat a tömörített fájlokat, amiket a vírus kódja maga hozott létre, szignatúra alapján megtalálja a NOD32 is.

A NOD32 modulos felépítésű, hogy ne terhelje a rendszert. Éppen ezért az IMON modulban alapértelmezett beállítás az, hogy az internetről letöltött fájlokat teljes mélységükben megvizsgálja, tehát az IMON a tömörített fájlokat is átnézi.

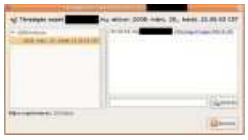
A fentiek miatt tehát elképzelhető, hogy a kézi indítású víruskeresésnél a NOD32 nem vizsgálta át a rengeteg ZIP, CAB, RAR, stb. fájlt, amiket a Kaspersky viszont igen. Mélyreható vizsgálatnál ez is megtörtént volna - a lényeg azonban így sem változik, a rendszerre közvetlen veszélyt jelentő vírusokat megtalálta volna a NOD32.

MSN balek kerestetik

2008.03.26. 18:00 | Csizmazia István [Rambo] | 16 komment

Címkék: msn név jelszó csalás phishing

Érdekes **MSN üzenet érkezett látszólag az egyik ismerőstől**. Rögtön szokatlan volt, hogy se bú, se bá, se hello hogy vagy, hanem **csak egy link érkezett**. Erre mondaná Leslie L. Lawrence, hogy **fejében megszólalt a vészcsengő, és jött a baljós megérzés**, ahogy azt Nágaföldön Radzs Kumar Szingh tanította neki.



A link egy bejelentkező ablakra néz, ahol a "PICS for MSN Friends" programot kínálnak nekünk, és **bizalomerősítésként rögtön az 1.1c változatot**. Ha már ennyi változat kijött belőle, akkor ez biztos nem csalás gondolhatnánk, de álljunk meg csak egy röpke pillanatra!

Ugyan minek kell az MSN nevet és jelszót egy vadidegen weboldalon begépeljük? Persze az sem tekinthető véletlennek, hogy mivel **az .info végződésű domainek adatait csak pénzért kérdezhetjük le**, erősen nőtt a népszerűsége a rosszfiúk körében.

Az úttörő ahol tud segít, és építi ~~a szocializmust~~ az adatbázist ;-)

Mindenesetre mi most hibaüzenetet kaptunk, kicsit úgy érezhetjük magunkat, hogy szépek lehetünk, de okosak nem.

Annyit azért hozzá kell tenni, hogy **az adatkezelési irányelvekben szerepel, hogy a nevünkben belépnek** és a programjuk népszerűsítésére használják majd accountunkat. Ezt a módszert határozottan nem kedveljük.

Akkor és ott jó ötletnek látszott belenézni a forrásba a Firebug nevű pluginnel, és van is mit nézni. Aki ekkora lúzer, hogy még a függvény nevében is bennehagyja a SPYCLICK nevű függvényt, az sikeres ember nem lehet.

Mátra alján falu, szélén, lakik az én öregnéném... Illetve egy ilyen jó sűrű erdőben **hosztolják ezt az jó kis amerikai oldalt** ;-) Szóval csak óvatosan azzal az MSN név-jelszó párossal.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/397897

Kommentek:

Vidi Rita · http://www.hosnok.hu 2008.03.26. 20:09:06

Jaaa, akkor amit én találtam (találtak nekem) valami hasonlónak volt a silány változata...
Magyarul...

A külföldi hülyékkel toleránsabb vagyok valahogy:) (az igazi hülyéktől ezennel elnézést kérek)

BKV figyelő.hu · http://bkvfigyelo.hu 2008.03.26. 23:16:3

Ez ubuntu ez?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.26. 23:25:31

Helló BKV figyelő!
Ez egy Gutsy Gibbon alatt futó Pidgin :-)

buherator · http://buhera.blog.hu 2008.03.26. 23:35:18

Akkor ha jól értem ez csak egy jelszólopó site, malware-t nem rak a gépre? Nem a saját gépemen (windowson és az otthoni biztonsági intézkedések nélkül) én is beszoptam ezt a kicsikét (persze a jelszavam nem adtam meg). Pont egy olyan buli utáni napon kaptam az üzenetet, mikor a haverok csináltak vagy száz fotót...Pech, de úgy tűnik senki sincs biztonságban.

BKV figyelő.hu · http://bkvfigyelo.hu 2008.03.27. 00:08:43

Pedig épp tegnap tettem fel a 7.10-es ubit, és kicsit hasonlított. Bár leszedtem, mert a telepítésekkel baj volt (később a terminálba megoldottam), viszont több probléma is volt vele:(

Pidgin amugy jó, a kopete nem akart bejelentkezni:(

Jó éjt!

átlátszó 2008.03.27. 02:41:58

Nem véletlen hasonlított az a 7.10-es ubi:)

lorandy 2008.03.28. 11:23:25

Hogy lehet kiírtani? Format C vagy új msn fiók kell?

buherator · http://buhera.blog.hu 2008.03.28. 12:25:42

@lorandy

Szvsz. elég ha lecseréled az MSN jelszavad.

Ben Dash 2008.03.30. 18:09:25

Hali,

Elvileg lejelszavaztam az oldalt :) mivel a hülyegyerek aki csinálta, nem tudom hogy de letörölte az oldalt, viszont fent hagyta a XAMPP-ot, és nem tiltotta a kívülről történő hozzáférést, vagyis simán le lehetett .htaccess-el jelszavazni. Ne próbáljátok ki, de elvileg nem tudtok hozzáférni; csak hogy még biztonságosabb legyen a dolog :D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.31. 08:32:54

@Lorandy:
Jól mondja Buherator, itt a mihamarabbi jelszó csere a fontos. És persze a sűrű elnézés kérés azoktól, akiknek látszólag küldözgetted a linket, hogy sorry, mégse te voltál...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.31. 08:36:38

@Ben Dash:
Akkor most ezért ír csak annyit, hogy "It works!"?
Heh, jó ötlet, és köszönjük a nép nevében :-D

Maura 2008.06.05. 23:00:06

En vagyok a hulye, hogy barki barmilyen linket kuld nekem, foleg ha koszones nelku, mindig rakerdezek, hogy ez szandekos-e eppen? es mit tartalmaz?

Ez nem alap dolog?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 08:39:06

Szia Maura!
Ez szerintem is alap, de sajnos sokaknak mégsem. Szerintem lassan ki fog alakulni mindenkiben egy alap gyanakvási szint, és akkor talán-talán kevesebben okoznak saját maguknak ilyen fejfájást.

koppola 2008.08.19. 14:45:24

Sziasztok! Az a nagy helyzet hogy a fenti linket én is beszoptam:D De ennél nagyobb a gondom. Freemailos msn ID.m van és hiába kérem a jelszóváltást, nem töltődik be az msn live oldala illetve folyamatosan a betöltés folyik de nem csinál semmit. Mit tuudok tenni hogy meg tudjam változtatni a jelszót vagy hogy egyáltalán kinyeshessem ezt a rohadék linken terjedó szarságot? Köszi előre is

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.21. 09:57:57

Hello Koppola!
Nem tudok róla, hogy a freemailes cím ilyen gondokat okozna.
Én ezt a linket ismerem a név-jelszó állításhoz:
login.live.com/login.srf?vv=400&lc=1038
Ha nem megy, próbáld megnézni, nincs-e valami cookie, script letiltva, nézd meg FF, IE, Opera alatt is, elvileg mennie kell.
Szólj majd vissza, hogy ezek segítettek-e, ha kell, agyalunk még.

koppola 2008.08.22. 09:46:02

Helló mindenki! Neked külön szép napot Rambo! Az általd adott linken sikerült megváltoztatnom a jelszót. A sima live messenger linken nem engedett de ezen igen. Ezer hálám! Végre nem fertőzök senkit és magam sem idegesítem magam:D Mivel hálálhatom meg. Tényleg örülök mint majom a ...:D

Olvasóink küldték - Frissítve!!!

2008.03.31. 16:43 | Csizmazia István [Rambo] | 21 komment

Címkék: vírus sample feldolgozás minta virustotal

Narancsos kolléga gyűjtéséből **kaptunk két különböző kártevőt**. Igyekeztünk segíteni és továbbítani őket az ESET víruslaboratóriumába.

Meg is lett az eredménye. Az MSNSERV.EXE állomány egy Windows alatti IRCBOT backdoor program, illetve annak egy más sokadik változata.

A másik minta **látszólag egy JPG képállomány** volt, de valójában egy letöltő trójai programmal álltunk szemben.

Köszönjük a víruslabornak a gyors segítséget, az új adatállományokkal már sikeresen detektálhatóak a fájlok.

*** * * F R I S S Í T V E * * ***

Közben **további kísérleteket végeztünk, immár a magyar NOD32 3.0-ás változatával.** Ennek feltelepítése után **lekapcsoltuk a netet, hogy ne tudjon frissüln**i az adatbázis, ekkor **az adatbázis dátuma 2008.03.13., azaz 2945-ös** volt.

Végeztünk egy kézi keresést, de ez ugyanúgy nem találta meg a két fájlt.

A keresés eredménye, **ha a □eben keresztül történik a letöltési kísérlet**, mégis pozítiv lett a második mintával. Ez még akkor is igaz, ha a localhostról, vagyis a saját gépről szólítottuk meg a böngészővel. Figyeljük meg, hogy **az adatbázis ugyanúgy a régi, március 13-i, ennek ellenére van találat**.

Ami még érdekes lehet, hogy a VirusTotal alatt egyelőre a 2.7-es verzió dolgozik, a közeljövőben valamikor várható a frissülés az új, 3.0-ás programra.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/399583

Kommentek:

narancsos (törölt) 2008.03.27. 21:49:03

Én köszönöm, hogy tudtam segíteni. Remélem sokaknak detektálja, mivel MSN-es körökben eléggé elterjedt ez a féreg, úgy látom.

sheppard 2008.03.31. 08:08:33

Szia Rambo. Egy kérdésem lenne. Windows Xp indításakor, kiírja, hogy 3 olvasatlan üzenet a fiókomnál. Biztos nem emailre gondol :) Feltettem az új 3-as nod trialt, frissítettem. Normál ellenőrzés, és semmi :(

Csizmazia István [Rambo] • http://antivirus.blog.hu 2008.03.31. 08:52:09

Hello Shephard!
Szerintem sem vírus, inkább valami zavar az Outlook vagy Outlook Express körül, ugye azt használsz? Az lenne a legtutibb, ha írnál a PCWorld fórumba, szerintem ott villámgyorsan adnak rá konkrét megoldást, biztos vagyok benne, hogy már másnak is volt ilyen gondja, és tudni fogják, mi kell ehhez.

sheppard 2008.03.31. 09:02:59

Szia, nem használok semmi ilyen mail progit. Kizárólag webalapú oldalakon nézem meg a leveleimet. Azért köszi.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.31. 10:16:31

Egyetlen ötletem van még: esetleg az MSN postafiókodban található olvasatlan üzenetekre figyelmeztet.

hoster 2008.03.31. 15:00:50

Igen, az MSN fiókod lesz az.

narancsos (törölt) 2008.03.31. 17:03:07

Ez érdekes :)
Ha már a gépen van a vírus, akkor nem ismeri fel, de ha localhostból vagy netről töltjük le, akkor felismeri?
MSN-en, ha valaki megkapja, akkor ezekszerint ugyanúgy veszélyeztetett. Jól értem?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.03.31. 18:34:18

Szerintem ez azt jelenti, hogy internetezés közben a legerősebb a védelem. Ez csak egy kísérlet volt, olyasmi, mint amikor a heurisztát próbára teszik, és direkt régi adatállománnyal néznek meg új kártevőket. De a naprakész, frissített adatbázissal - ahogy azt mindannyian használjuk a napi életben - mindkettőt megfogja kézi keresésben és röptében is.

narancsos (törölt) 2008.03.31. 18:43:23

Értem. Az tény, hogy a legújabb adatbázissal már felismeri minden körülmények között, és ez a lényeg.

narancsos (törölt) 2008.03.31. 19:03:02

Van egy másik vírusom amit nem ismert fel a NOD32. Küldöm a mail címedre.

narancsos (törölt) 2008.04.01. 13:51:34

Megint szereztem egy másikat, amit nem ismert fel, de AVG, AntiVir eddig mindet felismerte. Kezdek pipa lenni. Küldhetem azt is?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.01. 16:25:57

Hello!
Ez egy ilyen business. Olyan program, ami 100% mindent megtalál, sajnos nem létezik. Egyébként már azzal is segítesz, ha a VirusTotalon vizsgálódsz, hiszen ők a publikus mintákat automatikusan elküldik az AV gyártók laborjainak, hogy felvehessék az adatbázisba. Itt a blogon is sokszor mellékeltem már különféle VirusTotal eredmény riportokat, és azok között sok olyat is találsz, ahol meg éppen az AVG, az AntiVir vagy épp egy másik antivirus volt éppen pillanatnyi lemaradásban. MIndenesetre köszi a jelzéseket.

Algernon 2008.04.01. 16:53:04

Egyetértek Ramboval. Nekem abban a "szerencsében" van részem, hogy a munkahelyi email címemre napi 100-150 spam érkezik (na jó, hétvégén általában több :)), s a symantech által átengedett gyanús dolgokat megvizslatom a virustotalon. Nem merném kijelenteni, hogy szignifikáns különbség van a népszerűbb termékek között. Persze azért, én is úgy látom, hogy van egy élményezőny...(inkább az ár-érték arányokon lehetne vitatkozni...)Ja, és olvasgatva a régebbi posztokat is, nem igazán értek egyet azokkal, akik csak fizetős (azok közül is csak 1-2) vírusirtóval mernek kimenni a netre...Úgy látom, hogy a vírusirtók harcának harcmezejét már nem a férgek felismerési képessége jelenti, hanem az egyre profibb kémprogramok

kiszűrése. Ezen a területen pedig messze vannak a tökéletestől...
Igazából nem is értem, miért nem fejlesztenek ki a vezető vállalatok (pl. eset, kaspersky) kémprogramirtókat, s miért az antivírusba integrálják...
Azt azért szeretném hangsúlyozni, hogy intelligens nethasználat mellett otthoni használatra bőven elégnek tartom az ingyenes termékeket. Főleg, ha valaki kicsit utánajár a tűzfalaknak, kémprogi irtóknak, antivírusoknak.

zoloe 2008.04.01. 16:55:31

Szia narancsos!

Kérlek ilyen esetekben küldd a fájlokat a support kukac sicontact pont hu címre, jelszóval tömörítve. Így tudjuk beletetetni leggyorsabban az adatbázisba. Köszönjük együttműködésed!

hoster 2008.04.01. 18:14:07

@Algernon!
Abszolúte egyetértek veled. Az internetet ésszel kéne használni és kész.

narancsos (törölt) 2008.04.01. 20:40:59

Én is ésszel használom, de nem mindenki ért a számítógéphez meg kell hogy mondjam. Antivírus nélkül is meglennék, de fontosnak tartom azt, hogyha valaki kifizet 10 000Ft-ot egy vírusírtóért, akkor meg kapja azt amiért fizetett. NOD32 nem kicsi cég, biztos van bevétele, de az utóbbi időben 4 vírussal találkoztam, ami a "legnépszerübb" csevegő programon keresztül terjed, és nem ismerte fel. Az tény, hogy a NOD32 supportja gyors, és másnapra benne is volt a vírusadatbázisban a vírus amit küldtem. Az MSN nem hibás, hanem azok az emberek akik megnyitják a kapott fájl(oka)t. A spyware-ekről meg annyit, hogy többsége az interneten található, de az emberek jelentős része fel sem megy a netre, hanem különböző csevegőprogramokat használ inkább. Rengeteg ilyen embert ismerek, és azok jelentős része nem nagyon ért a géphez, ezért elfogadnak mindenféle fájlokat, de ha nincs megfelelő védelmük több, mint 10 000Ft-ért? Én elhiszem, hogy a NOD32 eléggé kiemelkedik a többi neves gyártó közül, de akkor is nevetséges, hogy 4 vírust eddig lazán beengedett. Hol van a ThreatSense ilyenkor?

hoster 2008.04.02. 00:24:27

Az emberek jelentős része nem azért kattint a hírtelen előugró linkekre, mert nem ért a számítógéphez, hanem azért mert naiv és figyelmetlen. Nem mondom, van abban igazság, amit mondasz, éppen ezért szükségesnek is tartom az antivírus használatát, de 100%-os megoldás nem létezik, hiszen ebben a gépezetben maga a felhasználó a leggyengébb láncszem. Úgy gondolom, hogyha a meglévő biztonsági szoftverek használata mellet az emberek is odafigyelnek, mire klikkelnek, akkor nagy baj nem történhet.

üdv,
xfaktor

Algernon 2008.04.02. 01:18:46

Valahol én narancsos koma nézetét is osztom. Ha úgy dönt valaki, hogy beruház egy internet security-be, szétnéz az egyes forgalmazók honlapján, jobbnál jobb, tökéletesebbnél tökéletesebb, díjnyertesebbnél díjnyertesebb, stb. terméket talál. A termékhez kapcsolódó kommunikáció (na és ár) alapján talán joggal várja el, hogy pár hét nethasználat (na persze az átlagosnál némiképp "kalandvágyóbb" nethasználat) után a gépe ne hasonlítson egy virtuális kártevőgyűjteményre. Csalódni fog.
(Csak így zárójelben: én még a boldog békeidőkben szocializálódtam a "presp1" és kazaa idejében, amikor hiába volt vírusirtó és tűzfal a gépen, 2-3 havonta sikerült levinnem a masinát a nirvánába...Na és persze hőbörögtem, hogy mi a fenét csinál akkor a víruskergető????
A mai helyzetet azonban rosszabbnak látom. Aki ma teszi meg az első lépéseket a neten, az jó eséllyel rengeteg észrevétlen élősködőt fog összegyűjteni, és ezek sajnos komoly veszélyt jelenthetnek a pénztárcájára. Az üzlet, az üzlet...a vírusíróknak és antivírusíróknak egyaránt...
Ugyanakkor nem bántanám a nodot. Sem a főbb konkurenseit. A víruskészítők óriási előnyben vannak, hiszen a fontosabb antivírus szoftverek naprakész frissítéseit próbálgatva optimalizálhatják az új kártevőket. Threatsense ide vagy oda, így azért elég egyoldalú a küzdelem.

Ha kapnék egy 10 e Ft-os utalványt, amelyen valamilyen biztonsági terméket vehetek, tuti nem antivírusra költeném, sokkal inkább kémprogi irtóra ruháznék be. Az antispyware-ek mezőnyében jóval nagyobb a különbség az egyes termékek között mint a tűzfalak vagy vírusirtók fizetős vagy ingyenes változatai esetében.

zoloe 2008.04.02. 13:14:03

@narancsos
Mivel a vírusírás mára üzletté vált, nincsenek nagy víruskitörések, a készítők célja a "radar alatt repülés". Ez azt jelenti, hogy a minták lassabban érkeznek a víruslaborokba, ezért olyan technikákat kell alkalmazni, amelyek minta nélkül képesek felismerni a kártékony kódokat. A proaktív felismerés a vírusdefiníció alapján történő felismeréssel ellentétben nem egzakt tudomány. Léteznek szakértők által végzett proaktív tesztek (pl: www.av-comparatives.org/seiten/ergebnisse/report16.pdf), amelyekből látszik, hogy egy-egy ilyen új technológia mennyire hatékony - az ilyen teszteken a NOD32 szokta a legjobb összesített eredményt elérni. Az olyan esetekre, amikor a vírusíróknak mégis sikerül olyan kártevőket létrehozni, amelyek "átverik" a felismerést, csak a könnyen elérhető terméktámogatás nyújthat megfelelő megoldást (ez az ingyenes termékek esetén nem áll rendelkezésre). Így a minta gyorsan eljut a laborba, illetve segítünk megtisztítani a számítógépet és így elkerülni a további fertőzéseket.

narancsos (törölt) 2008.04.02. 15:27:35

Elolvastam mindenki hozzászólását. No komment. Szerintem kitárgyaltuk. A további vírusokat, amiket nem ismer fel, azokat melyik e-mail címre küldhetem?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.02. 15:41:20

A legjobb, ha a support kukac sicontact pont hu címre, és jelszóval tömörítve. Köszi :-)

Shakira a célkeresztben

2008.03.31. 16:03 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: porno hamis shakira clip kártevő video.exe

A webes **kártevők terjesztői egy dologban igencsak naprakészek**: milyen csalogató tartalmommal lehet megkörnyékezni az embereket, mire van szükségük, **mire lennének kíváncsiak**. Napok óta Shakira állítólagos pornográf videójáról szóló, illetve arra linket tartalmazó levelektől hemzseg sokak postaládája.

A népszerű kolumbiai énekesnő valószínűleg sok fiatal hálószobafalán található meg poszter formájában. A **célközönség persze tökéletes találatnak számít**: azok a 10-18 év közötti fiúk, akik közül néhányan **nagy valószínűséggel nem eredeti Windowst használnak**, és emiatt aztán **a biztonsági frissítésekkel is le vannak maradva**, ergó ki lehet használni a sebezhetőségekre írt exploit kódokat. Aztán ez a korosztály még jobbára (tisztelet a kivételnek) **nem elég érzékeny és fogékony a veszélyekre, bátran kattint mindenhova**, sőt a közösségi oldalakon is **túlinformálja az ismeretleneket saját személyes adataival**, elérhetőségeivel.

Ki nem kattint a linkre? Valószínűleg a nők egyáltalán nem kíváncsiak Shakira pornó klipjére (de Christina Aguilera sem esélyesebb;-), aztán azok, **akik már ismerik az efféle támadásokat, valószínűleg ők sem dőlnek be ilyen átlátszó trükknek**.

Itt az ideje, hogy megnézzük, mi található a levélben található linken: reméljük senkit nem ér meglepetésként, hogy **egy azonnal letöltődni akaró video.exe fájl pattan elő egy ablakban**. Eddig kétféle hosszban találkoztunk vele: 61.5 KB és 72.5 KB, de a VirusTotal szerint egyforma fertőzést tartalmaznak: Win32/Agent.ETH.

A kártevő terjesztésén túlmenően még azzal is elégedetlenek lehetünk, hogy sajnos szinte nincs is olyan sztár (és ezt most valódi és jó értelemben használom, a villalakó nekem nem sztár), akit valamilyen módon **ne próbálnának meg besározni hamis információkkal**.

Miközben a Wikipédián nézegettem a Shakiráról szóló bejegyzést, akkor olvastam a hamisított szócikkről szóló blogot, **ami számomra elég meglepő és érdekes volt**. Búcsuzóul megállapíthatjuk, hogy **amit az interneten látunk vagy olvasunk, nem kell mindig készpénznek venni**, bízzunk valamit a józan eszünkre, korábbi tapasztalatainkra illetve kételkedésünkre is, és soha ne támaszkodjunk Wendriner Aladár feliratú oroszlánketrecnek...

Ajánlott bejegyzések:

- A PRISM szeme mindent lát

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/404294

Kommentek:

Nincsenek hozzászólások.

A szeme sem áll jól...

2008.04.01. 21:30 | Csizmazia István [Rambo] | 8 komment

Címkék: szem hamis nod32 csaló pc spy álkémirtó pc antispyware

Többször is foglalkoztunk már csalárd programokkal: álvírusirtó, amely nem csinál semmit, **álkémirtó, ami maga a trójai kémprogram**, és működéséért még pénzt is kér. Ami miatt a mai delikvens a nyomozás látóterébe került - ezt Garamvölgyi László sem mondhatta volna frappánsabban - **az a kémirtó fertőzött állományokkal kapcsolatos figyelmeztetés ablaka** volt. De ne szaladjunk az események elé, jöjjön, aminek jönnie kell.

A PC-Antispyware programról van szó. **Egy kedves olvasó küldte be a képernyőképet**, és jól meglepődtünk, **mennyire megtévesztően hasonló a NOD32 2.7-es találati képéhez**.

Védjük meg magunkat a kémprogramoktól és a vírusoktól - szólít meg a reklám a weboldalon, és biztos van, aki ezt el is hiszi. Mi valamilyen rejtélyes okból nem tartozunk ezek közé.

Ha vesszük a fáradtságot és kíváncsiságból feltelepítjük, **a NOD32 szépen beriaszt** már a puszta telepítési kísérletre is, hiszen kéretlen reklámokat jelenít meg a gépeken.

Ahhoz, **hogy feltelepíthessük, ki kellett kapcsolnunk a NOD32-t**. Ezekután végeztünk egy keresést az új kémirtóval, és lám, máris három fenyegető kémprogramot fedez fel gépünkön.

Nem kizárható, hogy **egy frissen telepített gépnél is talált volna valamit**, mert enélkül **mivel lehetne rávenni a kuncsaftokat, hogy vegyék meg** a teljes verziót?

Mert a **mentesítésre persze csak a teljes, fizetős változat** képes...

Egy "életveszélyes" ;-) Aurate cookie bejegyzés és a tágra nyílt pupilla. **Ne dőljünk be neki!**

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/406598

Kommentek:

virkid 2008.04.02. 08:51:45

Mivel az általam védett gépeken többször találkoztam már hasonló programokkal. így a következő módon tudtam leszedni... Egy folyamat indulásokat figyelő progit feltettem, és a gépet átnéztem spy illetve vírusirtó programmal... Valamelyik rátalál a kérdéses állományra, és a folyamat figyelővel tudtam megállítani a káros program újra keletkezését. A riasztott registry kulcsot pedig kézzel kell törölni. :-)))
Nod esetében is így kéne eljárni?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.02. 15:37:41

Ha a kérdés a fenti programra vonatkozik, a NOD32 már települni sem engedte, ehhez ki kellett kapcsoljam az aktív védelmet. Ha pedig már fent van, simán irtja, törli vagy karanténba teszi a beállítástól függően. Én az új, 3.0 verzióval játszottam, a korábbi 2.7-esnél nem tudom, de valószínűleg az is ugyanúgy megfogta volna.
Ha a kérdés általános jellegű, úgy igen, a kártevő törlése/karanténba zárása a mentesítése történik, a registry kulcs így önmagában már nem okoz gondot, kézzel is törölhető, de számos esetben a külön kémirtók megteszik ezt a "gyomlálási munkát".

töti 2008.05.06. 21:00:57

Hellosztok!
Mit tegyek hogy leírtsam a gépről ezt a PC-Antispyware-t mert, próbáltam avast-al és Spyware Terminator-ral is, az utóbbi meg is találta etavolítom és ugyanúgy küldi ezeket a reklámokat hogy fertőzött a gép. És az lehet hogy ez a program letiltja a Feladatkezelőt? Ezekre a próblémákra keresnék mielőbbi megoldásokat, ha valami ingyenes antivirussal le lehetne írtani, az érdekelne. Előre is köszönöm a válaszokat!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 21:16:56

Szia Töti!
Először is részvétem. Amint a képeken látod, a NOD32 észleli és irtja is, tudsz belőle 30 napos próbaváltozatot is letölteni. Azt javaslom, válassz ki benne minden opciót (pl. veszélyes alkalmazások keresése, kiterjesztett heusriztika, stb.) frissítsd az adatbázist, és úgy állj neki az irtásnak. A Terminator mellett szeretem még a SpyBot SD progit is, szerintem erre a bajra is jó lehet. Dobj majd egy kommentet, ha túl vagy az akción!

töti 2008.05.06. 21:51:49

Hi!
Próbáltam már NOD32-vel , de amikor adatbázist akarok frissíteni regisztrációt kér, ha lehetne tudnál adni egy linket ahonnan letudom tölteni. És a Feladatkezelőt letilthatja? Vagy azt hogyan kell visszaállítani?

Algernon 2008.05.07. 09:52:14

Szia Töti!

Próbáld ki ezt a progit, sztem megoldja.
download6.emsisoft.com/a2FreeSetup.exe

Vagy nagyon jó még az avg antispyware.
www.avg.hu

töti 2008.05.11. 20:16:55

Hi!
Még Pénteken lefuttattam az elsőt amit Algernon belinkelt , tegnap még rajt volt és rendesen jöttek a reklámok. Ma amikor bekapcsoltam a gépet meglepő módon nem jöttek be a reklámok és a Feladatkezelőt is meg tudom már nyitni. Véleményem szerint egy jó vírusírtó kell meg várni egy hetet, ha feltelepíted(mivel pontosan egy hete települt fel a gépemre:D).Köszönöm mindenkinek a segítséget! :D

titan 2010.04.28. 17:03:34

Nekem a kedvenceim azok, amik egyszerű böngészős popupban jelennek meg, és úgy figyelmeztetnek, hogy a látogatott oldal beépített víruskeresője x db spyt és y db vírust talált a gépemen :) Olyankor elmosolyodom egy pillanatra, de aztán eszembe jut, hogy ennek tényleg van aki bedől...

Április bolondja

2008.04.03. 12:54 | Csizmazia István [Rambo] | 7 komment

Címkék: web internet vírus 1 rossz tréfa kártevő nuwar aprilis

Sok vicces hírt olvashattunk 1-én, többek közt a vissza az MS DOS-szal a számítógépekre, és a Feltörték a Linuxfórumot sem volt rossz tréfa, bár lehet, hogy nem jó az ördögöt a falrafesteni. Mint minden alkalom, ez sem maradt ki azonban a kártevő terjesztők repertoárjából, vírusküldésre nagyon is alkalmas a bolondok napja. Csak ez sajnos egyáltalán nem vicces...

Egyedül abban bízhatunk, hogy a recept már annyira sablonos, hogy **talán ez már előbb-utóbb feltűnik** a számítógépet használóknak, és kétszer nem lépnek bele ugyanabba a folyóba. Szóval érkezik egy - szerencsére nem magyar - angol nyelvű e-mail, benne egy IP címes linkkel, és az susogja a fülünkbe: **Meglepetés!**

A szószátyárság nem sajátja a brigádoknak, ez van. S hogy a meglepetés kiknél lesz kellemetlen, abban nyilván része lesz az olyanoknak, akik vírus- és kémirtó nélkül végzik napi sétájukat az internet országútján.

A weboldalon azonnal megpróbál letöltődni egy Funny.exe nevű állomány

Azt kell észrevenni, hogy az ilyen támadások **már nem jelentenek külön extra munkát a rosszfiúknak**, egy pici ötlet kell hozzá, **milyen képet jelenítsen meg, hány fertőzött gépet használjon, hány percenként cserélődjenek a fertőzött oldalak címei, és slussz-passz kész**: sorozatgyártásban, automatikusan generálják őket. **Amikor ez a mostani fut, már rég a következő** ünnep, alkalom, tragédia, olimpia, politikai eseményt keresik és készül a még újabb kampány.

A keletkező állomány neve lehet kickme.exe vagy foolsday.exe is

A mi házunk táján meg a **naprakész vírusvédelem, a naprakész operációs rendszer, és minden biztonsági javítással felvértezett alkalmazások kelle(né)nek**, és nyugalom lenne.

Az, hogy a vírusírók írják és szétküldik, ez szinte olyan, mint hogy kék az ég és zöld a fű - nem igazán tudjuk megváltoztatni. De az, ahogy **a tudatlan felhasználókból élnek, őket kihasználják** és a botnetekben irányítható fertőzött gépek seregével terjesztik a kórt, az már igen is a mi felelősségünk, **a felhasználók közös problémája**. Ne legyünk mi egész évben április bolondja!

Szerencsére a víruskeresők jó részében már a heurisztika riaszt

Amíg lesznek olyanok, **akik vagy nem értenek hozzá**, és nem értik mi a probléma, vagy csak lusták esetleg **nem is érdekli őket, hogy másoknak mit okoznak** saját felelőtlenségükkel és figyelmetlenségükkel, addig gépeik mindenkire ontják az internet szemetét, kártevőit, támadásait. Lehet, hogy mégis kéne jogosítvány az internetezéshez?

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/409124

Kommentek:

Algernon 2008.04.04. 19:45:02

Az oldalon megváltoztatták a képet és a "programot" is. Az új változat tényleg vírusmentes lenne?
www.virustotal.com/hu/analisis/96dacb162ee81d92181f2538cfc31952

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.04. 22:35:13

Szia Algernon!
Szerintem vigyázz inkább, mert szinte biztos, hogy ez újabb Storm variáns. A VirusTotal oldalon még a régebbi, 2.7-es verzió van, de ha az új, 3.0-s változattal próbálom letölteni, a NOD32 rögtön riaszt rá az alábbi üzenettel: "Valószínűleg módosult Win32/Statik alkalmazás" és karanténba teszi a withlove.exe állományt.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.05. 14:25:30

Az is jól látható, hogy Algernon exéjének MD5-je teljesen különbözik attól, amit én vizsgáltam, vagyis a weboldal ontja különféle variánsokat, talán minden egyes letöltött fájl különbözik.
Algernon féle exe:
File size: 139776 bytes
MD5...: f602901cf345b5279e8099b27e240d1a
SHA1..: 96a97e479bd61a544ab4525f699b3a3d538e24cd
Amit én néztem:
File size: 139777 bytes
MD5...: e6c08ec8e4bd8dcfff118eed25a50508
SHA1..: 45081aa3d91b26be00e35e4d3ad1a71656eaf7c7

Algernon 2008.04.05. 22:17:56

Én Avasttal néztem, nem morgott rá. Az exe-t letöltöttem, feltöltöttem, majd kitöröltem, remélem, így nem veszélyes. A biztonság kedvéért futtattam egy eset online scant is, de nem talált semmit. Az Avast egy kicsit fejlődhetne a heurisztikájában... A withlove exén kívül más kártevő be lehetett ágyazva az oldalba? Ugyanis a temp könyvtáramból valami abrakadabra.exe internethozzáférésért folyamodott, de csak karantént kapott.:)

Viszont el kell ismerni, nem lehetnek rosszak a stormos fiúk, hétről-hétre a víruskergetők előtt járnak. Szép teljesítmény a nodtól, hogy elkapta.

Algernon 2008.04.07. 12:21:20

Aki szeretne angelina jolies screen savert, figyelje a postaládájában a legfrissebb spameket. :)

www.virustotal.com/de/analisis/e85d14b15f7b6758b01318ed237e17d8

zoloe 2008.04.07. 16:12:44

Szia Algernon,
megnéztem, és tényleg volt a kukámban ilyen spam! :)
Köszi, hogy szóltál, a 3007-es adatbázistól (20080407) már a NOD32 is felismeri, Win32/Wigon.BM trójai néven.

Algernon 2008.04.07. 16:21:18

Ez gyors volt. :)

A Storm saga folytatódik

2008.04.07. 21:03 | Csizmazia István [Rambo] | 7 komment

Címkék: letöltés storm kártevő kéretlen withlove heurisztika

Kedves olvasónk, Algernon kommentjében jelezte, hogy április elseje után **új kinézettel új kártevőket** kezdett terjeszteni a korábbi cikkünkben szereplő weboldal.

A bolondok napja után **visszatért a Valentin napi rózsaszín szíves stílus**, de a kártevők látszólag **egyre újabb és újabb variánsok**.

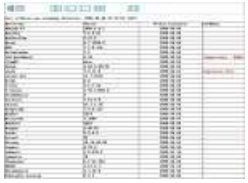
Egy amerikai weboldal próbálja ránktukmálni a kéretlen letöltéssel érkező kártevőit, a térképen látható helyen alighanem egy engedelmes, sztahanovista **zombi gép** szolgálja immár hetek óta hűségesen a "vadak urát".

Több különböző letöltést kipróbálva - ez persze csak kikapcsolt vírusirtóval sikerült - az állományok bár egyforma hosszúak vagy csak minimálisan térnek el egymástól, de **az MD5SUM segítségével is jól látható, hogy tartalmukban különböznek.** Úgy tűnik, minden letöltésnél más állományt kapunk, de legalábbis igen nagyszámú variáns közül választódik ki véletlenszerűen a letöltött withlove.exe.

File 1 size: 139776 bytes
MD5...: f602901cf345b5279e8099b27e240d1a
SHA1..: 96a97e479bd61a544ab4525f699b3a3d538e24cd

File 2 size: 139777 bytes
MD5...: e6c08ec8e4bd8dcfff118eed25a50508
SHA1..: 45081aa3d91b26be00e35e4d3ad1a71656eaf7c7

File 3 size: 139777 bytes
MD5...: bb23ca2c46d54bfb14a9cefd04183e43
SHA1..: 2621274481a77e520abe74969f8b93b54234840a



Szerencsére az új NOD32 heurisztika jól teljesít, gépünkön az új, magyar nyelvű ESET Smart Security változat fut, és hiába látjuk azt,

hogy a VirusTotal-on nincs találat - mert ott még egyelőre a 2.7-es verzió dolgozik - élesben, a számítógépünkön az újabb Storm változatoknak esélye sincsen.

Egy kicsit módosítva a James Bond film címét: az Amerikából szeretettel küldött holmit köszönjük, de momentán nem kérjük.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/415904

Kommentek:

zvaragabor 2008.04.08. 17:17:30

A cikk címe tetszik a legjobban. :)
"Storm saga"
Üdv.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.08. 22:36:51

Szia Gábor!
Hát ennek a folytatásos családregénynek sem látszik a vége ;-)

Algernon 2008.04.09. 12:04:32

Ha ezek a viharos úriemberek tényleg ilyen szeniorok a vírusírás területén, hálásnak kell lennünk nekik, hogy a terjesztési, "hálózatépítési" stratégiájuk ilyen alacsony szintű. Ha ezeket az önmutálódó bacilusokat elkezdenék msn-en terjeszteni, esetleg egy-két weblapot feltörnének, s beléjük ágyaznák a kódokat, influenza-szerűen tudnák terjeszkedni, s egyszer csak egy virtuális

holtak hajnalára ébrednénk. :)

zvaragabor 2008.04.09. 14:39:29

Különben a valentínos oldal megváltozott, most már egy stormcodec-et lehet letölteni.

Algernon 2008.04.09. 14:48:39

Szélesedik a termékpaletta...:)

Tegnap úgysem sikerült elindítanom egy videó file-t, lehet, ez megoldja a problémát.:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.09. 14:56:16

Gyerekek!
Már írom is, este a képenyőképeket is leszedtem, de az oldal már szinte gyorsabban változik, mint ahogy én a postokat teszem fel :-D Hamarosan folytatása következik...

Algernon 2008.04.09. 15:15:08

A Dallasban ehhez képest alig voltak fordulatok....:)

Magyar kártevő toplista - 2008 március

2008.04.09. 14:43 | Csizmazia István [Rambo] | 9 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

A NOD32 antivírus rendszer gyártója, az ESET havonta elkészíti a legelterjedtebb **internetes kórokozók top tízes** listáját. Nézzük akkor, milyen hónapot is zártunk **márciusban Magyarországon**! Következzen a **NOD32 antivírus rendszert gyártó ESET ThreatSense.NET Center** felmérése.

A vírusstatisztika alapját a vállalat ThreatSense.Net vírusfigyelő rendszere képezi, amely a NOD32 felhasználók önkéntes adatszolgáltatásának köszönhetően az e-mailekben terjedő vírusok mellett a böngészés közben a számítógépekre került kórokozókat is listázza és mostantól ezt országokra lebontva is le tudjuk kérni, így végre arra is mód nyílik, hogy a havi toplista teljes egészében a magyarországi észlelésekre alapozva jelenhessen meg.

A listán szereplő tételek **minden esetben konkrét károkozókat jelölnek**, az eredeti listában található csak gyanítható, de egyértelmű azonosításra nem alkalmas észlelési adatokat nem vettük figyelembe. **Igyekeztünk a legtöbb kártevő mellett feltüntetni** a weboldalunkon található részletes vírusleírásra mutató linkeket is.

Íme a lista!

1. Win32/Adware.Virtumonde application (8.76%)
A Virtumonde (Vundo) program a Kéretlen alkalmazások (Potentially Unwanted) kategóriába esik, készítői arra használják, hogy **segítségével kéretlen reklámokat** másoljanak a felhasználó PC-jére.

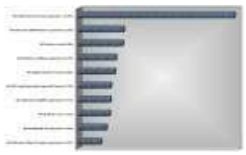
2. Win32/Toolbar.MyWebSearch application (2.53%)
Az Internet Explorer és Firefox alatt működő keresőszolgáltatás. Telepítésekor **számtalan Registry kulcsot módosít, és kéretlen reklámokat jelenít meg** az adott számítógépen. Az alkalmazás **figyeli a felhasználó böngészési szokásait és adatokat gyűjt** ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kliens kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

3. INF/Autorun virus (2.49%)
Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő **fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul**.

4. Win32/Adware.AdMedia application (2.10%)
Windows rendszereken terjedő kéretlen reklámprogram. A megtámadott számítógépbe beépülve különböző kártékony DLL állományokat hoz létre, illetve tölt le az internetről, a Registry adatbázisba pedig olyan bejegyzésket készít, amellyel gondoskodik arról, hogy a kártékony kód minden rendszerindításkor automatikusan lefuthasson. Működése során több különböző kártékony weboldalhoz is megpróbál kapcsolódni, és a megfertőződött rendszer a tulajdonos tudtán kívül **képes más weboldalak ellen indított DoS támadásban is részt venni**.

5. Win32/Obfuscated.A1 trojan (2.02%)
Az Obfuscated (összezavart kódú) elnevezés egy olyan általános kategória, amellyel számos fájl már proaktívan felismerésre és eltávolításra kerül, **amelyek gyanús technikákat használva igyekeznek kibújni az antivírus vizsgálat elől**. Az ilyen állományok többsége reklámprogramokkal (Adware) ellátott alkalmazások telepítő csomagjaiból származnak, mint amilyen például a korábban is említett Virtumonde. Futása közben **kéretlen reklám ablakokat jelenít meg**.

6. Win32/TrojanDownloader.Agent.KGV trojan (1.79%)
Hatodik helyen egy **trójai alkalmazást** találunk, illetve egész pontosan annak már egy sokadik változatát. Ez a trójai fertőzéskor különféle kártékony állományokat hoz létre a Windows/System32 mappában, emellett Registry kulcsok létrehozásával gondoskodik arról, hogy a számítógép újraindítása után is automatikusan lefuthasson.



7. Win32/Adware.PlayMP3Z application (1.77%)
Ez az alkalmazás a kéretlen és felesleges alkalmazások körébe tartozik. **Kéretlenül reklámokat jelenít meg, MP3 tartalmakat és lejátszóprogram komponenseket tölt le**. Automatikusan nem képes terjedni, ehhez szüksége van felhasználó közreműködésre is. Az elemzése alapján feltételezhetően Kínából származik.

8. Win32/VB.EL worm (1.73%)
A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható **adathordozókon és hálózati meghajtókon képes terjedni**. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is.

9. Win32/CMDOW.143 application (1.54%)
A cmdow.exe állományra sok antivírus program nem jelez, hiszen nem vírusról, hanem egy hacker eszközről van szó. A cmdow egy olyan **parancssori segédprogram**, melynek segítségével Windows NT4/2K/XP/2003 rendszereken kilistázhatjuk, átmozgathatjuk, átméretezhetjük, átnevezhetük, illetve elrejthetjük vagy ismét láthatóvá tehetjük, minimalizálhatjuk vagy kinagyíthatjuk, helyreállíthatjuk, aktiválhatjuk illetve inaktiválhatjuk, továbbá bezárhatjuk, leállíthatjuk az ablakokat. Az eredeti cmdow alkalmazás egy 31 KB-os végrehajtható fájl, amely nem ír a Registrybe, **nem igényel külön telepítést, elég lefuttatni**. Eltávolításához elegendő ezt az állományt törölni.

10. Win32/Adware.WhenU.SaveNow application (1.24%)
Ingyenes programokba beépítve érkezik - ilyen például a BS Player - és **kéretlenül reklámokat jelenít meg**, illetve kémkedik a felhasználó

szokások után. Sok esetben a saját uninstall procedúrája nem képes sikeresen eltávolítani. Működése közben a process listában is látható save.exe rendkívül magas , sokszor **80% feletti erőforrás terhelést okoz, és jelentősen lelassítja a számítógép működését**.

Ezek tizen adják az összes észlelés 25.97 százalékát, vagyis a további megközelítőleg 74 százalékon már sok, kisebb arányban előforduló kártevő osztozik.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/418243

Kommentek:

Algernon 2008.04.09. 15:32:30

"Ingyenes programokba beépítve érkezik - ilyen például a BS Player - és kéretlenül reklámokat jelenít meg..."

Ha feltelepítem a BS Playert, automatikusan megkapom ezt is?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.09. 15:36:55

A régebbi változatokban biztosan nem volt, állítólag az újakban azonban már igen. Én szerencsére jó ideje átálltam VLC-re: mindenevő,ingyenes és nincs benne kéretlen meglepetés ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.09. 15:39:06

Ha rákeresen Google-val, ott vannak infók, pl.1.38-as verziótól felfele:
www.spywaredb.com/remove-whenusave/

Algernon 2008.04.09. 15:49:25

Érdekes, nekem van BS Playerem, de eddig még nem szóltak az antispywarek (spycatcher, avg, ad-aware), de ha hazaértem, a link alapján majd utánanézek.
Köszi az infot!

Algernon 2008.04.10. 13:11:48

Megvizslattam a masinát a fenti antispywareken kívül (ezek nem találtak semmit) még a-squareddel is, ami néhány bs-playeres registry kulcsut veszélyesnek ítélt, és törölt, de whenusave-nek nyoma sem volt. Vagy nem volt benne az általam telepített verzióban, vagy a spycatcher/avast progik valamelyike fel sem engedte települni.

Kipróbáltam a VLC Playert is. A feliratok kezelésében azért sokkal jobb a BS Player...

Nolfo 2008.04.16. 10:34:19

Egyébként ha tehetitek szerezzétek be a BSPlayer réges-régi (talán 1.1?) változatát, az akkor még ingyenes volt és nem volt benne semmi vírus- vagy kémprogram.

Algernon 2008.04.16. 14:50:32

A szoftverbázisról letölthető az 1.36-os verzió magyarul, abban sincs még benne a whenusave.

bryan 2008.05.04. 15:09:41

A legjobb médialejátszók szerintem:
mpf.dzm.hu/download.php (mplayer frontend) linux alapú, windows alatt is tökéletesen fut mindent játszik, még part file-okat is. Ráadásul magyar a kitalálója:)
Van még az erre épülő Dziobas rar player is, ami még feliratkezelésben is felveszi a versenyt a bs playerrel.
ds6.ovh.org/drp.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.05. 10:34:07

Hi Bryan!
Volt szerencsém egy munkahelyen dolgozni egy rövid ideig Bérczi Gáborral (Gabucino) és Ponekker Zoltánnal (Pontscho) :-)

Neverending Story

2008.04.09. 15:08 | Csizmazia István [Rambo] | 1 komment

Címkék: story storm nuwar neverending gen

Storm ügyben úgy látszik **a blogger nem lehet elég serény ahhoz, hogy csak egyetlen weblap kaméleon-szerű átalakulását is nyomon kövesse**. Néha már olyan feelingje van a dolognak, mintha a kártevő készítő olvasná a blogot, hogy aztán egyre újabb és újabb fejezetet karcoljon a történelembe. Tisztára mint a Whiskys rabló: lehet, hogyha bejelentenénk, hogy csak keddenként írunk postot, akkor hétfőre tenné át a kódváltásokat ;-)

Tegnap este már látszott az új tartalom a már annyit emlegetett weboldalon: most **a már szinte viccesnek ható Storm Codec** található rajta. Ilyen nincs, és mégis van.

Azazhogy csak egy annak látszó tárgy, de **valójában persze egy új Nuwar (Storm/Zhelatin) variáns** az, ami szeretne bejönni.

A heurisztika szép, a heurisztika jó, a heurisztikát szeretjük :-)

Meg kell menteni Fantázia birodalmát, mielőtt bekebelezi azt a Storm Semmi - és ebben alighanem Sebastian komoly segítségre szorul...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/418461

Kommentek:

Algernon 2008.04.10. 13:48:20

Aki kapott ma Obama nagyijára utaló linket, szerezhet storm-codecet.
newoneforyou.cn

Viszont már a weboldalba is bele van ágyazva a vírus...Folyik azért intenzívem a "product development".:)

Ugye mi jó barátok vagyunk?

2008.04.11. 11:00 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam iwiw levél hi5 kéretlen

Ha van még **valami ici-pici értelme** az olyan közösségi oldalaknak, mint például az IWIW, az éppen az, hogy **esélyt kínál arra, megtalálhassuk** azokat, akikkel együtt szórtunk homokot a tökünkre az óvodában, ismét láthassuk alsótagozatos korunkból az osztály szépét, vagy szinte **elfeledett ismerőseinkkel** újra találkozhassunk a virtuális térben, de akár egy valóságos krigli sör mellett is.

A közösségi oldalak jól reprezentálják a felhasználók sokszínűségét. Az óvatosabb, vagy technikailag már **rutinos versenyzők - nagyon helyesen - jóval szűkebb adathalmazt adnak meg magukról**, mint a tizenéves fiatalok vagy a naiv felnőttek. Közhely, hogy a munkaadók, sőt a titkosszolgálat is előszeretettel vizsgálódik ebben a közegben.

A köszönöm majd máskor helyett inkább a sohanapján lenne a jó válasz

Az már inkább negatív jelenség, hogy **adathalász jellegű módszerek is előkerülnek** némely közösségépítő portálon, amellyel ha anyagi értelemben nem is szenvedünk közvetlen kárt, kapcsolatrendszerünknek **tudtunkon és akaratunkon kívül jelzést adhatunk, mekkora nagy idióta lamerek, Isten barmai is vagyunk** mi itten kérem tisztelettel.

Nem sikerült a címjegyzék importálás, vajon miért ;-)

A Hi5 portálos regisztrációnk után vajon **mit szól az összes Gmail, Yahoo, stb. címjegyzékbeli ismerős, ha kéretlen reklámlevelet kap**, amelyben mi vagyunk a feladók? Mert ez történik, ha gyanútlanul begépeljük az adott levelezéshez tartozó név-jelszó párost.

Kétségbeesett kedves jóbarát jelezte, hogy óvatlanul megadta a Gmail-es accountját, és az összes címjegyzékbeli ismerőse (száz feletti címre, még saját magát is beleértve) **kapott egy kéretlen spamet, hogy legyen a barátja**.

A **kellemetlen feladatokat is el kell időnként végezni**, mert hát az élet nem habostorta. Segíthet az EULA - magyarul a felhasználói licenc szerződés - **alapos elolvasása**, illetve az **1. elolvasás. 2. megértés. 3. döntés. 4. cselekvés munkafázisok** tudatos alkalmazása a csimpánz módra "könyököljünk gyorsan a Next gombra" módszer helyett. **Ha nem tetszik amit látunk, akkor arra a helyre ne regisztráljunk**, hiszen nem kötelező. A képen olyan passzusok is láthatók, amivel nem biztos, hogy mindenki egyetért és aláírná. Pedig **a figyelmetlen kattintással éppen ezt teszi: jóváhagyja, elfogadja**. Bár alaposan végigböngésztük a szerződést, **arra nem találtunk jóváhagyást benne, hogy a nevünkben leveleket küldözgessen**.

Ezt is elfogadtuk: vitás esetben írkálhatunk angolul az amerikai bíróságra.

Egyetlen módszer (a redőnyhúzóval végzett "szelíd rábeszélés" mellett) létezik csak, amit mélyen a felhasználók tudatába kellene vésni - esetleg beletetoválni a retinájukba - **sose adjuk meg egy regisztrációnál egy másik helyre vonatkozó belépési nevünket-jelszavunkat is**.

A **spamek egyetlen pozitív mellékhatását** (amihez korábban a telefonkönyvet kellett böngészni, és leszámítva, hogy elég ritkán van rá szükség), amikor **születendő gyermekünk számára keresünk valamilyen jól csengő keresztnevet** (William, Hanna, Joseph, Barbera, Tom, Jerry, stb.) sajnos - vagy talán hál' Istennek - egyelőre még csak az angol nyelvterületen élők élvezhetik ;-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/420844

Kommentek:

Nincsenek hozzászólások.

Zombi-e vagy?

2008.04.14. 13:43 | Csizmazia István [Rambo] | 2 komment

Címkék: kína security smart zombi zone botnet storm eset ess

Köszönjük a kérdést, reméljük a legjobbakat, vagyis hogy nem. Mindenesetre vigyázó szemünket egy érdekes weboldalra vetjük, ez pedig nem más, mint a Security Zone sok érdekes biztonsággal kapcsolatos információt közöl, a Stormmal kapcsolatos cikkében pedig név szerint láthatjuk **az éppen aktív fertőző - főleg Kínában regisztrált - weboldalak címeit**.

A Neverending Story kapcsán kaptunk egy kommentet, az ott említett weboldal címe szintén ott vírit a listán. Ugyan a http://newoneforyou.cn/ oldal jelenleg **már nem működik** - csak remélhetjük, hogy már végleg lekapcsolták.

Azonban **a többi oldalról automatikusan és kéretlenül próbál települni** egy Nuwar (Storm) variáns a gépünkre. A **Smart Security szerencsére szépen teszi a dolgát**: a kopogtatás után udvariasan a karanténba tessékeli a hivatlan látogatót, és megkéri, a továbbaikban legyen kedves legott várakozni...

Nem voltunk restek, és végignyálaztuk a domaintoolsban, **ki és mikor regisztrálta be** az oldalakat, és úgy látszik, **Linson George sajnos nem volt álmos április 9-én**, és kilóra foglalta le yahoos e-mail címéről a listában szereplő címek többségét.

Lehet, hogy **mindannyian jobban járunk, ha mégis bevette volna** az ágy alá gurult altató piruláit, vagy ha aznap éppen valami jó horror film megy a TV-ben. Sajna bebuktuk.

A fertőzött gépek **fizikailag szétszórtan helyezkednek el**: van japán, török, USA-beli, koreai, kanadai, lengyel, román, argentín, stb.

Azt egészen biztosan kijelenthetjük, **sajnos nem utoljára került terítékre** ez a téma. Uri Geller szavaival élve: Botnet, áz internetes színpád (sajnos) á tiéd...

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/424711

Kommentek:

zvaragabor 2008.04.14. 16:55:40

orthelike.com hostot lescannoltam nmap-pal, talált egy nyitott tcp 80-as portot. Fogtam egy flooder(DoS-oló) programot, és adtam neki. Egy üres oldalt hoz be a böngésző. :D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.13. 16:15:32

Egy kis érdekesség:
index.hu/tech/biztonsag/zom130508/

A tanú

2008.04.15. 11:36 | Csizmazia István [Rambo] | 1 komment

Címkék: bíróság légy phishing adathalászat heurisztika tanúkihallgatás résen

Nem, ezúttal nem Bacsó Péter örökbecsű és szívünknek kedves darabjáról lesz szó, hanem a megtévesztés egy újabb rafinált módjáról: phishing kampány indult kifejezetten cégvezetők, vezető beosztású menedzserek ellen, ahol egy **látszólag a bíróságtól érkező e-mail üzenetben** - amely **hibátlanul tartalmazza teljes nevüket, telefonszámukat** - egy adathalász oldalra igyekeznek csábítani az áldozatokat.

És látszólag nem is sikertelenül, **mintegy 1800-an meg is tették ezt a kis szívességet**, hogy átkattintottak a levélben szereplő linkre.

A sok Viagrás, Rolexes, tőzsdés levélen vagy codec letöltési ajánlaton nevelkedve már szinte Pavlovi reflexszel könyöklünk a Delete gombra, de ki nem hőköl vissza, vagy mer nem komolyan venni egy bírósági üzenetet, amely tanúkihallgatásról szól? Talán esetleg az, aki tudja, hogy ez csak postán és levélben érkezhet ;-)

Lassan valódi 50-es évekbeli feelingje lesz az internetes böngészésnek: akkor **mindenhol a gaz imperialisták kémeit kellett sejtenünk**, manapság pedig **mindenhol trójai és kémprogramot kell gyanítsunk**, sokszor sajnos nem is alaptalanul. A mostani csalás lényege, hogy **egy preparált weboldalon** azzal az ürüggyel, hogy a bírósági dokumentumokat megtekinthessük, le kell tölteni egy böngésző plugint (beépülő modult), ráveszik a látogatót egy kémprogram letöltésére. Innentől aztán - megfelelő antivírus program híján - már sima az út: **megszerzik a hozzáférést az áldozat számítógéphez**, adatokat és jelszavakat tudnak lopni, meg minden ilyesmi, ahol **éppen ez a "minden ilyesmi" elég rosszul hangzik**.

Nyilván kellett egy kis adatbányászkodás, és előtanulmány, **kiknek érdemes egy ilyet célzottan elküldeni**, és ezzel is növelni a hatékonyságot. A kevés számú kifejezetten IT profilú céget leszámítva valószínűleg Amerikában sem a cégvezetők a legparanoidabbak az ilyen fenyegetéseket illetően, tehát **az ürgebőrbe öltözött támadók láthatóan jól számítottak**.

Be prepared! - azaz Legyünk résen! - szól a régi cserkész mondás, ennél jobbat mi sem tanácsolhatunk a számítógép használóknak.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/426288

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.05.09. 19:41:59

Érkeznek is lassan a beszámolók:
index.hu/tech/biztonsag/whal060508/

Elsőnek lenni

2008.04.16. 14:04 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: security smart nod32 eset virustotal

Elsőnek lenni nem könnyű, nem is sikerül mindig, folyamatosan megtartani lehetetlen, állandó erőfeszítést igényel, de **azért néha vannak az életben pillanatok, amikor látványos jelet kapunk: megmérettettünk és nehéznek találtattunk :-)**

Kifejezetten egy **banki adatokat, név-jelszó párost lopó kémprogramról van szó**, a visszafejtett kódban tucatnyi weboldal és **pénzintézeti hivatkozás található**, bennük az elmaradhatatlan e-gold és a PayPal is szerepel.

A Win32/Spy.Agent.NFS kártevő első VirusTotalos elemzése április 10-én történt, és jól látható, **egyedül a NOD32-nek sikerült azt felismernie**. Ritka az ilyen látvány, sok esetben ugyanis az **egyes résztvevők érzékeny, de sok hamis riasztást adó heurisztikája bejelez**, ez most - valószínűleg az exe tömörítés hiányában - nem történt meg. Közismert jópofaság, amikor a száz százalékig **megbízható, vírusmentes Notepad.exe vagy a Calc.exe állományt összetömörítjük UPX-szel**, és a mezőny néhány tagja máris farkast - azaz trójait vagy vírust kiált.

Most, **hat nappal később már javult a helyzet**, a mezőny több tagja is helyesen és név szerint észleli és irtja.

Szóval nem PhotoShop trükköt láttunk, hanem a folyamatos víruslabor-munka és kedvező csillagállás együttes hatása volt a nem mindennapi látvány ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/427857

Kommentek:

Nincsenek hozzászólások.

Járt utat a járatlanért el ne hagyd!

2008.04.17. 14:31 | Csizmazia István [Rambo] | 1 komment

Címkék: apple wifi gps iphone hamisítás spoofing wps

Sokan vannak, akik **a kinyomtatott szöveget, a leírt betűt azonmód hitelesnek is gondolják**. Hasonló a helyzet azokkal az információkkal, amit csak azért hiszünk igaznak, mert hiszen a TV-ben vagy a rádióban mondták be. Nem jár rossz nyomon az, aki azért a gépekben, az általuk szolgáltatott adatokban **sem bízik meg teljesen vakon**.

Meghamisítható a Wi-Fi Positioning System (WPS) rendszer, amit az Apple iPhone, iPod Touch és más mobil készülékek is használnak a fizikai tartózkodási helyszín azonosításához. A módszer lényege, hogy ezek az eszközök **nem a GSM alapján már jól ismert és fejlettebb háromszögelés elvén működnek**, hanem SkyHook Wireless adatbázisát használják a meghatározáshoz a Symbianos Nokia telefonokhoz hasonlóan. Ilyenkor elmegy egy adott koordináta a lekérdezésben, amire **a válasz egy a listából kikeresett helyszín kódja** lesz.

A trükkhöz mindössze **egy laptopra, egy WiFi hozzáférésre és a WiFi hozzáférési helyszínek adatbázisának** egy példányára van szükség. Ezek birtokában egy adott Mac címről érkező azonosításnál **tetszőleges helyszín információk adhatók át az aktív WiFi felhasználói kéréshez** - állítja a zürichi kutatócsoport, és demonstrálták is a jelenséget.

Mivel az iPhone van olyan intelligens, hogy a GSM adatok alapján felülbírálná a helytelennek látszó WPS adatokat, ezért a kísérletben a GSM adatfolyamot is meg kellett szakítaniuk. Miután ezt megtették, sikerült elérni, hogy **egy zürichi iPhone egy 6300 km-re lévő New Yorki alagút pozícióját jelezze ki**.

Sőt nem csak az Apple iPhone volt átverhető ezzel a módszerrel, megismételték a manipulációt egy PC-vel is, amelyre a Loki plugin volt telepítve, és ott is sikeresen a földrajzilag teljesen idegen területre lehetett pozícionálni.

Nem függ össze az esettel, de köztudott, hogy a GPS eszközöknél is volt már többször különféle malőr, amikor a készülékek vírusfertőzötten kerültek az üzletek polcaira, és az első számítógéppel való összekapcsoláskor megfertőzték azokat. Hasznos szabály, ha minden használt és új készüléknél úgy járunk el, mintha ismeretlen - hiszen így is van - forrásból származna. Egy vírusellenőrzés - és/vagy üres adattároló esetén egy saját particionálás és formattálás - segíthet elkerülni az ilyen jellegű bajt. A helymeghatározás dolgában pedig

félő, hogy a kártevő készítők kedvet kaphatnak az ilyen típusú félrevezető támadásokra is.

Ha Murphy törvényt kellene fogalmazni a dologgal kapcsolatban, az valahogy úgy szólna, hogy **amit fel lehet törni, az fel is törik, illetve eltérítik és úgy manipulálják, hogy ne nekünk legyen jó a végén**.

Az okos kütyük használata jó, az okos kütyük használata szép, de emellett azért a józan észnek, és a térképnek a szerepe sem veszik el örökre. Gyaníthatóan **az ilyen eltérítéses trükkről nem most hallottunk utoljára**, hiszen ez most csak egy jószándékú bemutató volt.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/429753

Kommentek:

Csizmazia István [Rambo] • http://antivirus.blog.hu 2009.03.17. 10:09:29

Tájékozódni jó, tájékozódni szép, tájékozódni hasznos :-)
Például, hogy merre vannak ellopható fémtetők:

www.theregister.co.uk/2009/03/16/lead_roof_thief/

Adathalász technikák földön, vízen, levegőben

2008.04.21. 11:35 | Csizmazia István [Rambo] | 10 komment

Címkék: telefon scam bank email lopás csalás phising identity biztosító személyiség theft megtévesztés adathalászat

Sokan az adathalászatot komoly veszélynek tartják, míg **a személyiséglopás** fogalmát esetleg nem is értik pontosan, netán **lebecsülik annak jelentőségét** (én egy jelentéktelen szürke pont vagyok, mire mennének pont az én adataimmal, stb.). Pedig sokszor úgy **egymásbafonódik a két technika**, mint a Laokoón szoborcsoport, de hogy kiegészítik és segítik egymást, az senki számára nem lehet kétséges.

Ahogy a kártevő terjesztők igyekeznek minnél leleményesebben meglovagolni világpolitikai és más eseményeket: **zavargások Tibetben és Burmában, fejbelőtt nem létező álspammer, Bhuttó halála**; ugyanígy megvannak a szokványos adathalász módszerek, trükkök is, amelyek **kíváncsiságunkra, kéjvágyunkra vagy pénzsóvárságunkra építenek**. Nem sok ember lehet, aki egyik terület által sem környékezhető meg.

Az internetről (vagy kukabúvárkodással) megszerzett név, születési dátum, lakcím, e-mailcím, telefonszám aranyat ér a bűnözők számára, ennek ismeretében a **megfelelő social engineering érzékkel megáldott csaló vonzó ajánlattal, kecsegtető megkereséssel** jelentkezik. Persze a telefonkagylóba nem lehet beletuszkolni egy számítógépes kártevőt, de ez még korántsem jelenti azt, hogy ilyenkor nem fenyeget veszély bennünket.

Halló, itt a hivatal beszél

Az ajánlat lényege egy **nagy összegű életbiztosítás**, amihez az "ügyintéző" máris diktálja a hívott fél nevét, lakcímét és telefonszámát, és **"egyeztetésre" kéri bemondani az adószámot, illetve a társadalombiztosítási számot**. Egy másik módszer, hogy az adóhivatal nevében **adóvisszatérítést ígérnek**, ehhez is mindössze a társadalombiztosítási számot kell bediktálni, vagy rafináltabb esetben egy véletlenszerű számot (vagyis hibásat) olvasnak fel, és "egyeztetést" kérnek. Aki felháborodva "kijavíttatja" a helyes szám megadásával, biztos lehet abban, hogy adatai máris értékesítésre kerülnek, illetve segítségükkel valamilyen visszaélést fognak elkövetni. Ha a hívott fél nagy későn észbekap és rákérdez arra, hogy pontosan kivel is beszél, az esetek nagy részében **azonnal leteszik a telefont**.

Álbankár és álvízvezetékszerelő

Ne legyenek illúzióink. Amikor a csalók nálunk is sokadjára vetik be az olyan ósdi trükköket a szerencsétlen nyugdíjasok ellen, mint az **állítólagos hamis bankjegyek sorszámának ellenőrzése**, a vízvezeték állapotának felmérése oly módon, hogy elküldik őket a másik szobába falat kopogtatni, amíg ők zsebreteszik az értéktárgyakat és eltűnnek, a hasonló telefonos és e-mailes csalások is gombamód terjedni fognak - Fülig Jimmy őszinte sajnálatára. Egy külföldi bank hasonló esetéről már itt is írtunk egy tavalyi postban.

A vélt vagy valós kényelem mindig a biztonság ellen hat

Hancu barátom a közösségi portálokról szóló cikkében úgy fogalmaz: "*Hasonló automatizmus, amikor az oldal elkéri az emailcímünket és jelszavunkat (igen, ez elég rémisztően hangzik, csak megbízható, nagy oldalaknál játsszuk meg!), és a levelező szolgáltatónál levő címlistánkból gyűjti össze az ismerőseinket. A jobb oldalak 5-6 nagyobb ingyenes levelezőszolgáltatást is ismernek, ami egy újonnan regisztrált júzernek rengeteg időt spórol meg.*" Egy korábbi Hi5-ről szóló postban már beszámoltunk egy ilyenről, amikor a **személyes levelezési adatok megadásával elinduló levéláradat kellemetlen szituációba sodorta a gyanútlan netezőt**. Ki tudja, milyen gondosan kezelik ezt az adatot, pontosan kihez, és hány emberhez jut el a belépési kódunk, hogyan őrzik, a későbbiekben olvassa-e rajtunk kívül valaki a személyes levelezésünket, bevallanák-e, ha ellopnák tőlük az ilyen adatokat - **csupa-csupa nyitva maradt és nyugtalanító kérdés**. Jómagam úgy vélekedem, ahhoz, hogy én a máshova szóló accountjaimat bármilyen közösségi oldalon begépeljem, hát shanghai táncosnő legyen az öreganyám és baltával pucolja az ablakot.

Kételkedem, tehát vagyok

Azzal a tudattal persze nehéz a mindennapi életet élni, hogy **a levelek mindössze 10 százaléka hasznos, a többi vagy csalás, vagy kártevőt illetve spamet terjeszt**, ezért mindig ezzel a gondolattal nyitogassuk az elektronikus postánkat. Inkább az lehet a megoldás, ha **valaki intenzíven érdeklődik olyan adatok után, amihez semmi köze**, akkor kell(ene) megszólalni fejünkben a vészcsengőnek. Ahogy a bankok is állandóan hangoztatják, **sosem kérnek elektronikus levélben vagy telefon adategyeztetést**, azt kizárólag személyesen intézik. Azt készséggel elismerjük, hogy **nem egyszerű feladat** a hihető és hihetetlen között egyensúlyozva megtalálni a biztonságos lét aranyösvényét, különösen egy olyan világban, ahol a csalás már annyira bevett gyakorlat, hogy például a hétvégén román álrendőröket lőttek le Bécsben, akik magukat osztrák rendőrnek kiadva gyanútlan külföldi autósokat büntettek meg rendszeresen saját zsebre.

Továbbra se igyunk tehát mosatlan gyümölcslevet ;-) és **számítógépünkön használjuk rendszeresen frissített vírus- és kémirtó programot**. A fentiek fényében mellesleg a telefonnal sem árt vigyázni, a naív fiatalabbak és a gyanútlan idősebbek figyelmét pedig nekünk kell felhívni az ilyen jellegű veszélyekre.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/434917

Kommentek:

ViKtOr 2008.04.21. 12:50:24

Most kaptam, ide vezet:
natwalium.com/default.aspxrefererident=GH60917E554C671227F945LHC5726787123B5GG0E052K8&cookieid=189035&noscr=true/Login.html

Van értelme jelenteni valahol?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.21. 13:07:27

Szia ViKtOr!
A Phistank.com oldalon lehet jelezni az ilyeneket, magyar csalások és spamek esetében pedig a Nemzeti Hírközlési Hivatal az illetékes, ők tudnak eljárni.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.22. 07:04:43

Itt egy lehetséges adatfelhasználási veszély, ami _MINDENKIT_ érinthet:
www.penzcentrum.hu/cikk-1010691-1.html

Törölt felhasználó 2008.04.25. 11:41:40

Helló!
Van egy Robert Barr novella, "Szórakozottak vámszedői" a címe.
Kb ilyesmiről szól, mint amiről a cikkben írtál.

Szélhámosék újságban hírdetnek, hogy feledékenységre kínálnak kúrát, úgyhogy aki érintve érzi magát, az írjon egy adott címre, adja meg az adatait, szokásait és majd felkeresik a személyre szabott kezeléssel.
Egyik pofa ír nekik, kiteregeti magát és felkeresik valami nevetséges megoldással.
Nem sokkal ezt követően hogy-hogy nem beállít hozzá egy könyvügynök, aki borzasztó jutányosan egy könyvritkaságot kínál neki (mert imádja a könyveket, ezt meg is gyónta a szenilitást-kezelőnek). A kedvező üzlet megköttetik és azt követően még sok másik - RÉSZLETFIZETÉSSEL.

A csavar: ez a vállalkozás arra játszott, hogy először kipuhatolja a kuncsaftok gyengéjét, megnyerő modorú ügynökeik révén előáll valami csábos ajánlattal, a fizetés pedig roppant kedvező részletekben történik. De mivel ezek a kuncsaftok totál szenilisek, így addig fizetnek, amíg eszükbe nem jut, hogy már a sokszorosát törlesztették a megegyezés szerinti vételárnak.

Bocs, ha hosszúra sikerült, de annyira idekívánkozott.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.05. 17:02:03

Szia hErpEsz!

Bocsánat a késő reakcióért, nekem tetszett a történeted :-)

Én is amiatt jártam ezen az elárvult, kihalt folyosón, hogy idehelyezzek egy másikat ;-)
zugugyved.blog.hu/2008/08/05/elevult_fantomceg

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.04. 12:19:24

A tanárok Németországban sincsenek könnyű helyzetben:
oktatas.origo.hu/20081204/tanaralazas_a_neten
A más nevében való társkereső oldalra való feltöltés különösen durvoid.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.10. 17:37:00

Ahogy látom, sajnos már a magyar iskolákban is dívik a tanárok adataival való visszaélés:
www.szoljon.hu/jasz-nagykun-szolnok/bulvar/ket-tanar-es-harom-tanarno-fotoja-kerult-fel-egy-szexoldalra-210740

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.15. 10:37:58

Itt is egy tanulságos történet a személyazonossággal való visszaélésről:
mavfigyelo.blog.hu/2009/03/13/hiaba_a_jegyzokonyv_behajtokat_kuld_a_mav

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.24. 12:28:13

Mára már senki nem hiányolhatja a magyar eseteket:
www.origo.hu/itthon/20090324-a-prima-primissima-neveben-szaglaszik-valaki-bankszamlak-utan.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.23. 11:47:41

Ami ellen lehetetlen védekezni: a korrupt hivatalnok ügyféladatokkal él vissza:
www.penzcentrum.hu/cikk/1017461/1/lebukott_az_adoellenor_2000_ember_adataival_elt_vissza

Sanita ismerkedne - fotóval

2008.04.22. 12:21 | Csizmazia István [Rambo] | 1 komment

Címkék: spam email malware spyware csalás trójai kártevő kémprogram rita sanita

Mintha egy a Hírkereső portálon szereplő cikkről esne szó, úgy cseng a fenti - **figyelem felkeltésre kétségkívül alkalmas módon** - választott cím. Nem akarunk pesszimisták lenni, sőt még annak sem látszani, mert a nagybetűs Életben időnként azért ha ritkán is, de valóban kaphatunk önzetlen segítséget, barátságot, szerelmet. Azonban hogy ez **szinte sosem e-mailben érkezik ismeretlenektől**, nos erre akár mérget is vehetünk (lehessen ez esetünkben mondjuk Martini pezsgő ;-).

Ritka naivnak kell annak lennie, aki úgy gondolja, **merő véletlenségből úgy kapunk egy úszni és táncolni szerető 18 éves leányzótól ismerkedő levelet**, hogy még csak be sem jelentkezünk valamilyen társkereső portálra.

Gyakorlatilag ez azzal adekvát eset, mint amikor azon a lottón nyerünk, amelyre még csak szelvényt sem vettünk - piszok egy mázli, mondhatnánk erre :-) Akinek van türelme továbbolvasni a levelet, megtudhatja, hogy **Sanita a mamája szerint még viheti valamire a tánc területén, és később ilyen versenyeket szeretne majd nyerni**. Az e-mail címéből ítélve valószínűleg a motorozást sem veti meg...

Természetesen megvizsgáltuk Sanita ZIP fájlban megbújó photo.scr nevű "fotóját" is a VirusTotalon, ugye senkit nem lep meg az eredmény.

Még be sem fejeztük a postot, máris beesett egy még újabb levél, Ritától. És hogy **milyen érdekes a világ, Rita is pont úszni és táncolni szeret, naná hogy szintén 18 éves**, és készségesen tolja orrunk alá a fotónak látszó bitsorozatot. Az pedig már-már **szinte elképesztő, hogy Rita is a mamája szerint még ő is viheti valamire a tánc területén, és később ő is ilyen versenyeket szeretne majd nyerni**.

Elképesztő egy hasonlóság, sőt **ez már hiba a Mátrixban :-)** Kicsit a "Hogyan jutok el az Operába?" kezdetű vicc jutott az eszünkbe, és ennek fényében csak azt tanácsolhatjuk nekik, mint amit a vicc poénja is: "Csak gyakorolni, gyakorolni, gyakorolni..."

Statisztikai adatok szerint **mindig akad néhány százalék**, akiknek minden vicc új, akik mindent elhisznek, akik mindenre rákattintanak. Ha aztán náluk **nem csak fejben, hanem ráadásul az antivírus fronton és a Windows frissítések naprakészségének terén sincs minden rendben**, akkor ezzel sikeresen toborozták is az illetőt közlegénynek az Egyesült Botnet Hadseregbe ;-)

Vigasztalásul elmondjuk, azért igazi Saniták is léteznek, képünkön a Sanita ausztrál cipőgyár plakátja

A "hear from you soon" vagyis hogy még hallunk felőle színigaz. Mindenesetre sajnos vagy Hál'Istennek sok ilyen akció futószalagon adja a muníciót ehhez a bloghoz is. Azt hiszem, a legjobb heurisztikus tanácsunk az lehetne, ha **bármilyen női névvel** érkezik olyan levél, amelyben úszni, dancingozni - esetleg szimbolázni - szerető 18 éves ifjú hölgyek ajánlgatják fotóikat, ne dőljön be senki. **Ugyanez persze vonatkozik a baletttáncosokra és a kőfaragókra is ;-)**

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/436623

Kommentek:

Algernon 2008.04.22. 16:41:43

Teljesen össze vagyok zuhanva, én egyik hölgytől sem kaptam semmit, pedig spamileg mindig up-to-date vagyok...Hol lehet kérni? :)

Sztem a botnet hálózatot az avast üzemelteti, de minimum kölcsönös megnemtámadási szerződést kötöttek a rosszfiúkkal, oly következetesen ignorálják ezen file-okat. :)

A Photoshop is sebezhető

2008.04.23. 18:30 | Csizmazia István [Rambo] | 8 komment

Sőt, **nem is ez az első alkalom**, volt már korábban is néhány eset, például tavaly, **amely puffertúlcsordulási hibát okozva** a Highly critical kategóriába soroltan került fel a Secunia oldalára.

A mostani hibára Scott Laurie hívta fel a figyelmet, ahol **egy preparált BMP állomány segítségével az Adobe PS CS3-ban kártevőt lehet a rendszerbe injektálni**. A módszert be is mutatta egy Windows XP SP2 alatt futó Photoshop Album Starter Edition 3.2 programmal.

A szokásos közhely biztosan alkalmazható: a hiba kijavításáig **csak megbízható forrásból származó** képállományokat nyissunk meg PhotoShop programunkkal ;-)

És persze sajnos arra is számíthatunk, hogy **megkezdődik a fertőzött képfájlok küldözgetése a kéretlen levelekben** is.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/438776

Kommentek:

rszarvas · **http://rszarvas.blog.hu** **2008.04.23. 22:25:04**

A CS3 alapvetően tele van még hibával, hiszen viszonylag új. Soha nem jutna eszembe a megjelenés évében, vagy az azt követően szoftvert venni. Sajnálom is azokat, akik gyorsan beleugrottak a tutiba. Szerintem felelőtlenség.

TBC 2008.04.24. 01:39:44

Fertőzött képfájlok küldözgetése... Háát (tudom, hát-tal nem kezdünk mondatot), szerintem ezek 99,9%-át nem Photoshop-pal fogják megnyitni, és nagy részük soha nem kerül fertőzési helyzetbe. Meg a védelmi szoftverek is fel fogják ismerni, szóval annyira nem gyászos a helyzet...
rszarvas: azért kicsit túl óvatosság ez, nem? Akinek most van rá szüksége, az nem fog a megjelenés után még másfél évet várni, csak azért, mert új a szoftver. Felelőtlenség? Nem az. Le merem fogadni, hogy napokon belül kijön egy patch, ami orvosolja a problémát. És azért 2-3-4 éves szoftverekben is jócskán lehetnek hibák. Azokat sem nagyobb felelőtlenség használni...

nevetőharmadik 2008.04.24. 07:30:01

TBC: azért kevés olyan szoftver van (pláne Photoshop kaliberű), amiben egy következő verzió annyival többet tud, hogy nem lehet nélküle élni. ' év mondjuk lehet, hogy tényleg sok, legyen fél, de akkor sem feltétlen túlzás.

Gery Greyhound · http://www.bestofgyurcsany.hu/news.php 2008.04.24. 07:45:58

"l egy preparált BMP állomány segítségével az Adobe PS CS3-ban kártevőt lehet a rendszerbe injektálni (...) a hiba kijavításáig csak megbízható forrásból származó képállományokat nyissunk meg"

Vagyis csak megbízható forrásból származó BMP fájlokat, gif,tif, jpg, png ezek szerint nem okozhat bajt. Mást meg szerintem manapság nem nagyon használ senki...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.26. 09:29:33

Hello Rszarvas!
Nem ismerem közelebbről a PS-t, Paint Shop Pro és Gimp használó vagyok. Azt azért jól láttam, hogy a különböző programok aktív használói mindig is tűkön ülve várják már az új verziót és rögtön fejest is ugranak bele.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.26. 09:32:40

Hello TBC!
Valószínű, hogy minden gépen lesz a képfájlokhoz társítva a PS automatikus megnyitásra, de elvileg ez az eset sem kizárt, és nem lehetetlen az sem, hogy valaki később egy emailből lementett képet PS-sel megnyisson. Szóval abban igazad van, hogy nem tömegesen, de azért szórványosan lehet így benyelni ezt-azt.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.26. 09:38:50

Szia Nevetőhatmadik!
A kérdés nem úgy vetődik fel, hogy az új verzió ficsőrei nélkül "nem lehet élni", hanem hogy "érdemes-e anélkül élni" ;-)
Például SwishMax user vagyok, és rögtön frissítek és azonnal használok minden újdoncságot.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.04.26. 09:41:22

Üdv Gery Greyhound!
Megbízható állomány esetleg az, amit magam készítettem. A többinél sosem lehetsz biztos...
Meglepne, ha nem készülne később preparált PNG, TIF stb is :-(

Ethical Hacking konferencia 2008

2008.04.25. 21:21 | Csizmazia István [Rambo] | 1 komment

Tegnap volt a nagy nap, **a Netacademia rendezésében** az Arena Plaza 14-es mozitermében gyűltek össze a téma iránt érdeklődők, és sikerült egy teltházas programot összehozni. **A színvonalas előadásokra és szakmai bemutatókra zsúfolásig megtelt a lelátó**.

Fóti Marcell köszöntője után **Rajive Kapor Londonban élő biztonsági szakember** tartott érdekes előadást a hackelési célpontokról, a **vállalati auditokon tapasztalt hajmeresztő furcsaságokról**. Jópofa sztorikkal fűszerezte angol nyelvű előadását, amely aztán picit túlnyúlva az eredeti időkereten, minden további műsorszámot odébbshiftelt pár perccel.

Fóti Marcell az Ördöklakat projekt kapcsán mutatott érdekes hackelési megoldásokat, itt az SQL injection és a Cross Site Scripting volt a végletekig kivesézve és szemléletesen demózva.

Helycserés támadással **Deim Ágoston (Ago) lépett a pástra Linux polóban :-)** és előadásában **hálózati protokollokat és azok gyengeségeit taglalta**, az érdekesebb lépéseket egy Cisco routerrel demonstrálta is élőben.

Ezt követte **Rideg Márton MKB szakember előadása, aki az informatikai rendszerek üzemeltetéséhez adott megszívlelendő tanácsokat**, valamint bemutotott egy **MIMT azaz Man In The Middle támadást** percek alatt letölthető programok segítségével.

Az ebédszünet után **Baki Gábort hallgathattuk meg, aki utánozhatatlan és szórakoztató stílusban a WiFi rendszerek biztonságáról értekezett**. Volt itt szó wardrivingról, WEP és WPA törésről, és tanácsokat kaptunk arra nézvést is, hogyan tehetjük biztonságosabbá vezetéknélküli hálózatunkat. Ha valaki ilyet akar, akkor a Radius szerver a kulcsszó.

Novák Zsolt a Social Engineering témakörben foglalt össze minden olyan körülményt, amely az informatikai biztonságot gyengítheti. Szemléletes, jó humorú példái találóan illusztrálta azt a módszert, amellyel csupán emberi megtévesztéssel hihetetlen sikereket lehet elérni.

Ezek után **Csiszér Béla (Sicontact) lépett az emelvényre, és a rootkitekkel kapcsolatban igen szemléletes előadást kaphattunk olyan kereskedelmi forgalomban megjelent csalárd DRM védelmekről**, melyek rejtett rootkit segítségével, a felhasználó tudta nélkül orvul elképesztő rendszer módosításokkal, **korlátozásokkal büntetik a legális vásárlót**. Egy újfajta veszélyről is beszélt, **a Master Boot Recordban terjedő Mebroot kártevőről**, amely vélhetően még sok kellemetlenséget fog okozni a felhasználóknak.

Végül, de nem utolsósorban **Rózsahegyi Zsolt következett Netlock szinekben, és a hitelesítés valamint az SSL kommunikáció meghamisításáról** tartott egy érdekes bemutatót. A már korábban emlegetett **MITM támadási mód itt is színrelépett, és sajnos igen hatásosan volt képes hamisított tanusítványt** felvonultatni.

Összességében **nagyon színvonalas előadásokat élvezhettünk**, a hébe-hóba felmerülő kérdéseknél finom üveg borokkal jutalmazták a helyes választ adó nagy érdeműt, a program pedig a **Kevin Mitnickről szóló film, a Takedown vetítésével zárult**.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/442245

Kommentek:

zvaragabor 2008.04.26. 16:05:44

Én is voltam, nagyon jó volt. Csiszér Béla előadása kapcsán taéán meg is veszem a zene cédt az ominózus rootkittel :)

Apád, anyád ide... izé mégse jöjjön

2008.04.28. 14:09 | Csizmazia István [Rambo] | 1 komment

Avagy **milyen szempontok szerint válasszunk** magunknak biztonsági programot? Arról, hogy **hogyan ne, elolvashatjuk** a tanmesét **az Anyádat** cikkében.

Mindenki igyekszik számítógépe biztonságát valamilyen helyes, ügyes programra rábízni, és ennek kiválasztásához **sokan letöltési oldalakat** böngésznek.

Vannak olyan oldalak, ahol a szerkesztők alaposan megnézik, mit töltenek fel, mit ajánlanak az embereknek, ne adj' Isten még feltöltés előtt vírusellenőrzik is az adott csomagot, sőt **állítólag már láttak olyan embert, aki látott olyan embert, aki előtte kipróbálta a programot**, mielőtt a feltöltések közé helyezte volna.

Így volt, nem-e, nem tudhatjuk, magyar lapok között például színvonalasnak tartjuk a Honosítóműhelyt, **ahol a letöltésekhez fórum, vélemény nyilvánítási lehetőség is tartozik**, így már a letöltés előtt is lehet némi fogalmunk, körülbelül mire számítsunk majd a használatnál.

Megvizsgálva **a telepítő fájlt a VirusTotallal**, ezt az eredményt kapjuk. De a **csaló programok nyilvántartásában sem kell sokat kutakodni**, hogy rábukkanjunk: már a domain foglalás és megjelenésének hónapjában, 2007 decemberben feketelistára került. Remélem nem tűnik túl rasszistának a kijelentésem, de ha **olyan védelmi porgramot tervezünk telepíteni**, aminek weboldalát az EST Media adja, pláne ha ez mindössze csak pár hetes, vagy pár hónapos bejegyzés - nos **ez már önmagában legyen egy intő jel**. Tudomásul kell venni, a **csalárd vírus- illetve kémirtó programok** is hozzátartoznak a megtévesztéshez, ezért kell megfontoltan ilyesmit választani.

Ha **több fórumban is dicsérik, nem szerepel a csalárd programok listáján, megbízható support, többévi megbízható cégtörténet és pontos elérhetőség társul hozzá, szép eredmények a független teszteken**, akkor szavazzunk csak bizalmat a programnak. Sajnos nem találtam meg az eredeti hírt, de **a napokban olvastam egy vicceset**. Egy üres csomagot próbaképpen elküldtek 200 shareware és freeware letöltési oldalnak. A zombi droid módra üzemelő CTRL-C CTRL-V helyek (kb. 80%) azonnal felvették, 50 helyen **még a szerkesztők ajánlatában is szerepelt**, és 15 helyen még a saját kategóriájában díjat is nyert - nos ennyit az alapos munkáról. (Ha esetleg valaki megtalálja az eredeti cikk linkjét, nagyon megköszönném ha egy kommentben megírná, hol is volt ez pontosan. Egy korsó sört tudok érte felajánlani a Hacktivity 2008-on.)

Ha **már a Googleban rákeresve az első oldal is csak a "hogyan szabaduljunk meg..." típusú találatoktól hemzseg**, úgy botorság fejest ugrani a telepítésbe...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/445313

Kommentek:

Algernon 2008.05.06. 10:41:51

Egy virtuális pc-re feltelepítettem ezt a kémprogramkeresőt, mellé winantiviruspro vírusirtót, nagyon szépen megy mindkettő...:)

A magánnyomozó sem kémkedhet

2008.04.30. 13:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: börtön büntetés spyware kémkedés kémprogram

Sokak által vitatott a határ a tisztességes és tisztességtelen közötti keskeny mezsgyén. Egy bizalmon alapuló párkapcsolatban **visszásnak tűnik, ha az egyik fél titokban kémkedik a másik után**, orvul elolvassa e-mailjeit, SMS üzeneteit. Ugyancsak sokaknak lehet kényes téma a gyerekek számítógép használatának szülők általi felügyelete. Egy biztos: **aki titkon kémprogramot telepít, az bűncselekményt követ el és akár börtönbüntetés elé is nézhet**.

Nincs ez másként a magánnyomozók esetében - vagy fogalmazhatunk úgy is, aki ilyen ügyetlenül intézi, hogy kiderüljön ;-) - **sem engedélyezettek az illegális módszerek**. A minap **tartóztattak le négy izraeli magándetektívet, akik kereskedelmi információk megszerzésére használtak trójai kémprogramokat Londonban**. A Michael és Ruth Haephrati által készített kártevő , melyet illegálisan számos cégnél, többek közt a HOT kábeltelevíziós, illetve az Audi és VW autók kereskedelmével foglalkozó cégekkel kapcsolatban használták bizalmas kereskedelmi adatok gyűjtésére. A cselekményt a hatóságok több hónap börtönbüntetéssel honorálták. Érdekes momentum az ügyben, hogy a detektív irodának nem először gyűlt meg a baja a törvénnyel: **a korábbi cégvezető elmenekült egy hasonló eset elől, ahol vétkesnek találták és amit végül csak 90 ezer USD büntetés befizetése mellett úszott meg** feltételes szabadlábra helyezéssel.

Bár az **természetes, hogy a vállalatok élénk figyelemmel követik versenytársaik lépéseit**, de a konkurrencia elemzésen túl illegális módszerekkel operáló cégek megbízása már túlmegy a megengedhető és tisztességes határán. Ilyen **illegális mód többek közt a lehallgatás illetve a számítógépes kémprogram telepítése**.

Az igen csekély számú lelepleződött és büntetéssel végződött spyware eset közül **erősen hiányoljuk a túlbuzgó munkaadók - sok esetben multicégek - saját dolgozóik ellen használt illegális megfigyeléseit**. Reméljük, a jövőben ezek az esetek sem maradnak büntető következmények nélkül.

Lassan **szinte hidegháborús állapotok** vannak: mindenki figyel, támad mindenkit, és nem igazán reménykedhetünk javulásban. Az éppen egy évvel ezelőtti Orosz-Észt kiberkonfliktus ráirányította a figyelmet arra, hogy aki nem képes védekezni, az elveszett. Ezek után az sem meglepetés, hogy a közelgő olimpiára is extra figyelem irányul - mindkét részről. A jövőben pedig sok országban már külön fegyvernem lesz az állami hackercsoport.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/448185

Kommentek:

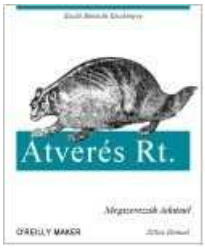
Nincsenek hozzászólások.

Hívjuk fel a bankot - kérik az e-mailben

2008.05.05. 12:08 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: voip telefon kód scam bank email csalás pin kártyaadatok oreilly

Lassan már érdemes lenne egy külön O'Reilly keményfedeles könyvben kiadni a "**Tippek-trükkök csalóknak és kezdő bűnözőknek**", vagy az "**1001 furmányos e-mail minta, amire mindig lesz elegendő számú beugró balek**" című kézikönyvet. De az is sikerre számíthat, aki csak a Donald Kacsás képregényeket forgatja.



Egy évekkel ezelőtt megjelent IPM magazinban volt egy eset, hogy valaki **egy Donald képregényben látta a trükköt**: egy üres papírdobozt kell a bank bejáratára akasztani *"Elnézést, technikai hiba miatt átmenetileg a befizetendő összegeket az automata helyett kérjük dobja egy borítékban a dobozba, és 2 órán belül garantáltan fel lesz dolgozva."* felirattal. **Emberünk a valóságban is megcsinálta a dobozt és a papírt**, és lássunk csodát, alig félóra alatt **sikerrel kaszált pár ezer akkori német márkát** egy müncheni banknál.

Mostani e-mailes történetünk kapcsán sokadszor ismételjük, sőt lassan mondjuk, hogy mindenki jól értse ;-) alapesetben **a bankok sosem (no never) kérnek adategyeztetést e-mailben**, sőt visszahívást sem kérnek - ennél azért több pénzt beszednek tőlünk, hogy még ezt is ránk hárítsák. Tavaly év végén már felhívtuk a figyelmet a jelenségre, de úgy tűnik, a napi rohanásban még mindig nem mindenkinek esik le a tantusz, **miért is kérne be a bank PIN kódot egy ügyféltől**. Ha valaki van olyan vigyázatlan, és mégis visszahívja a megadott számot, ott **a hamis ügyfélszolgálat megkérdezi a PIN (Personal Identification Number) kódját, a társadalombiztosítási-számát, a születési adatait, bankszámla-számát és lejáratát** esetleg az útlevél sorszámát, dátumát. Ezek (vagy egy részük) birtokában a csalók már sok mindent megtehetnek.

Bankkártya számmal, lejárattal és a háromjegyű ellenőrző kóddal tetszőleges kártyás vásárlást indíthatnak, bár itt még használható védelem, hogy először csak zárolásra kerül az összeg, és csak ezután vonják le a valóságban. A PIN kóddal pedig szabadon felvehetik akár minden pénzünket. De a személyes adatok is elegendőek lehetnek egy új bankszámla nyitáshoz, hitelkérelem beadásához, autóbérléshez vagy állami segély iránti kérelem benyújtásához - **természetesen anélkül, hogy egyáltalán tudnánk ezekről a lépésekről**. Ez az, amitől a legjobb vírusirtó vagy kémprogram-ellenes szoftver sem védhet meg: ha mi magunk figyelmetlenek, óvatlanok vagy felelőtlenek vagyunk.

Ennél egy fokkal már hajmeresztőbb a Homár cikke, ahol látszólag egy mobiltelefon vásárlás alkalmával lemásolt személyi igazolvánnyal és az ott megszerzett személyes adatokkal élt vissza egy alkalmazott, kis híján itt is a pénze bánta a naív ügyfélnek. Biztos, hogy Péterfalvi Attila **ellenzi elvben**, hogy a **személyinket lemásolják a gyakorlatban** - ahol ki tudja, mennyire megbízható módon tárolják, másolják vagy vesztik el ezeket - **mégsem történik változás, mégsincs felelőse** az ilyen rossz gyakorlatnak, ma is csak ugyanígy lehet mobiltelefonhoz jutni. Lehet tudni, hogy ezek után miért nem változik semmi? Talán emiatt a "**következmények nélküli ország**" cimke

miatt tartunk ott az elektronikus kereskedelemben, ahol tartunk: Ghana és Indonézia között.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/454534

Kommentek:

Nincsenek hozzászólások.

Mozizzunk rovat: kémprogram a mobilban

2008.05.05. 21:02 | Csizmazia István [Rambo] | 16 komment

Címkék: mobil telefon mms sms spyware gsm kémprogram mikko hypponen

Sok kommentár nem szükséges a filmhez, **a képek magukért beszélnek**. Akár hétfő esti horror filmnek is beillik. Aki eddig nem ismerte, annak garantáltan meglepő és szemléletes lesz.

Egyik kedvencem, az F-Securos Mikko Hypponen mutatja be, **milyen az, amikor egy galád kémprogram fészkeli be magát egy GSM telefonba**. Minden fogadott és küldött SMS, MMS üzenetről másolatot kap a kém. Figyelem: durvoid képsorok, csak erős idegzetűeknek ;-) , 18-as karika rulez!

http://www.youtube.com/watch?v=hQk8mmrbW-8

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/455536

Kommentek:

Skeptical 2008.05.05. 22:32:18

En nem ertem igazan, hogy ebben mi az extra. Siman lehet olyan programot irni, ami "lathatatlanul" forwardolja az smseket egy masik telefonra is. Ez most mitol ujdonsag vagy mitol veszelyes? Hogyan terjed ez a szoftver, latszik-e a szamlakimutatasban a masik sms, amit kuldott? Persze biztosan van realis veszely a mobilokban is, en csupan ezt a demot erzem kicsit erotlennek.

SUNexecutive · http://nezo.blog.hu 2008.05.05. 22:41:44

Csak néhány szó....reális veszély MÉG nem létezik. Pont. (Egyszerűen, akinek van pici rálátása a Symbian rendszerekre, az tudja, hogy még(!!!) túl egyszerű.)

HMS.NAGYSZINPAD 2008.05.05. 22:46:16

szerintem ebben a témában egy 2 éves videó öreganyám frissességével vetekszik.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.05. 22:54:56

@mindenki:
Sorry, de most idézek saját magamtól: "..Aki eddig nem ismerte, annak..." Szóval nem igértem, hogy feltaláltam a spanyolviaszkot ;-)
A filmből (emi csak nekem volt új) nem derült ki, pontosan mit használtak, de aki már látott ilyet élőben, írhatna pár szót róla.
Én ezt a címet ismerem:
www.flexispy.com/
Ez Symbian és Window Mobile alatt teszi a dolgát.

autosave 2008.05.05. 23:33:23

de van winmobile is, nem csak symbian
szóval létezik? :D

...0 .. 0... · http://wece.blog.hu/ 2008.05.05. 23:59:35

esetleg berakhatnád beágyazva, és akkor nem kéne elmenni a jutyúbra megnézni
és kiszedhetnéd a caphát a bejelentkezetteknek
admin felület, t'od! ;)

atleta.hu · http://www.atleta.hu 2008.05.06. 03:21:50

Rambo: de akkor mi ebben az ijeszto? Ez a szoftver csak akkor mukodik symbian alatt, ha telepited. Ahhoz 3-4x ra kell nyomni, hogy igen, akarom. Azt is megkockaztatom, hogy ez meg nem is eleg, es kell hozza egy megfeleloen eros alairas, amihez viszont at kell hajtani a cuccot a symbian signed nevu eljarason, aminek a kereteben szepen atvizsgaljak, hogy mit is csinal. Es ott elverzik az egesz.

Es ezzel vitatkoznek Helioport allitasaval, es nem feltetlenul azert nem lehetsegesek ilyen szoftverek, mert tul egyszeru a symbian, hanem azert, mert elegge kezben van tartva (platform security) es mert az alapoknal elegge figyeltek arra, hogy bizonyos egyszeruen kihasznalhato hibak ne fordulhassanak elo. (Persze a komplexitas novekedese szepen lassan nyitogathat varatlan lyukakat, es ha erre gondoltal, akkor sorry.)

atleta.hu · http://www.atleta.hu 2008.05.06. 03:23:24

Ja, megvalami - az F-Secure hosszu evek ota probal hisztit kelteni mobil virus temaban. Szeretnek mar eladni a mobil antivirus termekuket nagyon. Meg akkor is, ha nincs piac.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 06:56:08

@Sketical:
Arra én is kíváncsi lennék, hogy a részletes számlában mi látszik és mi nem :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 07:04:14

@atleta:
Ha jól emlékszem kb. 2000 óta kínálgatják az FSAV-ot mobil platformra. Ha nekem lenne ilyen készülékem, én sem szaladnék megvenni, ráér majd ha itt is napi többezer mintát küldenek majd a víruslaborba ;-) A Symbian R3 pl. a digitálisan aláírt telepítésekkel alaposan leszűkítette a valódi veszélyeket, ezért az ilyesmit én is inkább csak érdekesnek gondolom.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 07:20:29

@megmondo:
Elvileg mindkettő létezik.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 07:25:22

@Atleta:
Teljesen igazad van, a telepítési nehezségek miatt szerintem sem okozhat reális és széleskörű veszélyt, én is inkább csak szórakoztatni akartam a bemutatásával. Úgy vélem, ha a helyzet később megváltozik (pl. napi 5-10 iPhone kártevő hull az égből), majd az ESET is megjelenhet valami termekkel, de most szerintem ők sem tartják időszerűnek az ilyesmit.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 07:29:05

@Pepepe:
Megpróbáltam közvetlenül is belinkelni, de beszólt, hogy "This video is no longer available...", nekem meg most nem volt kedvem pepecselni :-) Sorry

fabatka 2008.05.06. 09:03:19

Rambo: amire te gondolsz az nem Symbian R3, hanem S60 3.0. A Symbianban a platform security a 9.0-ás verziótól jelent meg, ami a Nokiáéknál az S60 3.0-nak felel meg.

Helioport: szerintem aki ismeri a Symbian rendszereket, az még véletlenül sem mondaná, hogy túl egyszerűek lennének. Arról nem is beszélve, hogy a vírusok, vagy más rosszindulatú programok megléte egyáltalán nem attól függ, hogy egyszerű vagy sem egy rendszer. Gondolj csak a DOS-ra, ami a Symbian rendszereknél lényegesen egyszerűbb volt mégis rengeteg vírus készült rá.

Skeptical: amennyiben a számlakimutatásodban látszanak a küldött SMS-ek, akkor ebben az esetben is látszani fog, hiszen ugyanaz történik, mintha saját magad küldted volna. A telefonon természetesen megoldható, hogy ezek ne jelenjenek meg a küldött SMS-eknél.

A videó pedig csupán annyit mutat be, hogy lehet írni olyan programot, ami a kimenő és bejövő sms-eket elkapja és képes sms-t küldeni (ami egyébként nem is olyan bonyolult). Mivel egy programozható telefonról van szó, az, hogy SMS-t tud kapni és küldeni nem egy meglepő dolog.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.06. 12:03:06

Szia Fabatka!
Köszi a kiegészítéseket :-)
Úgy gondoltam, hogy mivel nagyon sok, és meglepően kis méretű Symbianos telefon létezik, valós veszély lehet egy féltékeny férj, gyanakvó főnök, aki egy ilyen cuccot titokban rátelepít valakinek a telefonjára, aki nem szakember. Ez - szemben a még kevéssé létező, ritka mobilvírusokkal .- igenis valódi veszély lehet.

fabatka 2008.05.06. 12:19:30

Persze, hogy valódi veszély, de kb. ahhoz hasonló, hogy a férj átirányíthatja a feleség e-mailjeit saját magának is :)

Magyar kártevő toplista - 2008 április

2008.05.08. 10:14 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

A NOD32 antivírus rendszer gyártója, **az ESET havonta elkészíti a legelterjedtebb internetes kórokozók top tízes listáját**. Nézzük akkor, **milyen hónapot is zártunk áprilisban Magyarországon**! Következzen a **NOD32 antivírus rendszert gyártó ESET ThreatSense.NET Center** felmérése.

A vírusstatisztika **alapját a vállalat ThreatSense.Net vírusfigyelő rendszere képezi**, amely a NOD32 felhasználók önkéntes adatszolgáltatásának köszönhetően **az e-mailekben terjedő vírusok mellett a böngészés közben a számítógépekre került kórokozókat is listázza** és ezt országokra lebontva is le tudjuk kérni, így módunk van rá, hogy **a havi toplista teljes egészében a magyarországi észlelésekre alapozva** jelenhessen meg.

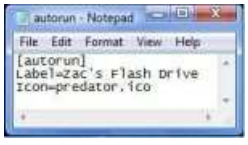
A listán szereplő tételek minden esetben konkrét károkozókat jelölnek, az eredeti listában található csak gyanítható, de egyértelmű azonosításra nem alkalmas észlelési adatokat nem vettük figyelembe. **Lehetőség szerint igyekeztünk a legtöbb kártevő mellett feltüntetni a weboldalunkon található részletes vírusleírásra mutató linkeket is**.

Íme a lista!

1. Win32/Adware.Virtumonde.FP application (10.29%)
Ez a kártevő szintén **a Kéretlen alkalmazások táborába tartozik** az ESET kategorizálása szerint. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában (alapértelmezés szerint C:\ Windows\ System32) véletlenszerűen generált névvel fájl(oka)t hoz létre, melyeknek kiterjesztése .dll. A trójai **megkísérel egy távoli szerverhez csatlakozni**, és onnan további komponenseket letölteni.

2. Win32/Adware.Virtumonde application (9.78%)
A Virtumonde (Vundo) program a Kéretlen alkalmazások (Potentially Unwanted) kategóriába esik, készítői arra használják, hogy **segítségével kéretlen reklámokat másoljanak a felhasználó PC-jére**.

3. INF/Autorun virus (2.24%)
Az INF/Autorun egyfajta gyűjtőneve **az autorun.inf automatikus** programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.



4. JS/TrojanDownloader.Iframe.EY.gen trojan (1.94%)
A HTML oldalaknál komoly veszélyt jelent az olyan **JavaScript kód észrevétlen beszúrása**, amely az Iframe segítségével kártékony tartalmakat tölt le titokban a látogatók számítógépeire. Ez a kártevő ebből a fajtából való EY jelű variáns.

5. Win32/VB.EL worm (1.74%)

A VB.EL (vagy más néven VBWorm, SillyFDC) féreg **hordozható adathordozókon és hálózati meghajtókon képes terjedni**. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is.

6. Win32/Toolbar.MyWebSearch application (1.71%)

Az Internet Explorer és Firefox alatt működő keresőszolgáltatás. Telepítésekor számtalan Registry kulcsot módosít, és **kéretlen reklámokat jelenít meg az adott számítógépen**. Az alkalmazás figyeli a felhasználó böngészési szokásait és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kliens kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

7. Win32/Adware.AdMedia application (1.50%)

Windows rendszereken terjedő kéretlen reklámprogram. **A megtámadott számítógépbe beépülve különböző kártékony DLL állományokat hoz létre, illetve tölt le az internetről**, a Registry adatbázisba pedig olyan bejegyzéseket készít, amellyel gondoskodik arról, hogy a kártékony kód minden rendszerindításkor automatikusan lefuthasson. Működése során több különböző kártékony weboldalhoz is megpróbál kapcsolódni, és a megfertőződött rendszer a tulajdonos tudtán kívül képes más weboldalak ellen indított DoS támadásban is részt venni.

8. Win32/CMDOW.143 application (1.46%)

A cmdow.exe állományra sok antivírus program nem jelez, hiszen nem vírusról, hanem egy hacker eszközről van szó. **A Cmdow egy olyan parancssori segédprogram**, melynek segítségével Windows NT4/2K/XP/2003 rendszereken kilistázhatjuk, átmozgathatjuk, átméretezhetjük, átnevezhetük, illetve elrejthetjük vagy ismét láthatóvá tehetjük, minimalizálhatjuk vagy kinagyíthatjuk, helyreállíthatjuk, aktiválhatjuk illetve inaktiválhatjuk, továbbá bezárhatjuk, leállíthatjuk az ablakokat. Az eredeti cmdow alkalmazás egy 31 KB-os végrehajtható fájl, amely nem ír a Registrybe, nem igényel külön telepítést, elég lefuttatni. Eltávolításához elegendő ezt az állományt törölni.

9. Win32/Adware.PlayMP3Z application (1.40%)

Ez az alkalmazás a kéretlen és felesleges alkalmazások körébe tartozik. **Kéretlenül reklámokat jelenít meg, MP3 tartalmakat és lejátszóprogram komponenseket tölt le**. Automatikusan nem képes terjedni, ehhez szüksége van felhasználó közreműködésre is. Az elemzése alapján feltételezhetően Kínából származik.

10. Win32/Obfuscated.A1 trojan (1.30%)

Az Obfuscated (összezavart kódú) elnevezés egy olyan általános kategória, amellyel számos fájl már proaktívan felismerésre és eltávolításra kerül, amelyek gyanús technikákat használva igyekeznek kibújni az antivírus vizsgálat elől. Az ilyen állományok többsége reklámprogramokkal (Adware) ellátott alkalmazások telepítő csomagjaiból származnak, mint amilyen például a korábban is említett Virtumonde. **Futása közben kéretlen reklám ablakokat jelenít meg**.

Ezek **tizen adják az összes észlelés 33.36 százalékát**, vagyis a további megközelítőleg 66 százalékon már sok, kisebb arányban előforduló kártevő osztozik.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/459512

Kommentek:

Nincsenek hozzászólások.

Gyermekeink védelmében

2008.05.09. 13:30 | Csizmazia István [Rambo] | 1 komment

Címkék: internet pedofil csalás védelem közösségi oldalak kártevő

Komoly lépéseket terveznek a közösségi oldalakon előforduló káros jelenségek ellen Facebook és a MySpace üzemeltetői. A veszélyek közül nemcsak a vírusfertőzések és csalások elleni küzdelmet, de az etikátlan hirdetések, **kéretlen és kémkedő reklámok, szexuális és egyéb bűnözők elleni** hatékonyabb fellépést is szorgalmazzák.

A tervek szerint ilyen lépéseket fontolgatnak a fiatal korosztály védelmében:
- a céges szolgáltatások adatkezelési gyakorlata legyen biztonságos és betartott
- a dohány és alkohol hirdetéseket tartsák távol a fiatalkorúaktól
- a nemkívánatos csoportokat (öngyilkosságra bátorító, vérfertőzéssel vagy pedofíliával kapcsolatos, terrorista és egyéb törvényileg vagy etikailag kifogásolható) haladéktalanul távolítsák el

Technikailag mindenesetre nehéz elképzelni, hogyan ellenőrizhető valaki, hogy csak a valós életkorát gépelhesse be. Arról nem is beszélve, ha a rendszer csak azt figyeli, a gyerekkorú (vagy ilyen adatokkal bejelentkező) ne adhasson ki figyelmeztetés nélkül személyes adatot felnőttkorúnak, **ez korántsem tökéletes**: hiszen ehhez elég a pedofilnak magát gyerekkorúnak regisztrálni (a beszámolók szerint éppen ezt szokták tenni), és máris megkaphatja a másik fél adatait.

A részletesebb adatok ismeretének hiányában úgy látjuk, a megalkotandó szabályozás nem lesz tökéletes és kijátszhatatlan - mert hogy ilyesmi nem létezik - de talán kijelöli az utat, merre érdemes figyelni, szigorítani, ellenőrizni, naplózni - és legalább megpróbálnak valamit tenni, ami méltánylandó.

Végül ha még azt is sikerülne elérni, hogy mindenki naprakészen frissített operációs rendszer, valódi kétirányú tűzfal, valamint vírus- és kémprogram elleni védelem mögött üljön, ez nagy lépés lenne a kártevőmentes internetezés felé. Amiben **az antivírus cégek tudnak segíteni**, az például a kedvezményes diáklicencek biztosítása.

Egy biztos: a **biztonságos internetezésre való nevelés, oktatás** a legfontosabb és leghasznosabb, amit gyermekeinknek átadhatunk.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/461189

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.08.03. 09:44:30

Nem csak elektor kalandorok, hanem igazi hiénák is indulnak a versenyben :-(
hvg.hu/itthon/20090803_gyerekmodellek_portfolio_casting.aspx?s=hk

Azok az átkozott következmények

2008.05.13. 14:49 | Csizmazia István [Rambo] | Szólj hozzá!

Régebben a klasszikus vírusok időszakában egy fertőzéssel **egy vagy több állományunk megváltozott, megsérült esetleg megsemmisült**. Később aztán az olyan kártevők, mint például a Sircam, **egy véletlenszűren a számítógépben levő dokumentumunkat vitte magával**, és ennek illetéktelen kezekbe vagy nyilvánosságra kerülése már rejthetett komoly kellemetlenségeket intim vagy civilszféránkat illetően. Ekkor még nem sejtettük, hogy Murphynek mennyire igaza volt - van - lesz: **"Ha a dolgok úgy tűnnek, már nem romolhatnak tovább, mégis tovább romlanak..."**

A helyzet akkor kezdett el erőteljesen megváltozni, mikor **a csendben lapuló, internetes forgalmat, böngészőbeli viselkedésünket, jelszavainkat fürkésző kémprogramok** kapták a nagyobb hangsúlyt. És még itt is eleinte jöttek az ellenérvek: én egyszerű kisember vagyok, engem biztos nem fognak piszkálni, tőlem nincs mit kémkedni. Ennek ellenére láthattuk, hogy a személyes adataink (születés, lakcím, TB szám, útlevélszám, stb.) megszerzése és a velük való visszaélés: a személyiség lopástól kezdve a banki adatok kifürkészésén át fertőzött gépek felhasználásáig a botnet hadseregbe milyen széles skálán mozog.

A napokban az okozott ijedtséget, hogy **egy chilei hacker** egyszerűen feltette az internetre a mintegy hatmillió személyes adatot tartalmazó fájlokat. Az Anonymus Coward - névtelen gyáva - nevű elkövető által feltöltött, és részletes neveket, címeket, telefonszámokat, adószámokat és szavazási információkat tartalmazó csomag több órán keresztül elérhető volt egy technikai blogban. Miután felfedezték, és a rendőrség kezdeményezésére eltávolították onnan azokat - bebizonyosodott az ősi igazság: **ami egyszer felkerült a netre, az onnan soha többet nem távolítható el**. Azóta párhuzamosan több helyen is újra felbukkantak a személyes adatokat tartalmazó állományok, és az esély, hogy ezek máris nem kerültek, vagy a közeljövőben nem kerülhetnek rossz kezekbe nagyjából annyi, minthogy újra 3.60 legyen a kenyér ára, esetleg Michael Jackson legyen az Egyesült Államok elnöke.

Sokszor szoktak azzal érvelni, hogy **a hacker csak jót akar, felhívja a figyelmet a biztonsági hiányosságra, ezzel nagy szolgálatot t nekünk**. Biztos vannak esetek, amikor ez talán így van, most azonban ezt azt okfejtést biztosan nem méltányolja majd az a pár millió vétlen ember, akinek adatait - feltételezve, de nem megerősítve, hogy a hivatalok esetleg nem megfelelő módon gondoskodtak a biztonságról - közprédává tették. Szép dolog a Ludas Matyi módszer, meg a "Mózesre tanítás", csakhogy ezzel éppen azokat kellene megleckéztetni, akik rászolgáltak, nem pedig védtelen átlagembereket, akik jelen esetben az egészről mit sem tehettek.

És mit tehetünk mi a lánc végén, hogyan tanuljunk más kárán? Érdemes vészhelyzet esetén a fontosabb eléréseinknél azonnal jelszót

cserélni, bizalmas adatainkat tartsuk mindig titkosított partíción és vírusirtónk mellől ne hiányozzon a naprakész kémirtó program sem, vagy használjunk komplett internet biztonsági csomagot.

A kémprogram nélküli netezés ideje lejárt: ideje lenne erre **minden átlagfelhasználónak** rádöbbenie. Vagy másképpen: "**A gravitáció nemismerete nem mentesít a zuhanás alól!**" - ennyit tehetünk magunk helyett. A többi már sajnos nem rajtunk múlik.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/466348

Kommentek:

Nincsenek hozzászólások.

Új dimenziók

2008.05.14. 14:10 | Csizmazia István [Rambo] | 2 komment

Címkék: elektronikus hacker között támadás országok botnet belül hadviselés országon

Mikor először olvastam Aldous Huxley Szép új világ című könyvét (mellesleg mekkora egy lúzerségnek látszik DOS-os, Linuxos ésszel az ilyen _ékezetes_ link: .../Sz%C3%A9p_%C3%BAj_vil%C3%A1g), vagy amikor az HBO műsorán ment a Gattaca, még **az volt az érzésem, hogy fényévekre vagyunk ettől**, messze mint az 1968-ban készült 2001 Űrodüsszeia világa az általunk megélt magyar 2001-től.

A Gattacabeli főhős eredetileg **nem is lehetett volna űrhajós szívbetegsége miatt**, és a sportversenyekről ismert doppingellenőrzésekhez hasonló vizsgálatokon idegen vér- és vizeletmintákkal kellett trükköznie. Aztán mint derült égből a villámcsapás, kaptuk a hírt: a magyar munkaadók mostantól beletekinthetnek a munkavállalók genetikai vizsgálataiba.

Az új magyar törvény éppen ellentétes az angol vagy éppen amerikai gyakorlattal, **ahol a munkadókat és az egészségbiztosítókat éppenhogy korlátozták** az ilyesfajta magánszférabeli információszerzésben, emellett a józan észt, a társadalmi rétegek védelmét még nem is emlegettük. Az egy dolog, hogy szerintünk nem tartozik rájuk a mi adatunk, de felmerülhet még az is, **ki és hogyan tárolja (másolja le, veszti el) ezeket az információkat**, ki tekinthet majd bele, **megosztják-e egymással** a munkaadók, a fejvadász cégek (persze nem hivatalosan) mint a bankok BAR listáikat - ezeket az információkat.

Szépen és lassan az elektronikus hadviselésben is elérünk korábbi scifi regényes fantáziabeli szintre, csak éppen annihilátorok lövései helyett internetes támadások zajlanak. Az állam ellenőrző szerepénél inkább csak a tájékozatlanok lepődnek meg, ha az ellenőrzés konkrét módjairól olvashatnak. Ami viszont ennél sokkal érdekesebb, távolabbra mutat és veszélyesebbnek is látszik: az a **nem egy országon belüli, hanem az országok közötti elektronikus kémkedés és hadviselés**. Először az Észt-Orosz konfliktusról olvashattunk, majd gyanús és erőteljes jelei mutatkoztak az állami szintre emelt külföldi kormányok ellen folytatott kínai kémkedésnek.

Most pedig arról olvashatunk, hogy az **enyhén szólva is kétes eredményű** zimbabwei választások után, ahol hetekig nem hirdették ki a végeredményt, ismeretlen hackerek napokra kikapcsolták és blokkolták a helyi Herald újság online webhelyét. Nehéz ezt nem célzott akciónak értékelni, bár pontosan azt sem tudni, országon belüli vagy kívüli lehetett-e az elkövető. Mindenesetre **a hackelés mint eszköz** kinőtte magát jogvédő csoportok, katonák, szervezetek **féllegális eszközének**.

És ha hozzávesszük, hogy az Egyesült Államok hadseregének egy tisztje a minap saját botnethadsereg létrehozását látja időszerűnek - szerencsére **saját számítógépeikre alapozva** - akkor nyilvánvaló, hogy eljött az az idő, amikor sok jól képzett hacker **jól fizető munkát találhat végre hazájában a jó oldalon** is.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/467931

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.05. 20:15:04

Lassan itt a "szép új világ", betegségi adatgyűjtés ma, holnap pedig az állásinterjún már talán DNS tesztet is fognak kérni :-O
www.zoom.hu/kulfold/ujabb-botrany-a-lidlnel-44485.html?ref=hk

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.08.05. 10:37:48

Gattaca a nyakunkon, az emberi jogokkal kevésbé szöszmötölők jól elkezdik, aztán majd az egész világ szépen átveszi, és a végén kötelező lesz :-(((
mediq.blog.hu/2009/08/05/genteszteket_vegeznek_kinai_gyerekeken

Bigyó felügyelő: reloaded

2008.05.15. 11:40 | Csizmazia István [Rambo] | Szólj hozzá!

Megjelent **az ESET ingyenes felügyeleti eszközének, a SysInspectornak a végleges változata**, amely segít felderíteni a rejtett fertőzéseket.

Korábban márt hírt adtunk az akkor már használható, de még béta állapotban leledző segédprogramról, amely inkább a powerusereket és rendszergazdákat célozza meg. A szoftver segítségével a szakemberek megvizsgálhatják **az egyes gépeken aktív folyamatokat, a regisztrációs adatbázisok tartalmát, illetve többek közt kilistázhatják az automatikusan elinduló, valamint a hálózati kommunikációt folytató programokat**.

Szűrhetjük a tételeket a veszélyesség szint alapján is

Az integrált Anti-Stealth technológiának köszönhetően az ESET SysInspector emellett **felismeri a rejtett károkozókat - például rootkiteket - is**.

A HackerDefender rootkit drivere és a futó processz

Ez a funkció különösen hasznos azon vállalatok számára, melyek nem az ESET vírusvédelmi szoftvereit alkalmazzák. **A program menüjéből elérhető az ESET ingyenes online vírusirtója**, aminek segítségével a felfedezett fertőzések hatástalaníthatóak.

A képen a Vanquis rootkit el nem indított, de mégis felismert szervizfolyamata

A SysInspector ezzel együtt **a hozzáértő felhasználók kezébe való rendszerdiagnosztikai eszköz, mely nem helyettesíti a vírusirtót**. A program által **generált logfájlok** személyes adatokat nem tartalmaznak, kizárólag azt a célt szolgálják, hogy a kárelhárítást végző szakemberek minél egyszerűbben **felderíthessék a fertőzések okát**.

A képen a SpyBot által manipulált HOSTS fájlra kapunk figyelmeztetést

A SysInspector Windows 2000, XP, Vista, valamint Windows Server 2003 és Windows Server 2008 **operációs rendszereken fut**. 35 MB memóriát és 3 MB lemezterületet igényel, és a grafikus menü mellett parancssorból is vezérelhető.

A program **ingyenesen letölthető az ESET magyarországi honlapjáról**: http://www.eset.hu/segitseg/sysinspector

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/470335

Kommentek:

Nincsenek hozzászólások.

Még szódával sem megy el...

2008.05.16. 11:53 | Csizmazia István [Rambo] | 1 komment

A klasszikus mondás szerint egy újszülöttnek minden vicc új, ennek ellenére az adathalász próbálkozások is elérnek egy idő után egy olyan szintre, hogy **az előforduló árulkodó, de inkább ordító jeleknek már mindenkinek fel kellene tűnnie**. Egy vérszegény "amazonnal" randevúzunk.

A mostani levél is magán hordozza mintegy állatorvosi lóként a csalás stílusjegyeit: **bekéri a jelszót, a link és a hozzátartozó webhely címe eltérő, meglévő accountunkat kell "helyreállítani", stb.** Persze a magyar viszonylatban - aki már az Amazon weboldalról angolul rendel könyvet, az a szélesebbkörű tapasztalatai miatt talán több ismerettel rendelkezik a phishing tárgyában - legalábbis reméljük.

Az oldal egyes linkjei - szintén jó szokás szerint - **az eredeti oldalra mutatnak**, ezzel is fedezve a csalást.

Ami ilyenkor segíthet - bár **ehhez az idő múlása is szükséges** - a böngésző tartalmi tanácsadói pl. Finjan, McAfee, Netcaft Toolbar, stb. is figyelmeztetnek előbbutóbb a veszélyre.

Nem kell üveggömb hozzá, hogy megjósoljuk, ez a fajta trükk bár sosem fog kiveszni teljesen, **egyre inkább háttérbe szorul majd a sokkal hatékonyabb**, magát a weboldalakat megfertőző módszerhez képest, amelynek tömeges elterjedése már látható és erősödése várható a jövőben.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Az XP élt, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/472052

Kommentek:

titan 2010.04.29. 12:50:12

Épp nemrég rendeltem amazontól egy pár könyvet, és furcsamód pont akkor kezdtek el megszórni ezekkel a levelekkel (ráadásul olyan tartalommal, hogy valamiért késik a megrendelés - természetesen részletezés nélkül). Majdnem sikerült nekik, pedig hozzád hasonló szinten vagyok paranoiás :) Csak óvatosan.

Sebezhetőségek a Safariban

2008.05.19. 15:11 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac apple biztonság safari win macintosh exploit sebezhetőség rés nitesh dhanjani

Úgy tűnik, a Safari böngészőre is rájár a rúd. Az Apple programjában egy **Nitesh Dhanjani nevű úriember több sérülékenységre** is figyelmeztetett.

A három különféle hiba közül az egyik bizalmas adatok szivárgását teszi lehetővé. A kutató szerint a hibák mindegyike kritikus, erről bővebben a blogjában olvashatunk Safari Carpet Bomb címmel. Itt találhatjuk a beszámolót, köztük egy IFRAME-es mintapéldát képernyőképpel is láthatunk a "szőnyegbombázásról", ami lényegében azt mutatja be, hogy **egy preparált weboldalon a felhasználó jóváhagyása nélkül lehet káros tartalmakat a számítógépre letölteni** Windows és OSX rendszeren. Ki ki eldöntheti, hogy mennyire valósak a jelzett veszélyek. Érdekes, hogy az Apple csak az egyiknél ígért gyors javítást, a másik két esetben időt kért illetve nem tartotta kritikusnak a problémát.

Sok MacIntosh tulajdonos használ ettől függetlenül Firefoxot, hiszen az nagyságrendekkel kényelmesebb illetve testreszabhatóbb böngésző, és szabadon elérhető mindhárom platformon: Windows, Linux, Mac. (Safari és IE csak több-kevesebb hackeléssel létezik Linux alatt)

A Macen egyébként **eléggé biztonságban érezhetik magukat a felhasználók**, a nagy tömegben áradó Windowsos vírusok mellett eddig csak olyan kártevők bukkantak fel, amelyek kísérleti kódként, **minden esetben a felhasználó aktív közreműködését megkívánva** (kattintani kellett rá) tudtak csak futni, és ezek is csak mutatóba jelentkeztek.

A mostani rések egyébként nem az elsők ebben a böngészőben, **a Secunia adatai szerint** már 59 esetben tettek közzé valamilyen szintű riasztást a honlapjukon, persze egy Internet Explorerhez képest ez a szám szinte elenyésző.

Ami a Mac-en és a Linuxon is probléma lehet a biztonság szempontjából, az **a hivatalos és ellenőrzött szoftvercsatornákon, tárolókon kívüli szoftverek telepítése**. Az ismeretlen forrásból származó programok (video kodekek, alkalmazások) közé nem lehetetlen egy trójai kódot becsempészni - persze ezeket előbb-utóbb ugyan felfedezik, de addig is kárt okoznak. Ám egy idő után egyre jobban **számolni kell majd az olyan kihasználható résekkel is**, amelyek XSS, Flash-be ágyazott, SQL injection, más böngészőbeli eltérítés, vagy egyéb trükk kihasználása révén következik be. Csak érdekességképpen a 2007-es CanSecWesten láthattuk, hogy ott egy nulladik napi Safari sebezhetőség révén sikerült egy MacBookot feltörni, de igen tanulságos volt az idei meccs is, ahol a tanulság semmiképpen sem az volt,

hogy lám a Mac esett el elsőnek, a Win és Ubuntu pedig később (ez inkább azért történhetett, mert mindenki MacBookot akart nyerni ;-), hanem inkább az: **legyőzhetetlen rendszer gyakorlatilag nem létezik**.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/476794

Kommentek:

Nincsenek hozzászólások.

Biztonságosabb weblapok

2008.05.20. 12:12 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: weboldal biztonság sql malware fertőzés injection

Pár évvel ezelőtt, ha adatainkat ellopták, esetleg kényes dokumentumaink bánták, pénzügyi szempontból pedig **maximum idegenek is használhatták internetelérésünket**. Manapság, mikor már **szinte mindent a számítógépről intézünk: üzleti-, banki-, adó- és magánügyeinket**, a tét már jóval nagyobb. És ebben a játszmában azoknak is van felelőssége, akik a weblapokat készítik és fenntartják.

A weboldalak megfertőzésének egyik leggyakoribb technikája az SQL injection, vagyis **az SQL adatbázis lekérdezéseibe történő** (ez lehet akár MS SQL, MySQL, stb.) **kódbefecskendezés** (elég sután hangzik így magyarul). Szinte **minden típusú weboldal ellen sikerült már ilyen támadást végrehajtani** - legyen az egy magánember honlapja, egy egyesület vagy cég weboldala, vagy akár kormányzati, sportfogadási esetleg nagy látogatottságú hírportál.

A biztonságos netezés világában ránk felhasználókra hárul a feladat azon része, hogy számítógépeinket naprakészen tartsuk, az alkalmazások és **az operációs rendszer biztonsági javításaival** rendszeresen frissítsük környezetünket, **használjunk vírus és kémirtó programot, alkalmazzunk hardveres vagy szoftveres tűzfalat**, elfajzottabbak logokat olvasgassanak, és emellett úgy egyáltalán legyünk figyelmesek a nethasználat közben.

Amire viszont nem nekünk, hanem a weblapok készítőinek kellene ügyelni - ezügyben szemléletes demonstrációkat legutóbb az Ethical Hacking 2008 konferencián is láthattunk - az az elvárható legnagyobb gondosság, amivel a fejlesztők a programjaikat megírják. Sok jó információs oldal létezik e témában, számtalan figyelmeztetést adnak ki a szakértők is, még egy átlagos PHP+SQL programozó tanfolyam keretében is tanusíthatom, sok ilyen hasznos információt igyekeznek átadni erről is az oktatók. **A feltört weblapok aztán különféle kártevőket igyekeznek letölteni a látogatók gépeire**, és itt már bezárul a kör, mi felhasználók kerülünk közvetlen veszélybe. Tanulni kellene már ezekből az esetekből, legalább ne adjunk ekkora magaslabdát senkinek, meg főleg ne ilyen sokat.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/478214

Kommentek:

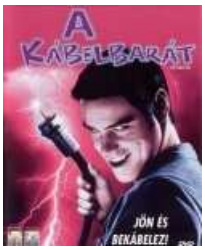
Nincsenek hozzászólások.

A kábelbarát

2008.05.21. 15:05 | Csizmazia István [Rambo] | 7 komment

Címkék: javítás john los angeles botnet kémprogram szervíz csaló schiefer

Remélem mindenkinek megvolt ez a film, még azoknak is ajánlom, akik esetleg nem bírják Jim Carreyt, mert **a tanulság benne örök érvényű**: bízz embertársaidban, de azért emeld meg a kártyapaklit.



Az átlagember agya úgy van huzalozva - és erre játszanak rá a social engineering bajnokai - hogy **a hivatalos szervekben**, a rendőrben, a szerelőben (vagy szerelőruhás szerelőnek gondolt illetőben) **nagy a bizalmunk**. Épp ezért fáj sokkal jobban, és épp **ezért kéne duplán büntetni**, ha épp a rendőr visszaélve előnyével bűncselekményt követ el, vagy ha pont az egészségügyi dolgozó igyekszik minket eltenni láb alól - hiszen nem ezt várnánk tőlük.

A fentiek fényében érdemes azt is átgondolni, **kihez és hova adjuk be számítógépünket javításra**. Történetünkben egy John Schiefer nevű, de korántsem úriember és munkatársai **alattomban kémprogramokat telepítettek a javításra kapott gépekre**. Ezekről titokban nagyszámú bizalmas adathoz (nevek, kártyaszámok, jelszavak, PayPal adatok) jutottak hozzá, melyek segítségével **ezek kontójára vásárolgattak**. Azonban nem álltak meg itt, a fertőzött gépeket egy hatalmas botnethálózatban üzemeltették, **mintegy 250 ezer számítógép volt nekik kiszolgáltatva**. A jelentések szerint egy holland reklámcéget is becsaptak, ahol az lett volna a feladatuk, hogy ahol a felhasználók engedélyezik, ott feltelepítsék a programjukat. A Los Angelesben élő Schiefer most **nem kicsi büntetéssel** kénytelen szembenézni: **akár 60 éves börtönre és 1.75 millió dollár kártérítésre** is rúghat a majdani ítélet.

Van egy olyan mondás, hogy **ha autót veszünk ne (csak) az autót nézzük meg alaposan, hanem az eladót is**. Ha nem bizalomgerjesztő, inkább álljunk el az üzlettől. Egyszer sikerült az utolsó pillanatban visszakozni egy olyan autótól, amelyet felemelve, alánézve és megvakargatva derült csak ki, hogy két különböző színű autóból hegesztették össze. A tulajdonos - aki éppen autószerelő volt a szakmájára nézve - **ártatlan arccal állította, ő nem tudott semmiről**, na persze.

Szóval ahogy vízszerelőt, és egyéb mesterembert is akkor hív az ember szívesen, ha már a barátnál, testvérnél vagy a szomszédnál jól és megbízhatóan dolgozott, **a számítógépünk javítását se bízzuk akárkire**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/480413

Kommentek:

amondó (törölt) 2008.05.21. 16:27:22

Ez jó bejegyzés. A blog is jó, az ubuntu link külön tetszik. Viszont kicsit kevesebb mozgó izével könnyebben olvasható lenne.

Cigiző · http://cigi.blog.hu/ 2008.05.21. 16:29:59

ha majd már megszokott dolog lesz teljes mértékben a PC, akkor nem fog ilyen előfordulni - de a kapcát miért nem kapcsolod ki legalább a bejelentkezett felhasználók előtt?!?!?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.21. 16:36:49

Szia Amondó!
Köszi a dícséretet :-) Akkor ezek szerint továbbfűzve a gondolatot, nemcsak a blog jó, de az Ubi is remek :-D
Mozgó izé fronton talán jó hírem van: a számuk ennél biztosan nem fog tovább növekedni ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.21. 16:38:00

Helló Cigiző!
Öreg légiósok mostantól kapca nélkül jöhetnek a kantinba ;-)

Cigiző · http://cigi.blog.hu/ 2008.05.21. 17:42:25

Na végre!
;)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.15. 21:40:53

Van magyar szervizes eset is:
www.rtlhirek.hu/cikk/193469

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.09. 11:23:42

Lassan mindenki kezd paranoid lenni, és úgy látszik, nem is ok nélkül:
www.itpages.hu/20080808/lemasoljak-a-szamitogepeink-tartalmat-a-szervizekben

Szigorúan ellenőrzött alattvalók

2008.05.22. 14:01 | Csizmazia István [Rambo] | 9 komment

Címkék: anglia brit megfigyelés nsa isp

Lehet, hogy a brit állampolgároknak hamarosan **nem kell majd külön Big Brother valóságshowt nézniük** a televízióban ahhoz, hogy valakinek minden mozdulatát figyelemmel kísérhessék. Ha egy tervezet megvalósul, **ők maguk lesznek az alanyai annak a megfigyelésnek**, amelyben minden telefonhívásuk és smsük, minden e-mailjük, minden általuk meglátogatott weboldal 12 hónapra visszamenőleg egy gigantikus adatbázisba kerülhet.

Tulajdonképpen a Home Office programnak nem is azzal a részével van baj, amikor egyedi esetekben ügyészségi felhatalmazás után beletekintenek ilyen adatokba, hiszen ez úgymond nemzetbiztonsági érdek: terroristák, pedofilok, fenyegetőzők és bűnözők ellen ez szükséges, törvényes keretek között végzett lehallgatás pedig mindig is volt, és mindig is lesz. Hanem **ha esetleg a hatalom, illetve egy korrupt vagy túlbuzgó alkalmazott extra felhatalmazás nélkül is úgy gondolja, úgy gondolhatja, hogy az éppen aktuális politikai vagy gazdasági ellenfelei körmére néz illegális módszerekkel**. Rossz esetben pedig tömegesen és mindezt az adófizetők pénzén. Hogy a veszély fennáll és az embereket igenis foglalkoztatja, arra jó példa volt a németországi Skype lehallgatással kapcsolatos szerződés nyilvánosságra kerülése. Ideillő Murphy törvénnyel szólva: "Egyetlen állampolgár élete, szabadsága és vagyona sincs biztonságban, amíg ülésezik az Országgyűlés!" ;-)

Emlékezetes volt az a jó pár éve történt eset, amikor a brit rendőrség úgy nyilatkozott, már nem hallgatják le teljeskörűen a telefonhívásokat, mégis amikor egy fülkéből valaki a királynőt fenyegette meg, a 30 másodpercen belül kiérkező nyomozók nyomban elkapták az elkövetőt.

Visszatérve a témánkhoz, adataink kezelésének az a szegmense, ahol **a rólunk és velünk kapcsolatos információkat gyűjtik, őrzik a különféle hivatalok, egészségügyi intézmények**, stb. semmilyen módon nem láthatunk bele, és **nincs rá semmiféle befolyásunk**. Reménykedünk, hogy gondosan kezelik, reménykedünk hogy titkosítva tárolják, reménykedünk, hogy csak az nézhet bele, akinek kell, reménykedünk hogy nem másolja vagy lopja el senki, **reménykedünk, hogy minden betekintést rendesen naplóznak**.

Hiába netezünk mi a legnagyobb gondossággal, hiába vagyunk óvatosak a közösségi portálokon, ha közben a rólunk szóló aktákat, fájlokat ellopják, elvesztik vagy adatainkhoz illetéktelenek is hozzáférhetnek, abból adatokat gyűjthetnek, vagy ne adj' Isten magát az adathordozót vagy a számítógépet vesztik el mindenestül.

De persze az sem sokkal biztatóbb, ha a "Birodalom" gátlástalanul, nyakló nélkül személyes adatokat gyűjthet. Lehet, hogy sokan ennek nem is értik a jelentőségét, de kb. úgy kell elképzelni, hogy ha **valaki például pár év múlva majd polgármesternek szeretné** jelöltetni magát, akkor valahol majd **egyszer csak előhúznak egy aktát**, és jönnek a kompromittáló cikkek: hogy hohó: milyen ember ez, tíz évvel ezelőtt háromszor is ellátogatott egy homoszexuális oldalra! Ejha, 3 éve levelezte le a szlovák rendszámú gépkocsiját, szóval ez egy csaló? Nocsak, 2 éve megcsalja a feleségét, itt a levelezése a szeretőjével! Hűha, és milyen telefonhívásai voltak 8 éve 6 hónapja és 12 napja! Egy ilyen embert akarnak önök egy közhivatal élére?

Valószínűleg itt is a **megfelelő és szigorú szabályozás** adja, adhatja meg a mindenki számára üdvözítő és egyben megnyugtató megoldást.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/481782

Kommentek:

Bucii 2008.05.22. 18:18:48

Az baj ezekkel a nagy adatgyűjteményekkel, hogy csak azok ellen tudják használni, akik nem védekeznek ellene. Aki terroristatámadást készít elő, és tudja hogy védekeznie kell egy ilyen adattár ellen, nyilvánvalóan a megfelelő módon titkosított üzenetekkel fog kommunikálni, amit aztán a nemzetbiztonságiak baszhatnak.

Egy ilyen rendszer a magánszféra megsértésén kívül teljesen felesleges pénz, idő és energiapazarlás is.

átlátó 2008.05.22. 20:22:54

Mint az előző. Igen, yes, ja, da, si,...

buherator · http://buhera.blog.hu 2008.05.22. 21:08:32

Ide nem kell szigorú szabályozás: az államnak egyszerűen el kéne vetnie azt a gondolatot, hogy minden állampolgárt potenciális bűnözőnek tekint. Egyébként nem csak kormányzati szinteken van jelen a probléma, mi a helyzet pl. a Google Health-el: ha.ckers.org/blog/20080521/google-health/ ?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.23. 13:53:16

Szia Bucii!
Éppen tegnap olvastam egy cikket, hogy egy korábbi gépeltérítő dolgozott a Heathrowi reptéren rakodó munkásként, és ezt csak most vették észre. Pedig ott aztán van kamera dögivel, adatbázis a négyzeten, meg állítólag hatékony ellenőrzés, és minden ilyesmi :-O

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.23. 13:56:09

Hello Buherátor!
A felvetett gondolat nekem is szimpatikus, csak abban vagyok pesszimista, hogy ez az alapfelállás mikor lesz végre úgy, ahogy mi szeretnénk ?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.29. 14:59:15

Egy kis magyar adalék hozzá:
www.hirszerzo.hu/cikk.legfeltettebb_titkaink_sincsenek_biztonsagban_-_figyelemfelkelto_eloadas_videoval.67645.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.06. 13:16:38

A demokrácia "hazája" is szolgál időnként meglepetésekkel, ez most kissé kellemetlen fajta:
biztonsagportal.hu/elkobozhatjak-laptopokat-amerikai-hataron.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.06. 16:36:25

Ha pedig az alattvaló (sajnos nem állampolgár) véletlenül túl sokat megtud, akkor jöhet ez:
www.origo.hu/tudomany/20090319-az-emlekek-szelektiv-torlese-hogyan-mukodik-a-memoria.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.12. 10:52:16

Újabb "nagyszerű" vívmány: ügyészségi felhatalmazás nélkül is tehetnek GPS adót a kocsikra:
www.chicagotribune.com/technology/chi-ap-wi-gps-police,0,5867383.story

Jó ötlet-e a vírusíró verseny?

2008.05.23. 13:20 | Csizmazia István [Rambo] | 6 komment

Címkék: verseny defcon to zero race vírusíró

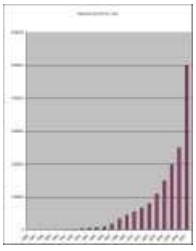
A múlt hónapban a Defcon szervezők egy **új műsorszámmal bővítették** a Las Vegasban augusztus 8-10. közötti Riviera hotelbeli rendezvényt. Race to Zero néven víruskészítő bajnokságot hirdettek. Ciki vagy cuki? **Ártalmatlan móka ez, vagy a feleslegesen növekvő kártevőhad**, ami többlet munkát és bosszúságot okoz a vírusvédelmi programok fejlesztőinek?

A verseny persze érdekesen hangzik, lehet, hogy akad, akinek ez még jópofának is tűnhet. De mi is lesz ez pontosan? A résztvevők **kapnak egy már kész, meglévő víruskódot, amit addig kell majd pofozgatniuk, amíg a lehető legtöbb antivírus program már nem veszi észre**. (A mostani vírusírók is így tesznek, amikor új kártevővel vagy új variánssal akarnak megjelenni.)

Volt egy szavazás a VirusBulletin oldalon is - most azt leszámítva, hogy a részszázalékokat összeadva nem jön ki a 100% - valami zavar van az erőtérben.

Nézzük hát meg az arányokat úgy, hogy az eddigi szavazatok arányát összeadva **(35+12+7=54) kivonjuk azt a teljes 100-ból, ez akkor 46%**. (Remélem nem követtem el semmilyen lebegőpontos hibát ;-) Nyilvánvaló az lenne, hogy azok, **akik idelátogatnak, kevésbbé lelkesednek egy ilyen verseny ötlete iránt**. De szemlátomást **ennek az ellenkezője történt**: az erről beszámoló cikk is azon bosszankodik, hogy milyen nagy rész, sőt **a szavazók legnagyobb szelete tartotta mégis jó ötletnek** ("Almost half of users think virus-writing contests are a good idea").

De mi a véleménye a szakértőknek? Vírusokban és variánsokban sajnos eddig sem volt hiány, az utóbbi években pedig annyi minta kerül naponta a laborokba - többszáz - amit pusztán **kézi módszerekkel, automatizálás nélkül képtelenség visszafejteni**, adatbázisfrissíteni. A változtatásoknak, **módosításoknak már komoly hagyománya va**n, legyen az egy-két gépi kódú utasítás felcserélése, extra NOP utasítások beszúrása, összezavart (obfuscated) JavaScriptes kódok írása, stb. A variánsgyártás egy módja a **különféle exetömörítőkkel (packer) való becsomagolása** a futtatható víruskódnak. A legtöbb esetben ez **nem teszi ugyan lehetetlenné a kicsomagolást** és elemzést, de erőteljesen **lelassítja a visszafejtési munkálatokat**. Manapság minden komoly víruslabornak már **saját készítésű kicsomagaló (unpacker) rutinjai** vannak, ennek ellenére folyamatosan zajlik a két oldal közt a háború, és készülnek igen kellemetlen, polimorfikus (azaz egyedi kódot generáló) tömörítők is, amelyek azért okoznak fejtörést.



Az F-Secure statisztikája

Szóval a verseny **a biztonsági programok készítői számára enyhén szólva nem igazán tűnik jó ötletnek**, első körben biztosan jó pár munkaóra többletet ró majd minden AV csapatra. Szerintük **semmi szükség újabb kártevőkre**, keletkezik belőlük így is éppen elég. Azt is kifogásolják, hogy a verseny ilyen módja igazából **semmi különösre nem tanítja meg a résztvevőket**, csak adatbázis növekedést okoz. És ha annyira meg akarják mutatni, **mennyire okosak, írjanak ki olyan versenyt, amely a kártevők megtalálásában segít**, nem pedig számuk gyarapításában.

Ennek pontosan az ellenkezőjét vallják a másik oldalon: (a linkért köszönet Buherátornak) úgy gondolják, **ideje felrázni kicsit a túl mechanikusan játszó, túlzottan a szignatúra alapú védelemre támaszkodó** AV fejlesztőket, és más, hatékonyabban működő, például HIPS (host intrusion prevention system), sandboxing és **virtualizációs technikákra épülő védelmet kérni tőlük** számon. Egyes kommentelők szerint bár újabban igen **divatos lett a heurisztika** szó, ennek valódi képességei nem igazán látszanak egyes antivírus termékek esetében.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/483695

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.23. 16:05:38

Most látom, hogy közben megjavították a linket a Virus Bulletinen, már jók a százalékok.

Maestro 2008.05.23. 17:19:34

a verseny célja nyilván az, hogy ha valaki előállna ott egy újfajta vírusmásoló ötlettel, akkor azt azon nyomban elkezdhetik feldolgozni az av fejlesztők.

másrészt jó móka lenne, hogy oké öcsi, hogy megírtad, most jön az, hogy hatástalanítsd:)

Rwindx 2008.05.23. 17:39:56

A vírusokban rengeteg tudás, technika van elrejtve az operációs rendszerről, a processzorról, és úgy egyáltalán a fejlesztésről.

Valamikor nagyon régen foglalkoztam virusanalizálással, amibe belefért saját vírus írása is :) Természetesen anélkül hogy szabadjára engedtem volna. Hehe anno fiatalon meg akartam írnia világ legkisebb vírusát, 31 byteos lett és fertőzött, de hallottam egy 26 byteosról, szóval nem sikerült :(

Viszont kb 2 évvel rá már az ezen tudást felhasználva egyedi víruspajzsokat csináltam a BackForm illetve OneHalf ellen, amikor még nem volt Mo-n (legalábbis nem tudtam róla) vírusírtó ami leszedte volna. Az enyém sem szedte le, de nem is

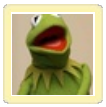
engedte fertőzni, meg pl lekódolni a winchestert.

No mindegy, lehet túllihegtem a dolgot, csak arra akartam utalni hogy amit a vírusokkal kapcsolatban meg lehet tanulni azt jóra is fel lehet használni. Nem feltétlenül arra hogy újabb vírusírók tucatjai álljanak hadba.

buherator · http://buhera.blog.hu 2008.05.23. 17:42:16

Nem nagyon követem az AV piacot, de én is úgy gondolom, hogy szemléletváltásra lenne szükség. Ma egy távoli kódfuttatást eredményező hibára napokon, vagy akár órákon belül kijöhet az exploit, amit aztán beépítenek a botnetekbe, wormokbe, az AV-k meg csak néznek, hogy alig indult el az adatbázisok frissítése, már a fél világ benyelte a békát. És akkor a gyártói patchek iszonyatos kiadási sebességéről még meg sem emlékeztünk :P

A böngészőket, levelezőket be kéne rakni a kis homokozójukba, aztán le van a gond (persze ha jó az implementáció), a kedves júzernek meg nem kéne hagyni adminként rombolni mindenütt. Ez persze egy részről nem (csak) az AV vendoron múlik, másrészt a felhasználók sem fogják szeretni a dolgot.



viktor134 2008.05.23. 18:41:24

de szőrözünk a százalélkokkal. fél cikk semmiről nem szól. :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.05.30. 09:14:16

Egy hosszú és alapos komment az ESET oldaláról:
www.eset.com/threat-center/blog/?p=123

Számítógépes csalók lakat alatt

2008.05.27. 11:33 | Csizmazia István [Rambo] | 2 komment

Címkék: csalás phising nemzetközi nemzetiség adathalászat

Négy különböző nemzetiség képviselője volt az asztalnál: egy amerikai gyalogos, egy francia őrvezető, egy angol géppuskás és egy orosz hússaláta. A gyalogos, az őrvezető és a géppuskás a padon foglaltak helyet, a hússaláta az asztalon, egy tálban. **Akár így is kezdődhetne ez a beszámoló...**

Szóval esetünkben ez a következőképpen nézhet ki. Hat különböző nemzetiség képviselője került letartóztatásra: **három amerikai** állampolgár, **öt vietnámi** illetőségű egyén, **egy kambodzsai, egy pakisztáni, két mexikói** és végül **sok román**. Van **több ismeretlen, kizárólag nicknéven ismert** elkövető is: "Cryptmaster"; "PaulXSS"; "euro_pin_atm" és "SeleQtor", akikről csupán feltételezik, hogy szintén a román csapatban szerepelhettek.

A nemzetközi szervezett bűnbanda tagjai nagystílű számítógépes csalásokban vettek részt, phishing weboldalakat üzemeltettek, amelynek segítségével **jelszavakat, kártyaszámokat tulajdonítottak el**. Először Romániaban csapolták meg a bankkártyákat, **később aztán már az Egyesült Államokban** is.

A bizonyítékok gyűjtése komoly feladat volt, és különböző konspirációs trükkökkel - hamis szerverek telepítése, román nyelvű SMS üzenetek küldése - **az amerikai nyomozást igyekeztek megnehezíteni**.

Bár a beszámolóban hússalátáról ugyan nem esik szó, de akinek a pénzét ellopták, valószínűleg szívesen csinálva valamelyikükből egy-két jól irányzott ökölcsapás és rúgás segítségével ilyet. Ezt azonban mélyen elítéljük, pfúj ;-), hiszen kultúrált és demokratikus országokban per, tárgyalás és ítélet helyettesíti a nyers erőszakot.

Az eset **kiemelt jelentőségű és precedens értékű az igazságszolgáltatás számára**: első ízben sikerült egy kiterjedt, több országon

keresztül ívelő, igazi csapatmunkát megvalósító ügyet felgöngyölíteni. És persze **a leleplezést itt is csak egyesült összefogással, illetve nemzetközi együttműködéssel** lehetett megvalósítani.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/489791

Kommentek:

liteminyuszika · http://nyuszika-portal.blog.hu 2008.07.10. 11:00:38

Nem jó az egyik címke! adathaláaszat -> adathalászat ;)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.10. 11:13:04

Köszi LiLO, javítottam :-)

Nehéz három óra

2008.05.28. 17:48 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hiba frissítés nod karantén eset

A vírusirtók esetében **az adatbázis frissítés az esetek 99.99 százalékában problémamentesen zajlik le**. Ezzel együtt minden gyártó esetében előfordult már egy-egy hiba, a legutóbb **a NOD32 3.0-ás verziójának frissítése okozott kisebb fejfájást**.

Könnyű az egyik legmegbízhatóbb vírusirtó hírnökének lenni, hiszen az ESET termékei a legritkább esetben hibáznak. A **múlt héten azonban nekünk osztott a szerencse rossz lapot**. Az ESET a megszokott alapos ellenőrzés dacára egy olyan NOD32 szignatúra frissítés bocsátott ki, amely **a gépek egy részén furcsa dolgokat művelt**. A 3119-es számú frissítés, amely 22-én 10:45-kor került kiadásra, **néhány gépen tiszta fájlokra is riasztott, egyes esetekben pedig lefagyást eredményezett**. A hiba kizárólag a vírusirtó 3.0-ás változatát érintette.

A laborba hamar eljutottak a visszajelzések, és **a 3121-es, 13:40-kor kiadott javított adatbázis korrigálta a hibát**. A mintegy három órán keresztül fennálló probléma **a felhasználók töredékét érintette**, mivel ahhoz, hogy a rossz adatbázis problémát okozzon, nem csupán az kellett, hogy a kritikus időszakban kerüljön frissítésre a vírusirtó, de az is, hogy **a felhasználó ugyanekkor indítson el bizonyos (például Adobe) alkalmazásokat**.

Sajnos azonban néhányan itt Magyarországon is belefutottak ebbe a problémába, és **emiatt olyan tiszta állományokat is töröltek, amiket később a karanténból kellett visszaállítani**. Ügyfélszolgálatunk szerencsére a helyzet magaslatán volt, és a beérkező (egyébként 10 alatti) panaszt sikerült rövid idő alatt orvosolni.

A teljes AV mezőnyt vizsgálva nem egyedi eset, ami történt, **a különféle vírusvédelmi programoknál ha ritkán is, de sajnos többször is történt már hasonló probléma**. 2007 decemberben a Kaspersky azonosított tévesen a Windows Explorerben kártevőt, míg 2007 június 27-én a VirusBuster frissítése és az APEH Abev programja veszett össze. Ugyancsak hasonló esetek történtek például a Nortonnál, ahol rendszerfájlok kerültek indokolatlanul karanténba, vagy 2006-ban a McAfee háza táján is volt egy hasonló sajnálatos esemény.

Az ilyen esetek azonban **szerencsére igen ritkák**, mivel a frissítés kibocsátása előtt a gyártók nagyszámú tiszta állomány esetében is ellenőrzik, hogy valóban vakriadó mentes-e az új szignatúra. És, bár a tiszta állományok esetében bár igen nagyszámú fájlgyűjteményről van szó, ez nem tartalmazhatja a világ összes programjának minden állományát, így **időnként a legjobb szándék, és alapos ellenőrzés dacára is előfordulhatnak malőrök**. Ilyenkor a versenytársak sem nyilatkoznak kárörvendően - sőt nem ritkán segítséget is nyújtanak, ha ez szükséges - hiszen tudják, **ez Damoklesz kardjaként egyformán ott lebeg mindegyikük feje felett**.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/491408

Kommentek:

Nincsenek hozzászólások.

Ahol nagyban játszanak

2008.05.29. 11:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: bank fbi adó phising visszatérítés adathalászat adóhivatal

Amerika nagy, én meg kicsi vagyok ;-) Az eredményes adathalász típusú csalásoknak nem csak a csaló és a hozzávaló hiszékeny felhasználó a szükséges kelléke, de nem árt, ha mindehhez **nagy számban terjeszthető, hihető és sokakat érintő téma járul**: ekkor szinte garantált a siker, és már pár aprócska százalék is jócskán hoz a konyhára - kleine Fische, gute Fische.

Két biztos és elkerülhetetlen dolog van az életben: az egyik adófizetés, a másik a halál. Az előbbivel kapcsolatosan figyelmezteti az állampolgárokat visszaélésekre az FBI közelménye. Mindenki boldogan fogadja, ha adóvisszatérítésről szóló - juhéé, pénz áll a házhoz anyukám - értesítést kap, ezzel eddig nincs is semmi baj. A baj akkor kezdődik, ha felfokozott heveny izgalmi állapotban elfelejtkezünk a már ezerszer tágyalt alapvető biztonsági szabályokról és az óvatosságról:

- **e-mailben érkezett linkre kattintva** lépünk egy hivatal oldalára ahelyett, hogy magunk gépelnénk be a címet

- nem vesszük észre, hogy enyhe **nyomást próbálnak ránk gyakorolni - nem lesz gyors pénz, ha nem lépünk tüstént -, miért kattintsunk a linkre** ("economic stimulus tax rebate may be delayed if they do not follow this link to directly deposit the money into the consumer's bank account")

- a weboldal szokatlan módon **nem csak a banki alapadatokat kéri be, hanem a hozzátartozó jelszót, pinkódot** is

Bár **a bikkfanyelvről néhány mostani hivatal sem szokott le**, egy nemzetközi banktól szokatlan lenne egy ilyen színvonaltalan iromá
nem is beszélve a tükörfordításból adódó "szövetségi hatóságról"

Elképzelhetjük, hogy a két évvel ezelőtti vérszegény magyar banki próbálkozásokhoz képest (én itten törve beszélni magyarni add ide te ottan nekem enyémbe tiéd számla kód unga-bunga ;-) egy ilyen hivatalosnak látszó, helyesírási hibáktól nem hemzsegő, **megfelelő időben kibocsátott és emberek millióit közvetlenül érintő dolognál mennyi pénz forog kockán**. Itt aztán abszolút igaz, hogy a **sok kicsi sokra megy**.

És ha valaki felelőtlenül és gyanútlanul mégis kiadja a banki adatait, nos az egy pillanat alatt statisztikai adattá változik, akik ismét növelték a számítógépes bűnözők bevételeit.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/493120

Kommentek:

Nincsenek hozzászólások.

Gitárosok lapja a célpontban

2008.05.30. 19:58 | Csizmazia István [Rambo] | Szólj hozzá!

Egy ideje már bebizonyosodott: **nem csak hétköznapi magánemberek weblapjai**, vagy nagyforgalmú sport- és közösségi portálok eshetnek áldozatul a megfertőződésnek, hanem **szinte bármilyen weboldal ellen indulhat** ilyen - sajnos sikeres - támadás.

Legutóbb a gitár zene kedvelői voltak egy rövid ideig veszélyben. Az oldal **egy kínai eredetű malware áldozata** lett. Szerencsére az üzemeltetők hamar észrevették a dolgot, **akadozott az adatbázis motor és furcsa jelenségek** történtek, ezért gyorsan lakapcsolták a szervert. Egy kb. három órás leállással járó javítással, és a fórumban néhány hozzászólás elvesztésével megúszták. Segített a dologban, hogy pedánsan, szépen és **rendszeresen mentették az anyagaikat, így semmilyen értékes adatvesztés** nem történt.

Jó sok évvel ezelőtt egy testőrtanfolyam keretén belül zajlott a fegyvertanfolyam illetve vizsga, és még jól emlékszem az ottani intelmekre: **"Töltetlen fegyver nincs!"** Ami annyit tesz, hogy ahányszor csak hozzányúlunk, mindig azt kell feltételezni, hogy az megtöltve és kibiztosítva van. Akinek ez nem válik a vérévé, könnyen okozhat vagy szenvedhet el balesetet. Lehet, hogy **lassan a weboldalakkal is kénytelenek leszünk egyre óvatosabban bánni**. A legutóbbi flash sebezhetőség egyelőre csak XP rendszeren okoz kárt bizonyítottan, de gyanítható, hogy később esetleg az alternatív oprendszereken is okozhat gondot. A védekezéshez egyelőre marad a **heurisztikus antivirus, a kedvenc NoScipt plugin, esetleg SandBoxie vagy Mac/Linux alatti** böngészés.

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/494680

Kommentek:

Nincsenek hozzászólások.

Szerepcsere

2008.06.02. 18:58 | Csizmazia István [Rambo] | 3 komment

Címkék: microsoft apple hiba ie safari idg szőnyegbombázás stopbadware

Korábban már beszámoltunk egy Safari böngészős hibáról, amit bár a felfedezője kritikusnak tartott, **az Apple nem értett ezzel egyet és nem tartotta sürgősnek** javítófolt kiadását. A hiba szerintük nem jelentős, és éppen csak azt nem mondták, hogy addig is böngésszük kizárólag megbízható forrásból származó weblapokat ;-) A sebezhetőség **azonban úgy tűnik, mégis komolyabb a vártnál**.

Érdekes módon most a korábban hasonló el nem ismerő-, és halogató taktikát folytató **Microsoft állt a sarkára és igyekszik a hibára jobban felhívni a figyelmet**: nem véletlenül. Ugyanis a Safariban Nitesh Dhanjani biztonsági kutató által május 15-én talált hiba és az Internet Explorerben lévő másik együttes hatásaként **tetszőleges program futtatható a sebezhetőség kihasználása révén**.

Az IDG News Service munkatársai **demonstrálták is a hibát**, melynek eredményeképpen képesek voltak az áldozat számítógépén lefuttatni a Windows Calculator programot. A dolog végrehajtásához **egy rosszindultú kódot tartalmazó weboldalt kellett előtte Safari böngészővel felkeresni** a bemutató kedvéért.

A Microsoft ezúttal komolyan veszi az esetet, hiszen az XP és Vista alatt is jelentkezik és máris kibocsátott egy biztonsági értesítőt. Ellenben **az Apple még mindig félvállról kezeli az automatikus fájlletöltési esetet** - némiképp csalódást okozva saját felhasználóinak is - pedig még a StopBadware.org is felszólította: vegye komolyan a szőnyegbombázás nevű sérülékenységet és adja közre mielőbb a biztonsági hiba javítását.

Az eddigi böngésző biztonsági összehasonlításokon a Safari **mindig büszkén hozakodott elő azzal, hogy extra rövid idő alatt befoltozza** a versenytáraihoz képest sokkal kevesebb biztonsági hibát, és ezzel igyekezett nimbuszát megóvni. Emiatt aztán **végképp érthetetlen részükről ez a hozzáállás**.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/499811

Kommentek:

lwolf · https://sites.google.com/site/enesbcs/ 2008.06.02. 20:35:56

Ha nem akarnak, vagy nem tudnak böngészőt fejleszteni, akkor végülis miért kínlódnak vele? Inkább tegyenek a macosx-be firefox böngészőt és később nem kell vele szórakozniuk. :)
Mindenki maradjon annál, amihez ért.

satie · http://321.hu/sas 2008.06.02. 20:45:00

ezért használ az ember nyílt forrás szoftvereket, nyílt forrású böngészőt, mert ott, ha van 1 hiba, valaki AZONNALI HATÁLLYAL KIJAVÍTJA !!

Szóval az Apple, Microsoft és a hasonló cégek maradjanak a kütyügyártásnál, a szoftvereket meg írják, akik merik nyíltan fejleszteni, és ami mellett a felhasználók nyugodtak maradhatnak.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.03. 07:07:56

Helló Lwolf és Satie!
Maximálisan egyetértek, sok Maces cimbora is inkább a FFoxra esküszik, maxumum webfejlesztésnél Safarival is teszteli az oldalt.

Én is használom mindhárom OS.t (Win, Mac, Linux) és a Firefox ketyeg mindegyikben. Persze külön érv mellette, hogy a kedvenc pluginjeimhez is ragaszkodom.

Gyorsító juice a VirusTotalnak

2008.06.03. 21:56 | Csizmazia István [Rambo] | 1 komment

Címkék: virustotal gyorsítás sha512 sha256 peinfo

Még **Rúgóláb Seriff is megirigyelhetné az újabb fejlesztéseket**, amikkel bár nem tudunk megelőzni egy kilőtt golyót, de azért **igen hasznosak és érezhetően gyorsítják** a munkát.

Kisebb, de a sebességre igen csak jó hatással voltak azok a fejlesztések, amik a VirusTotal oldalon zajlottak. A kereső motorok immár **nem egymásután ABC-ben rontanak neki** a vizsgált kódnak, hanem csoportokban párhuzamosan, és a kijelzés **menetközben rendezi aztán őket listába**.

A rendelkezésre állás és a minta vizsgálati ideje **szemlátomást rövidült** ezzel, a szolgáltatás kihasználtságát pedig **egy színes kijelzőn kísérhetjük** figyelemmel.

Bővült az információ tartalom is, már nem csak az MD5 és SHA1 hash, hanem **az SHA256 és SHA512 ellenőrző összeg is** szerepel, ezzel segítve, hogy a beazonosított mintát ne kelljen minden alkalommal újra megvizsgálni, ha a felhasználó megelégszik **egy korábbi elemzés eredményének megtekintésével**. Természetesen emellett lehetőség van ismételt elemzésre is.

Emellett a **PE (Portable Executable) fájlok fejlécének és fájlszerkezetének információi** is megjelenítésre kerültek, például a szekciók nevei, a program belépési pontja, milyen gépre (processzorra) készült a kód, stb.

Bővültek a keresőmotorok is, egyelőre a GData programmal, de **várható, hogy a következőkben további antivirusokkal is** gyarapszik a mezőny.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/502152

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.15. 22:13:23

Újabb fejlemény, hogy már 38 motor szerepel, a Comodo AV is bekerült a brancsba, plusz mostantól a vizsgálatnál extra szolgáltatásként megkapjuk a CWSandbox info linkjét is.

Szeretünk fertőződni

2008.06.05. 20:35 | Csizmazia István [Rambo] | 17 komment

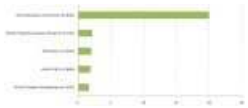
Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

A magyar felhasználók annyira **szeretik az ingyenes tartalmakat**, hogy amikor egy weboldal szabadon letölthető zenefájlokat ígér, a biztonsági kockázatokat **nem mérlegelve kattintanak a letöltés gombra**. Az adatokból kiderült, **Magyarországon a legtöbb vírust mi magunk telepítjük** a számítógépre. Következzen **a NOD32 antivírus rendszert gyártó ESET ThreatSense.NET Center felmérése.**

Számos vírusirtó cég közöl statisztikát arra nézve, hogy mely károkozók végzik a legnagyobb pusztítást az interneten. Az ESET statisztikai rendszere azonban **egyedülálló módon képes az egyes országokra lebontott** vírusstatisztika közlésére is, és **nem csupán az e-mailekben terjedő károkozókról** ad átfogó képet, hanem a számítógépet http protokollon keresztül, **böngészés közben megfertőzőkről is**.

A májusi adatokból kiderült, hazánkban azok a vírusok terjednek a legnagyobb számban, melyek **valamilyen ingyenes tartalmat** (például .mp3 fájlokat) ígérnek a felhasználóknak, akik a **megtévesztésnek bedőlve, saját maguk engedik be** számítógépükre a károkozókat.

"Sajnos - akár az angol nyelvtudás hiányában - sokan telepítenek olyan kéretlen reklámprogramokat, melyek később lelassítják a számítógép működését, vagy zavaró üzeneteket jelenítenek meg a monitoron" - emelte ki Csiszér Béla, az ESET magyarországi képviseletét ellátó Sicontact Kft. ügyvezetője. A szakember szerint a felhasználóknak **sokkal óvatosabban kellene** viselkedniük, amikor **ingyenes tartalmakat, illetve programokat ígérő üzenetekkel találkoznak**, és nagyobb figyelmet kellene fordítaniuk arra is, hogy milyen vírusvédelmi alkalmazást használnak. A vírusirtó **frissítése és helyes beállítása ugyanis elengedhetetlen** ahhoz, hogy folyamatos védelmet élvezzünk a károkozók ellen.



A májusi károkozó toplista első 5 helyezettje ugyanakkor csupán az összes fertőzés 25.95%-ért felelt, ami mutatja azt is, hogy a vírusok világa átalakulóban van. Míg korábban a nagy víruskitörések voltak jellemzők, és a károkozók közvetlen pusztításra törekedtek, addig **ma egy vírusnak számos variánsa létezik, melyek a közvetlen károkozás helyett inkább reklámüzeneteket jelenítenek meg** a felhasználóknak.

Az ESET statisztikai rendszere szerint májusban az alábbi 5 károkozó terjedt **a legnagyobb számban Magyarországon**, íme a lista!

1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a májusi fertőzések között: 19.94%.

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET kategorizálása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában (alapértelmezés szerint C:\ Windows\ System32) véletlenszerűen generált névvel fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Honnan lehet tudni, hogy a gépen van: a Windows System32 mappájában véletlenszerűen generált névvel fájl(oka)t hoz létre, melyeknek kiterjesztése .dll vagy .ini.

---

2. WMA/TrojanDownloader.Wimad.N trójai

Elterjedtsége a májusi fertőzések között: 2.13%.

M□ködés: A Wimad.N egy trójai letöltőprogram, amely a Win32/Adware.PlayMP3Z vírust telepíti a PC-re. A kártevő úgy kerül a számítógépre, hogy a felhasználó figyelmetlenül elfogadja a licencszerződést, amellyel egyúttal jóváhagyja a további tartalmak letöltését. Az Adware programok általában azáltal válnak ingyenessé, hogy cserébe bele kell egyezni, hogy reklámokat jelenítsenek meg a gépünkön.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Honnan lehet tudni, hogy a gépen van: a PLAY_MP3.exe állomány jelen van a számítógépen.

---

3. INF/Autorun vírus (2.02%)
Elterjedtsége a májusi fertőzések között: 2.02%.

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár .mp3 lejátszókon) terjed.

Honnan lehet tudni, hogy a gépen van: a számítógép működése drasztikusan lelassul

---

4. Win32/VB.EL féreg
Elterjedtsége a májusi fertőzések között: 1.86%.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg mobil adathordozókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni. Automatikus lefuttatásához módosítja a Windows regisztrációs adatbázisának HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is.

A számítógépre kerülés módja: fertőzött adathordozókon és hálózati meghajtókon terjed.

Honnan lehet tudni, hogy a gépen van: a merevlemez(ek) főkönyvtárában létrehozza az alábbi fájlokat: AUTORUN.INF, sal.xls.exe.

---

5. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a májusi fertőzések között: 1.63%.

Működés: Az Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan Registry kulcsot módosít, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kliens kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.

Honnan lehet tudni, hogy a gépen van: megváltoztatja a böngésző kliens kezdőlapját.

Ezek **öten adják az összes észlelés 25.95 százalékát**, vagyis a további megközelítőleg 74 százalékon már sok, kisebb arányban előforduló kártevő osztozik.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/502061

Kommentek:

mangorlo · http://mangorlo.tumblr.com 2008.06.05. 22:27:51

kétszer kaptam be egy hónap alatt a virtumondét, érdekelne hogy lehet leszedni, mert sehogy se ment, újra kellett raknom windowst

nod32 bejelzett, search and destroy, adaware semmi nem segített, megtalálták, visszatelepült. kihúzott kábel safe módos írtás sem megoldás.

a módszer érdekelne, mert szeretném legyőzni

ja hát igen warez keygenekkel kaptam...

és nem csak felugró ablakok, hanem nem megy a google, és egy csomó más oldal, néha explorer.exe is kimegy

□ók □http://poooOOoook.blog.hu 2008.06.06. 00:36:54

Nem a számítógép fertőződik, hanem a Windows. Megtévesztés azt állítani, hogy a vírusok a számítógépek szinte természetes velejárói. Nem igaz: a vírusok a Windows természetes velejárói. Egy Mac-felhasználó csak a fejét csóválja, ha ilyeneket olvas. Macre ez idáig egyetlen egy vírus sem terjedt el. Nulla. Zéró. Semennyi. Márpedig a számítógépek kb. 5%-a Macintosh...

kgl · http://hobbiasztalos.blog.hu 2008.06.06. 04:19:21

Pedig van mac-re is virus, örülj, hogy eddig még nem kaptál belőle. Linuxra és Unixra is van vírus.
A legkevesebb tényleg a mac-re van, mert ugyanis nem éri meg arra az 5 %-ra külön sok vírust írni.

rigormortis 2008.06.06. 04:21:59

Egyet értek az előttem szólóval! Egy 5%-os "piacra" nem éri meg fejleszteni. Azért jó csak célszámítógépnek a Mac...

Gyulimali 2008.06.06. 07:42:53

Nekem egyszer az ISTBar-ral gyűlt meg a bajom. ADAware észtrevette, letörölte, aztán restart után megint ott volt. Safe mód után megint.
Ekkor, olyan 5x-i ciklus után berágtam, és indítottam TotalCommander alatt egy keresését: *.exe, ami 24 óránál fiatalabb. Ekkor kijöttkb 3 file. ezeket töröltem, és azóta nincs vele bajom.
(esetleg lehet*.com-ra is keresni)
A keygenerátorokkal, és a "biztonsági másolatokkal " kapcsolatban pedig: letölt, jobb-gomb, és scan with xxxantivirus, és csak utána megnyit. Illetve egy másik jó megoldás, hogy winzippel kinyitni, mert általában önkicsomagoló zip-ben van. És csak azokat a fileket kitörölni, amik kellenek, a többit meg törölni.

zala 2008.06.06. 07:58:47

Pók 2008.06.06. 00:36:54

"Macre ez idáig egyetlen egy vírus sem terjedt el. Nulla. Zéró. Semennyi."

virushirado.hu 2006.10.24.

"Szakemberek szerint a Mac felhasználók egyik legnagyobb problémája az önámítás: a közösség tagjai jobb embernek hiszik magukat amiért nem az általános elterjedt operációs rendszereket használják – és emellett az Apple is folyamatosan adja alájuk a lovat. Erre a legjobb példa talán a múlt heti vírusos iPod ügy: a saját felelősség elismerése helyett az Apple a Microsoftot hibáztatta, és újra hangsúlyozta, hogy őket nem érinti a kártevő-probléma.

A megoldás természetesen az érzelmek félretevése, és a jövőben várható veszélyekre való felkészülése lenne. ..."

www.virushirado.hu/oldal.php?hid=6&aid=990

satie · http://321.hu/sas 2008.06.06. 08:23:41

'kétszer kaptam be egy hónap alatt a virtumondét, érdekelne hogy lehet leszedni'

debian.org

kényelmesebb, többet tud, és full biztonságos.

virkid 2008.06.06. 08:37:42

A vírusfertőzések legáltalánosabb módja, ha külső eszközzel boot-olsz. Ebből lehet több féle megoldást találni.
Kapásból: WINLIVE, hirren vagy bart-os. Ezekben lévő vírusirtóval áttekered a gépet. Utána ha sikerült beazonosítani a fertőzést és a felrakott fájlokat, registry értékeket ezeket kitörlöd, persze még "cd"-s oprendszerrel. És hogy minden lehetőséget kizárj, az összes temp-et kitörlöd.(Böngésző + Win) Ha sikeres volt, normál indítás és win frissítése.
ÉS az egyik fontos dolod, amit én elég gyakran elfelejtek sajnos, mindezek előtt a visszaállítási pont kikapcs.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 08:48:38

Helló .Mángorló.!
A NOD-nál még érdemes lehet megnézned a beállításokat is, ki van-e választva a Kéretlen alkalmazások keresése, a kiterjesztett heurisztika használata, stb, Windowsos gépeken jó kiegészítő lehet például a Spyware Terminator és a SpyBot SD, ezek együtt is szépen megférnek a NOD32 mellett. Az ilyen külön kémirtók nem csak az érintett fájlt törlik, hanem bátrabban nyúlkálnak bele a Registrybe is.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 08:57:32

Szia Pók!
Ötletes a felvetés, ez tényleg a Windowsos kártevők toplistája. Viszont a zéró számodat vitatnám Mac és Linux ügyben, technikaileg nem lehetetlen. Főként ha nem csak vírusra, hanem kártevőre nézzük (rootkitek, trójaiak, stb.) akkor ha elenyésző és nagyon kevésszámú is a dolog, de kétségkívül létezik. Pl. nézd meg a RootkitHunter vagy CheckRootkit programokat, amik pont ezekre az OS-ekre készültek.
Van aztán egy olyan gyanúm is, ha például valami csoda folytán pl. a Mac lenne 70%-ban a legelterjedtebb, akkor a vírusstatisztika se így nézne ki, mert akkor már megérné üzemszerűen kártevőket írni rá, ami egyelőre még nincs így.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 09:10:27

Kgl, Rigomortis!
Biztos, hogy nem a vírusírók tudásával van a baj, hanem nem éri meg nekik. Érdek a világ ura - és úgy hiszem, ez igaz. Ameddig a fertőzött gépek, ahova néznek, Windowst látnak, amit sokkal könnyebben levisznek ipponnal a tatamira, nem éri meg erőlködni egy másik rendszeren.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 09:12:43

Gyulamali!
A keygenerátorokkal, és a "biztonsági másolatokkal " kapcsolatban pedig használjunk inkább szabadszoftvert ;.-) :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 09:16:22

Szia Zala!
Az már egy haladás, ha a Maces tábor nem azt mondja, vagy mondaná, hogy "nulla, zéró, stb.", hanem hogy minimális, száz alatti, EGYELŐRE nem veszélyes, a felhasználónak magának kell kattintania, tehát korántsem automatikus, de VAN. A Safari böngésző biztonsági hibája kapcsán félő, hogy a hibabeismerési és javítási készség elkezd majd hasonlítani az MS gyakorlathoz, ami szerintem semmiképpen nem lenne jó a usereknek.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 09:20:54

Szia Satie!
Szívemből beszélsz, Linux rulez :-) De arra is kell gondolni, aki van, aki nem teheti ezt meg: pl. hardcore Wines gamer, AutoCAD, Macromedia Flash, SAP user, stb. De az átlag desktop felhasználók (otthoni és irodai) viszonylag fájdalommentesen átállhatnak, persze ehhez az is kellene, hogy egy közbeszerzési pályázat ne "Microsoft-szerű programot" írjon elő ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.06. 09:25:46

Hello Virkid :-)
Köszi a kommentet, reménytelennek látszó cudarabb ügyeknél hasznos az ilyen módszer. A temp ürítgetéseket emellett minden banki tranzakció előtt érdemes lehet megcsinálni (írjunk rá scriptet :-)

virkid 2008.06.06. 11:20:54

2000 gépet védek folyamatosan. Nálunk egy központi felügyeleti rendszeren keresztül nézem folyamatosan a riasztásokat. Így a napi szinten létrejövő fertőzéseket kiválóan lehet védeni, egy erős tüzfallal megerősítve.
Én itt a spéci vírusok általános levételéről beszéltem.
A win kontra linux-hoz hozzászólva, nálunk is voltak kísérletek, de elég gyorsan megbuktak, a speciális alkalmazások miatt pl:SAP. De helyi szinten is könnyebb fejleszteni win-re, mint linuxra.pl.: vonalkód leolvasó, munkaóra nyílvántartó, vagy csak egyszerű adatbázis kezelés.

Gyulimali 2008.06.07. 00:18:40

Kedves Rambo!

mivel szeretem pl. a Civ sorozatot, és nem átallottam érte pénzt adni, és linux alatt is akarok vele játszani, így sajnos szükségem van NoCD patch-ra is. Amúgy meg a másik kedvenc játékom a Transport tycoon DeLuxe, és még az is megvan eredetiben! De még Win alatt is van, hogy jobb a CD mentesített változet, mint az eredeti. pl. a Heroes 3 volt olyan, hogy minden ismerősöm a crackelt változattal játszott, pedig ott figyelt az eredeti is a polcon, de indításkor annyit xarakodott a játék, hogy az valami rémes volt.
Amúgy a szabad SW érvvel teljesen egyetértek! Én magam is arra törekszem!

Megérkeztek...

2008.06.06. 11:55 | Csizmazia István [Rambo] | 1 komment

Címkék: apeh adó csalás identity theft visszaigénylés személyiséglopás

Sok dolog érkezésének örülhet az ember: legyen az távollétről hazaérkező családtagunk, rég várt levél esetleg csomag, az örök élet vagy ingyen sör. És persze van olyasmi is, **amely érkezésének kevésbbé örülünk**. Azt azért vernei fantázaival is merész jóslatnak gondolhattuk volna, hogy a Virusok Varázslatos Világa 5. részében jelzett megtévesztők pár hónapon belül a valóságban is megérkezzenek kis hazánkba. Pedig így történt, **gyanútlan állampolgárok nevében és személyazonosságukat ellopva - többszáz fiktív adóvisszatérítési kérelmet adtak be** csalók.

Nagyjából 27 millió forintot próbáltak ismeretlenek **visszaigényelni az APEH-től, több régióan is**. A dolog szerencsére két helyen is megbukott: egyrészt a szúrópróbaszerű ellenőrzéskor az érintettek nem is tudtak róla, hogy a nevükben valaki 100-150 ezer forint visszatérítést igényelne, másrészt az elkövetők elkövették azt az amatőr hibát, hogy minden - ez az első hírek szerint 243 darab - csalással szerzett pénzt **ugyanarra a számlára és levelezési címre** kívántak visszaigényelni.

Az eset azért jól mutatja, hogy emberek személyes adatait (név, lakcím, személyi igazolvány szám, adóazonosító szám) **korántsem olyan nehéz megszerezni**. Saját korábbi tapasztalataimból is megerősíthetem, hogy számtalan olyan munkahelyem volt, ahol nem szándékosan - nem ethical test keretében, pusztán véletlenül - olyan tartalmakba ütköztem a mindenki által elért hálózati meghajtókon, amely elképesztő módon fizetési és más bizalmas adatokat is tartalmazott közprédaként. Szerencsére a rendszergazdák mindig megköszönték a figyelmeztetéseket, és gyorsan kitakarították Augiász istállóját, amit nem ritkán **a lusta és fegyelmezetlen alkalmazottak másolgattak ide-oda maguknak** a "könnyebb hozzáférhetőség" kedvéért. Ezekben az esetekben egy rosszindulatú munkatársnak **semmilyen erőfeszítésbe nem került volna** ezeket egy floppyra/cdre/usb kulcsra kimásolni és eltulajdonítani.

De vettem már ki **szemetesből olyan listát** is, amely a Paksi Atomerűműbe történt kirándulás **minden résztvevőjének neve, címe, személyi igazolvány száma** rajta volt, és az utazás után feleslegssé válva nem elégetve, széttépve vagy ledarálva lett, hanem **csak kettéhajtva kidobva**.

Nem árt tudatosítani mindenkiben, hogy ez egy elképesztően jól jövedelmező üzlet, a csalás ilyen formája pedig mindenkire leselkedik, csak tanácsolni lehet az óvatosságatot, azt pedig, hogy a szervezeten belül nem lopják és nem vesztik el az adatainkat - **például mikor lemásolják személyinket mobiltelefonvásárláskor** - mindössze remélhetjük.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/506540

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.21. 12:00:48

Személyes adatokkal éltek vissza, érdekes:
www.penzcentrum.hu/cikk-1012956-1.html

The running file

2008.06.10. 15:41 | Csizmazia István [Rambo] | 1 komment

Címkék: vírus smith mr rootkit autorun autorun.inf mrs msconfig

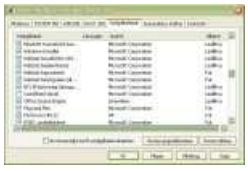
Futottak még - ezt inkább azokra a résztvevőkre szokták használni, akiket egy jobb futamon már szinte nem is jegyeznek a mezőnyben, pedig ezúttal főszereplőről van szó. Running man után running file, **sőt még ráadásul autorun is**, hát mi ez pontosan, hogyan, miért és egyáltalán?

Ha egy külső meghajtón - legyen az pendrive, USB-s merevlemez, CD vagy éppenséggel DVD lemez - található annak főkönyvtárában egy autorun.inf nevű állomány, akkor az abban található "OPEN=" szekciójában található program **azonnal, automatikusan lefut** a Windows rendszereken. Na persze csak akkor, ha **a védelmi programunk nyakon nem csípi**, ha éppen egy kártevő szeretne azonnal és automatikusan lefutni.

A májusi magyar fertőzési toplista 3-ik helyezettjéről van szó, az INF/Autorun vírusról. Az elnevezés egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó és azt manipuláló kórokozóknak. A kártevő fertőzésének egyik jele, hogy **a számítógép működése drasztikusan lelassul**, amely Windows rendszerek alatt fertőzött adathordozókon főleg USB kulcsokon, de akár mp3 lejátszókon is terjed. Egyes vállalatoknál az USB portok tiltásával igyekeznek elejét venni a fertőzésnek, ami elég **primitív fatengelyes módszer**, és az USB eszközök letiltása a hatékony munkavégzést is akadályozhatja.

A dolog érdekessége, ha rápillantunk az **ESET labor ugyanezen, 2008 májusi időszakának USA-beli statisztikájára**, úgy azt láthatjuk, hogy ott nem hogy a bronzérmet, hanem **egyenesen a dobogó legtetejét** aranyéremmel a nyakában foglalja el **az INF/Autorun**.

Emlékezetes, hogy a Mr és Mrs Smith DVD film német változatán rootkites másolásvédelem volt, amely szintén automatikusan lefutva lekapcsolta az összes optikai lemez elérhetőségét. A lelepleződés után aztán közreadták a mentesítő programot is, de ami nagyon érdekes volt, hogy **később már a DVD borítóra egy piros figyelmeztető matricát is ragasztottak**, hogy a lemez behelyezése után **a SHIFT billentyű 10 másodperces nyomvatartásával hatástalanítható** az autorun funkció.



Sok módja van, hogy a CD/DVD és USB eszközök automatikus indulását, az autorun.inf állomány csatlakozás utáni lefutását véglegesen megakadályozzuk. Lehet ez **turkálás a Registryben**, a Powertoys **TweakUI programja**, vagy az **MSCONFIG parancs** használata. "A

jó harcot megharcoltam, a pályát végigfutottam, a hitet megtartottam" - mondja Szent Pál. Mi pedig tartsuk szárazon a puskaport és a vírusirtót, és **autorun helyett fusson csak az és csak akkor, amit mi erre megkért□nk**.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/511430

□ommentek:

Csizmazia István [Rambo] □http://antivirus.blog.hu 2008.11.21. 08:22:05

Autorun ügyben érdekesség:
blog.wired.com/defense/2008/11/army-bans-usb-d.html

Pásztorok lakat alatt

2008.06.11. 17:55 | Csizmazia István [Rambo] | Szólj hozzá!

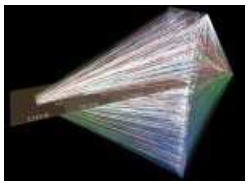
És itt nem a Pál utcai fiúkból ismert vörös ingesek egyik prominens alakjára tessenek gondolni, hanem haladva a korral **botnet pásztorról van szó**, aki terelgeti ~~nyáját~~ botnet hálózatát, amely mintegy 7000 gépből áll és akár **969 Mbps erejű DDoS támadást is lehet vele végezni**. Erre már a Nemecsek anyjával bensőséges viszonyt folytató Janó is csak ingatná a fejét.

Tikkadt botnet PC-k legelésznek rajta...

Már azon sem ütközik meg senki, hogy **az elkövető egy mindössze 21 esztendős** amerikai fiatalember, aki Kaliforniában 2004 és 2006 között intézett támadást **az adathalász ellenes Castlecops** és az online játékosok és grafikusok fórumát üzemeltető Killanet honlapja ellen.

Fotó emberünk Yahoos adatlapjáról

A nem kicsit erős méretű támadások szinte teljesen megbénították a Castlecops weboldalát. Gregory Kinget még október 1-én tartóztatták le, és korábbi beszámolók szerint **többször is támadott önkényesen olyan oldalakat**, amelyek szerinte méltánytalanul viselkedtek vele szemben, és a 2007-es Valentin napi támadás is az ő számlájára írható. Az FBI egyébként keményen és folyamatosan küzd a botnetek ellen, ezek közül King csak az egyik. Ha bűnösnek találják, két éves börtönbüntetéssel kell majd szembenéznie.



A DDoS támadás vizualizált képe

Aki mélyebben is érdekel a téma, itt találhat egy érdekes összefoglalót a botnetekről.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/514973

Kommentek:

Nincsenek hozzászólások.

Ötvenedszer a csúcson

2008.06.12. 13:22 | Csizmazia István [Rambo] | 5 komment

Címkék: vb díj virus rekord award nod32 eset bulletin 100% ötvenedik

Ez **egy kerek szám**, születésnap esetén az ember arra gondol, hogy több van már mögötte, mint előtte; házassági évfordulónál pedig aranylakodalomnak hívják. Nem kis szám ez tehát, mi most az 50. VirusBulletin 100% Award díj elérése kapcsán nézünk be az adatok mögé.

A **100% díj az egyik - ha nem a legnagyobb - szakmai elismerés**, amire szinte minden antivírus gyártó vágyik. Azért szinte, mert éppen most jelezte kiszállását a Trend Micro. A hírek szerint nem tartják elég megalapozottnak a tesztelést az aktívan terjedő (úgynevezett vadon élő, ITW, In the Wild) vírusokkal kapcsolatosan. Az mindenesetre tény, hogy a Trend Micronak az utóbbi tesztek folyamán nem termett babér, és lehet hogy némi sértődöttség is van a dologban. Már nem emlékszem pontosan, kitől hallottam, de van egy **dakota közmondás, miszerint "ha valaki már egyszer képes volt teljesíteni a VB100%-ot, utána már csak elrontani tudja azt"**. A mezőnyből egyébként sokan - **köztük az ESET szakembereivel az élen** - szorgalmaznak egy másik, még bonyolultabb és az élethű körülményekhez még közelebb álló tesztelési metódus kialakítását, ez AMTSO (Anti-Malware Testing Standards Organization néven szerveződik, és reményeink szerint a NOD32 programok ebben a környezetben is jól fognak majd teljesíteni.

Még ha a víruskollekció nehézségét, valósságát esetleg lehet is vitatni, arra nézve viszont igen **szigorú követelmények** vannak, hogy **úgy kell teljesíteni a maximális felismerést** - benne mindenféle kórokozóval: többek közt polimorf vírusok, férgeket, botok -, hogy **eközben nem szabad semmilyen tiszta állományra vakriasztást (false alarm) adni**.

- Failure 1 (February 1998) - akkor még NOD-iCE 7.19
- Failure 2 (November 2000) - NOD32 1.47 verzió
- Failure 3 (April 2002) - NOD32 1.19 verzió

Vissza az ESET tesztek eredményeire, az Ubuntu Linux 8.04LTS Server változata hozta meg az 50. díjat, ami **egyedülálló rekordnak számít**. Visszatekintve az elmúlt évekre, 53 alkalommal indultak a teszteken, és mindössze 3 alkalommal nem sikerült venni az akadályt.

Név	Teljesített teszt	Hibázott teszt	Teljesítmény
ESET	50	3	94.3%
Symantec	44	6	88.0%
Sophos	41	15	73.2%
Kaspersky	42	16	72.4%
CA eTrust	34	13	72.3%
Norman	39	16	70.9%
BitDefender	17	7	70.8%
McAfee	35	20	63.6%
FRISK	20	13	60.6%
Trend Micro	16	11	59.3%
F-Secure	29	24	54.7%
Alwil Avast	25	22	53.2%
AVG Grisoft	22	22	50.0%

A táblázatból látható, hogy eddig **csak két résztvevő tudott 75% feletti teljesítményt nyújtani** az összes indulásához képest, és ez a NOD32/ESET valamint a Norton/Symantec.

Randy Abrams kezében az elismeréssel

A NOD32 **az egyetlen anti-vírus program** a világon, amely az első Virus Bulletin tesztje óta (1998. május) **nem engedett át egyetlen vadon élő vírust sem** a rendszeres tesztek során, és ez a program kapta idáig a legtöbb Virus Bulletin díjat.

A teljes HTML oldal keskenyített JPG-be sűrítve: a lényeg így is lejön

Ha valaki szeretne **bővebben is VB cikkeket, teszteredményeket nézegetni**, weboldalukon ingyenes regisztráció után részletesen is olvasgathat ilyeneket.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/516193

Kommentek:

Algernon 2008.06.13. 12:19:29

Engem az érdekelne, hogy miért vannak jelentős eltérések más tesztlaborok által végzett vizsgálatoknál. Pl. blog.chip.de/0-security-blog/maerz-2008er-security-suiten-im-vergleich-20080310/

Nyilván más a minta, na de akkor melyik tesztnek lehet inkább hinni, melyik tükröz valós teljesítményeket?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.13. 13:16:40

Szia Algernon!
Véleményem szerint érdemes több összehasonlító tesztet is figyelemmel kísérni, és _szakmailag_ a VirusBulletint és az AV-Comparativest tartom a legmagasabb színvonalú külföldi tesztnek. A számítógépes magazinok is adhatnak emellé plusz információt, de ott inkább az ergonómia, kezelhetőség, (nem hivatalos) sebesség, kényelem és összbenyomás alapján szavaznak az újságírók.

Algernon 2008.06.13. 13:25:49

Amit belinkeltem, az nem a Chip tesztje, az av-test.org oldalról származnak az eredmények. De egyébként az AV-Comparatives is eléggé eltérő eredményeket szokott hozni mint a VB.
Szóval eléggé ellentmondásos eredmények születnek...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.14. 12:08:40

Igen láttam, de a német sajna nem az erősségem. Sorry, az AV_test.org is egy neves tesztoldal, ezt tényleg kihagytam a listámból.
Ha pedig a legutóbbi AV-Comparatives tesztre gondolsz (Proactive/Retrospective test, 2008. május), átnézve a riportot az derül ki belőle, hogy a NOD32 programból egy egyedi kísérleti tesztpéldányt kaptak, amiben a csak internetezés közben (IMON modult) által használt heurisztikus STATIK keresőmagot a kézi keresésre is bekapcsolhatóvá tették. Ez számomra megmagyarázza, hogy például a scanning speed miért lett a szokásostól eltérően lassabb.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.16. 11:22:50

A Trend Micro visszatért a Virus Total kebelére ;-)
blog.hispasec.com/virustotal/31

Akkor és most - péntek 13.

2008.06.13. 12:14 | Csizmazia István [Rambo] | 3 komment

Címkék: kis vírus ferenc péntek János 13 friday dos jerusalem checkvir leitold

Azoknak a fiataloknak, akik már nem is láttak PC-t CD/DVD meghajtó nélkül (Commodore 64-ről nem beszélve), valószínűleg nem mond sokat az **a hőskor, amikor a péntek 13-a még ijesztő volt a számítógép használók körében**. Az idősebbek és katonaviseltek ;-) viszont még emlékezhetnek arra az évre, amikor a rádió a Déli Krónikában **arra szólítottak fel mindenkit, hogy aznap lehetőleg ne kapcsolja be a számítógépét**... Miért is történt mindez?

Hol volt, holt nem volt, amikor a hülyét még pontos jével írták, a DOS operációs rendszeres időkben már kezdtek megjelenni az első vírusok. Az akkori **vírusirtók frissítései még körülbelül havi egy alkalommal** jelentek meg a BBS-en (Bulletin Board System), és hol a karakterek estek le a szöveges képernyő legalsó sorába, hol mentőautó száguldott át a képernyőn, esetleg a Yankee Doodle dallamai hangzottak fel a PC speaker hangszórójából. Ez még a feltűnési viszketegségről, a jópofa brahikról szólt (benne leszek a TV-ben :-), nem pedig a mai csendes és alattomos kémkedésről.


Hozzászólás vírusügyben

Korabeli dokumentum a Potyogós vírusról

Sokan tartják **babonaságból a 13-át szerencsétlen számnak**, a péntek 13-át pedig szerencsétlen dátumnak. 1989-ben Péntek 13 névvel jelent meg egy új vírus, amely program és overlay állományokat fertőzött, illetve írt felül. Egyéb ismert (Alias) nevei voltak még: **Jerusalem, Israel, 1813**. Ezek a nevek Farmosi István-Kis János-Szegedi Imre: Víruslélektan című könyve szerint onnan származnak, hogy vírust a Jeruzsálemi Héber Egyetemen fedezték fel, és akkoriban is péntek 13-ra esett az az időpont, amikor a palesztínok elkezdtek harcolni az izraeliek ellen. Az 1813 pedig a kezdeti változat **fertőzési hosszára utalt**: ennyivel nőtt a megfertőződött állományok mérete.

Kis János az elsők között foglalkozott a vírus témával

A Péntek 13 kódja képes volt **állandóan az operatív tárban (rezidensen) megbújva COM és EXE típusú állományokat megfertőzni**. Visszatérve még egy kicsit a leállásra, már akkor sem volt az olyan egyszerű, hogy ne használjanak egy nap számítógépet, hiszen a **közműszolgáltatók, repterek, tőzsdék, kórházak, bankok, hadsereg, adóhatóság** és még sorolhatnánk - már akkoriban is nagyban támaszkodtak ezekre. Ma pedig egyszerűen **kivitelezhetetlen egy ilyen szünet**, és persze az eredeti okot, **a fertőzést sem szüntette meg**.

Ha valaki ismeri a **Checkvir víruslabóratóriumot** és a kapcsolódó Antivirus.hu oldalt **Dr. Leitold Ferenc** gondozásában, az biztos nem lepődik meg, hogy ő már akkor a vírusok elkötelezett és értő ellenségeként írt egy sajátkészítésű víruskeresőt Cs és Egér néven, ahol a Cs betű Tábor Csaba nevű kollégáját jelentette. Ez a **Checkvir nevű program** már keresekedelmi forgalomba is került, és természetesen **hatékony segítséget jelentett nem csak a Péntek 13, hanem a többi vírus ellen is**.

Ma már nem kell tartani a dátumtól

Ez már történelem, manapság **napi többszáz kártékony kód keletkezik**, de szerencsére **senki nem tanácsolja, hogy aznap ne kapcsoljuk be** a gépünket. Ha **frissen tartjuk** az operációs rendszerünket, naprakész vírus- és kémirtót használunk, nem kapcsoljuk ki a tűzfalat, akkor **ezen a napon semmi különleges nem történik, ami máskor nem** - persze ezt a számítógépes értelemben gondolom, ettől még átszaladhat egy fekete macska előttünk, és eshet a fejünkre a tetőről virágcserép ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/517978

Kommentek:

ildsisy 2008.06.13. 20:21:12

erre nem is gondoltam ma,tényleg...pedig...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.14. 12:14:04

Hello Ildsisy!
Még C64-en is volt egyébként vírus anno, pl. BHP (Bayerische Hacker Post) néven floppyról floppyra fertőzött.

Lazításképp pedig belinkelem a Commodore64-re írt Friday 13th játék videóját ;-)
www.youtube.com/watch?v=LnqKzEdZNN0

A jó öreg Commi meg 25 éves volt az idén :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.09.30. 17:56:50

Ezeket most leltem, a régi Víruslélektan és Új víruslélektan könyvek letölthető formátumban:

mek.oszk.hu/03100/03153/
mek.niif.hu/07400/07407/

A vágy titokzatos tárgya: iPhone

2008.06.16. 16:32 | Csizmazia István [Rambo] | 2 komment

Címkék: ebay biztonság iphone rablás csalás

Sok embernek **megmozgatja a fantáziáját esztétikus külsejével, lenyűgöző tudásával**, nem tagadom családon belül is többen kíváncsian várják már a magyarországi eljövetelét, amit talán a T-Mobilenál lehet majd először megvásárolni.

Azonban egy vonzó technikai kütyű megjelenése **sokak számára lehúzási, csalási és rablási lehetőséget jelent**. Pár éve a tolvajok az utcán még arra utaztak, hogy akinek fehér színű fülhallgató van a fülében, az potenciális célpont az iPodjával.

Hallhattunk aztán olyan E-Bay tranzakciókról, ahol romániai csalók a tőlük licitált és megvásárolt árú helyett semmit, vagy **csak köveket és krumplit postáztak** az amerikai és kanadai pórul járt vásároknak. Volt szó az iPhone-beli GPS adatok hamisíthatóságáról, de arról is **folyt a vita**, vajon "hazatelefonál-e" a készülék.

Most arról olvashattunk, hogy **elitélték az első New-Yorki csalókat**, akik hamis iPhone internetes hirdetéssel léprecsalt áldozatoknak semmilyen telefon sem adtak, hanem a személyes találkozáson totálisan kirabolták őket: elvették nem csak a pénzüket, de minden értéktárgyukat is. A kedvező áron kínált iPhonet kínáló banda legalább négy alkalommal bizonyítottan ezzel a módszerrel könnyítette meg az áldozatok pénztárcáját, ellenük rablás és illegális lőfegyver birtoklás a vád.

Az ilyen erőszakos eseményeken kívül is résen kell lennie majd annak, aki **ellenőrizetlen forrásból vagy használtan szeretne ilyet készüléket** vásárolni, ugyanis a feketepiacon máris megjelentek az utánzatok és hamisítványok.

Ha pedig **mégis eredeti, de használt készülékhez jutunk**, lehet esetleg rajta trójai vagy kémprogram, amivel szintén kiszolgáltatottá válhatunk. **Az óvatosságot** minden bizonnyal itt sem tolhatjuk majd a háttérbe.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/523624

Kommentek:

fostalicska · http://fostalicska.blog.hu 2008.06.18. 19:22:38

Érdekes, hogy az ilyen kicsomagolós videókat készítő gyökereknek sosincs egy szaros, pár ezer forintos kameraállványuk, és mindig fél kézzel töketlenkednek.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.27. 17:51:19

Nem új, de tanulságos:
kereso.blog.hu/2008/11/27/celldorado_nyerj_egy_iphone_3g_t

Akár veled is megtörténhet...

2008.06.17. 16:03 | Csizmazia István [Rambo] | 3 komment

Címkék: laptop vírus pornó gyermek hamis trójai botnet vád fertőzött kompromittált

Az alábbi történet elég hajmeresztő, de semmiképpen nem hihetetlen. Herald Michael Fiola **egy használt céges laptopot kapott kölcsön** a sajátja helyett, és a nem működő antivírus program miatt kialakult helyzet **kis híján a vesztét okozta**.

Főhősünket **kirúgták a munkahelyéről, mert vállalati noteszgépén gyerekpornót találtak**. Ha csak ezt az egy mondatot halljuk, akkor gyorsan meg is születik fejünkben az ítélet: pfuj, kötelet az ilyennek ;-) De ha továbbolvasunk (és mint Török Szultánnál, meghallgatjuk a magyarázatot és a hátteret is megismerjük) akkor **kezd csak félelmetessé válni a dolog**. Nem véletlenül mondja az államügyész szóvivője, hogy ez a leghorrorisztikusabb történet, amit eddig látott. Ugyanis bár emberünk becsületes, szexuális és egyéb szokásai is normálisak és egészségesek, csak a sajátja helyett **kapott használt laptop volt kártevőkkel fertőzött**.

A nyomozás során **a szakértő, Tami Loehrs egy egész hónapig vizsgálta az illető noteszgépet**, és tapasztalatairól harmicoldalas jelentésben számolt be. A megsérült vírusvédelmen keresztül megfertőződött a gép, amire **távolról illegális, többek közt gyermekpornó anyagokat töltöttek fel** - a felhasználó tudta nélkül. Úgy értékelte, több vírus és trójai volt rajta, és igen valószínű, hogy korábban egy távoli támadó törte fel azt. Valószínűtlennek tartja, hogy ezeket az állományokat maga Fiola töltötte volna a számítógépre.

Fiola **megpróbáltatásai 2006 novemberében kezdődtek**, amikor azt a bizonyos pótszámítógépet kapta a saját ellopott gépe helyett. Alig egy hónappal később **a DIA (Department of Industrial Accidents) nevezetű, a dolgozókat ellenőrző hivatal informatikusai felfigyeltek rá, hogy ennek a gépnek az adatforgalma aránytalanul nagyobb**, mint a többi munkatársé. Észrevették, hogy mintegy négyszer több adatot forgalmaz, majd **átadták a rendőrségnek az ügyet**, aki megállapították: elképesztő mennyiségű gyermekekről készült pornográf kép **található a számítógép merevlemezén**. Az ügy 2007 augusztusában került a Bostoni bíróságra.

Bár **a talált fotók a webböngésző átmeneti tárolójában (cache) voltak**, a szakértő szerint **nincs bizonyosság arra, hogy felhasználói közreműködéssel** és aktivitással került volna oda. A kerületi ügyészség szóvivője a héten arról tájékoztatta a feleket, hogy a vád hamis volt, és **az ügyet kedden törölték**.

Fiola most Rhode Islandben él, és **reménykedik, hogy a hírnevén esett csorbát valahogy helyrehozza**. Az 53 éves férfi és felesége

összeomlott a hamis vád miatt, barátaik elpártoltak mellőlük és úgy érzik, a mintegy 15 hónapig tartó események teljességgel tönkretették az életüket, ezért pert fontolgatnak a DIA ellen.

A kafkai történet végén mi mást is mondhatnánk: ne igyunk mosatlan gyümölcslevet, és rendszeresen ellenőrizzük, frissítsük biztonsági programjainkat.

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/525399

Kommentek:

Djur (törölt) 2008.07.13. 08:59:43

Ügyes ügyvédi trükk :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.13. 09:33:55

Szia Higgadt !
Könnyen elképzelhető, amit mondasz,valóban van benne egy kis "tudatmódosító cukorkával kínálták meg" feeling :-), de ha a másik oldalt nézed: pl. veszel a szüleidnek egy gépet, vagy a nagymamádnak, akkor tényleg lehet, hogy észre sem venné, nem is értené, hogy mit művelnek vele az interneten keresztül

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.03. 21:25:50

Na ez is egy érdekes eset, hajmeresztő végkifejlettel :-O
itmania.hu/tart/cikk/e/0/30859/1/informatika/Kemprogramok_miatt_bocsatottak_el_egy_tanarnot_az_USAban

Ravasz, mint a róka

2008.06.18. 10:55 | Csizmazia István [Rambo] | 12 komment

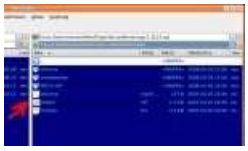
Címkék: firefox plugin kiegészítő biztonsag noscript finjan buherálás

Sokan szívesen használnak Mozilla Firefox böngésző klienst, mert kényelmesebb, és a **megfelelő kiegészítő pluginekkel a biztonsági szint is eredményesen fokozható**. Hogy csak a legkedvesebbeket említsük: NoScript, Finjan Secure Browsing, AdBlock Plus, ShowIP, FireBug, CacheStatus, Cookie Safe, stb. **De mit tegyünk**, ha a nagy világrekord letöltés után **a Firefox 3.0-hoz nincs még frissített pluginünk**? **Hát buheráljunk :-)**

Sok kiegészítő még nem áll rendelkezésre a tegnap debütált vadonatúj 3.0 végleges változathoz.

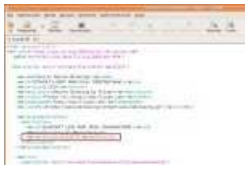
Hohó, ezt sajnos nem engedi telepíteni. Vagy mégis?

A pluginek egyszerű, **XPI kiterjesztésre átnevezett ZIP tömörített állományok**. Ebből kell kiválasztani **szerkesztésre az install.rdf nevű szöveges állományt**, és keresni benne a verzióra vonatkozó infokat.



G. Edit segítségünkre siet ;-)

Ez a "**maxVersion**" résznél a Finjan esetében "2.0.0.*". Ezt most nagy furmányosan írjuk át "3.*"-ra (ez jobb, mint a 3.0, hiszen úgyis jönnek majd a javítások) és **másoljuk vissza az XPI csomagba felülírással**.



A böngészőből a **CTRL+O paranccsal tudunk fájlt megnyitni** és máris indulhat a telepítés.

Ohne zsineg szépen települ, már **csak a böngészőt kell újraindítani**.

A módszer □ □**százalékban működni fog**, és várhatóan hamarosan a pluginek szerzői is észbekapnak és frissítik műveiket.

Telepít, működik, örül :-)

A zenei rádiócsatornák műsorvezetői utálják, ha valaki kér egy zenét, és amikor megkérdezik kinek küldi, **azt a fantáziátlan választ adja, hogy "mindenkinek, aki szereti"**. Az egyáltalán **nem új, de most jól használható trükköt mi most azoknak ajánljuk, akik még nem ismerték...**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/526783

Kommentek:

The Welsh 2008.06.18. 17:43:42

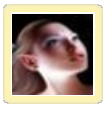
A nightly tester tool nevű extension telepítése lényegesen egyszerűbb.

Blogpont Huba 2008.06.18. 17:46:54

XPI fájlt hol keressem olyan formában, hogy szerkeszthessem is? Előre is köszi - és tudom, hogy láma vagyok :) .

Csizmazia István [Rambo] • http://antivirus.blog.hu 2008.06.18. 17:51:09

Szia Blogpont Huba!
Ezen az oldalon flangálsz és kikeresed ami érdekel:
addons.mozilla.org/en-US/firefox
Az Add to Firefox zöld gombon pedig File Save As/Hivatkozás mentése más néven.
Ennyi :-)



Blogpont Huba 2008.06.18. 17:52:02

Köszi!!!

□rdek Lődő 2008.06.18. 21:10:50

Kipróbáltam, amit írtál, s valóban a legtöbb pluginnál működik a szisztéma.
Azonban felkeltetted az érdeklődésem a Finjan addon iránt és meglepő módon, pont azzal nem tudtam boldogulni. Akárcsak az egyik gyakran használt pluginnal, az XE.com Universal Currency Converterrel sem.
"because: Signing could not be verifed. -260"

Szerinted egyébként ki írna számomra egy olyan plugint, amely a statusbarra 30 perces frissítéssel kiírná az Euro árfolyamát? :-)

Joe Pass · http://vegyes.blog.hu 2008.06.18. 23:46:32

Érdek Lődő,

tessék, neked gugliztam, Forex Fox:
addons.mozilla.org/en-US/firefox/addon/3370

Hogy a status barra írja -e, azt nem tudom... :)

kissbe1234 2008.06.19. 09:38:31

Firebug az jar, annál lehet trükközni?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.19. 10:25:10

Koszi Joe Pass :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.19. 10:26:21

Hello MTM :-)
Igen, a Firebug is szépen müxik így nálam

Érdek Lődő 2008.06.19. 17:20:27

Joe Pass, köszönöm a segítő szándékodat, de sajnos az EUR-HUF árfolyam lehívása és publikálása nem szerepel az ajánlott megoldás szolgáltatásában. Így marad a kérdés, hogy vajon miért nem sikerült a nevezett buherálás, ill. ki az aki ilyen pluginokat szeretettel megír!?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.19. 18:48:21

Kedves Érdek Lődő!
Megnéztem az eredei honlapon is, ott is csak működésképtelen változat van:-(
www.xe.com/ffxtn/

Ha készíttetni akarsz ilyet, szerintem a weblabor.hu oldalon adj fel hirdetést.

Érdek Lődő 2008.06.22. 00:31:38

István!

Köszönöm a tippet és azt is, hogy foglalkoztál a problémámmal!

Hideget is, meleget is kaptunk

2008.06.19. 16:31 | Csizmazia István [Rambo] | 1 komment

Már a részeredmények is biztatóak voltak, most pedig már biztos, hogy a rekord megvolt, az adatok szerint 24 óra alatt mintegy 8.2 millió letöltés történt világszerte, és ebből **hazánk is szépen kivette a részét**. Néha kicsit lehalt a kapcsolat, de az eredetileg tervezett 5 milliós álomhatárt így is sikerült jócskán túlszárnyalni.

Sok hasznos újdonságot üdvözölhettünk, beleértve **a jobb erőforrásgazdálkodást**, a 2.x egyik nagy hibája volt, hogy **két kanállal ette a szabad memóriát**. A másik ami szakmai szemmel szintén hasznosnak újításnak tűnik, az intelligens címsor, az okosabb bookmark, és persze **a csalárd oldalakkal kapcsolatos intő figyelmeztetések**.

Persze **pluszban ilyenkor is jól jöhet** a Netcraft Toolbar, mert ha például XSS (Cross Site Scripting) segítségével eltérített linkre kattintunk, egyből jön a figyelmeztető ablak.

XSS bajok ellen egyébként létezik két külön plugin is XSS Guardian Panel és XSS Warning néven, és a tegnap emlegetett berheléssel mindkettő **3.0 alatt is birtokba vehető**.

Azért hogy **az öröm ne legyen akkora**, hírt kaptunk egy olyan új kritikus sebezhetőségről is, amely a korábbi változat mellett úgyanúgy érinti a vadonatúj 3-as verziót is. A biztonsági javítás készítése állítólag már gőzerővel zajlik, ezt várjuk is nagy tisztelettel.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/529059

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.20. 12:17:12

Néztem ma is a térképet: Dél Korea: 70 ezer, Észak Korea: 0 azaz nulla :-O

Szőnyegjavítás: jobb későn, mint soha

2008.06.20. 12:01 | Csizmazia István [Rambo] | 5 komment

Címkék: windows apple safari patch javítás alatt bomb sebezhetőség carpet

Korábban hírt adtunk Nitesh Dhanjani által felfedezett kritikus sebezhetőségről, ami az Apple **Safari böngészőjében** található. A kutató által csak **szőnyegbombázásnak aposztrofált hibalehetőségek távoli kódfuttatást tettek lehetővé** Windows környezetben, mégis az Apple **nem tartotta fontosnak** a javítást.

Amikor a kártevők jelentős része már **böngészés közben próbál meg bejutni** hozzánk, abszolút nem mindegy, hogy mennyire sebezhető egy kliens. És az sem mindegy, hogy a már felfedezett hibák **mekkora időintervallum után kerülnek befoltozásra**: addig ugyanis olyan, mintha **egy nagy célkeresztet tetováltattunk volna a homlokunkra**. Dhanjani megmutatta, hogyan lehet a hibát kihasználva **teleszórni a felhasználó asztalát kéretlenül letöltött állományokkal**.

Később aztán Aviv Raff pedig **nyilvánosságra hozta** azt a módszert, amellyel a Safari és az Internet Explorer együtt már **tetszőleges kódot lehett futtatni az áldozat gépén**, ami azért nem hangzott túl jól. **Tiszta szívünkből féltettük azt a tíz embert**, akik Windows alatt IE, FF vagy Opera helyett Safarit használnak ;-)

Most **végre megtört a jég**, és a tegnapi nap folyamán napvilágot láttak a **javítások** a 3.1.2 változatban. Azért azt érdemes megjegyezni, hogy az Apple részéről mind a kritikus hibákra kiadandó frissítések sebességén, mind pedig a problémás esetek kommunikációján **lehetne még mit javítani**.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/530395

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.20. 14:53:45

Halihó!
Megnéztem, de itt minden rendbenlévőnek látszik :-O Vagy ez csak "vírus marketing" volt? ;-)

Inimma 2008.06.20. 14:59:19

Intellektuel, hol törték fel ezt szerinted?

Cigiző · http://cigi.blog.hu/ 2008.06.20. 16:26:21

Ja, ez csak czúnja virus marketing - mindenhová ezt a szöveget nyomja, le kell szedni, oszt'jónapot!
Nálam is jártak...

Karbonade · http://magyaropera.blog.hu 2008.06.20. 16:28:39

Szerintem ez csak kommentspam, illetve gerillamarketing magyar módra. Szánalmas.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.24. 11:41:13

Állítólag a javítás dacára még él a probléma:
blogs.zdnet.com/security/?p=1319

A hülye is tud férget írni

2008.06.24. 22:09 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: worm to trójai trojan féreg generátor

Hancu kolléga egy korábbi írására rímelhet ez a mostani bejegyzés. **Szomorúan állapíthatjuk meg, hogy túl könnyedén**, szinte Guiness rekordokat megszégyenítő sebességgel (kb. 1 perc guglizás után) már tölthetjük is le álmaink programját: a bármilyen futtatható állományból wormot generáló kézi készüléket ;-)

A **Trojan to Worm** V2 megfelelő lelki defektusokkal rendelkező egyének számára ígéretes nevű **generátor program már önmaga is riasztást okoz** a víruskeresőben, ezért hogy egyáltalán nézegethessük, nos ehhez **ki kellett kapcsolni a valósidejű védelmet**.

A program **igazi internacionalista mű**, az alap spanyol mellett szerencsére van angol, de emellett gondoltak a portugál és katalán felhasználókra is. Magyarul sajnos vagy inkább **hál'Istennek nem tud**, ezért remélhetőleg Pistikék helyett inkább Carloskák fogják próbálgatni ;-)

Sok szakismeret nem is szükséges a használatához, kattintunk, legördülőből választunk, oszt annyi. Betöltünk hát egy kiválasztott állományt, és nekilátunk, hogy az egyébként **ártalmatlan zsebszámológépből (Calc.exe) pudingpróbáló zombinyuszit faragjunk**. A hivogatóan csillogó nagy zöld Generate gomb megnyomása előtt azért még lesz egy pici dolgunk.

Beállítási lehetőségek egész garmadája fogadja a nagyérdeműt. Az **UPX tömörítési lehetőség már szinte alapfelszereltségnek** számít. A Mutex lehetőség valószínűleg egy külön végrehajtási szálat tud rendelni a készítendő programhoz. Az automatikus indulás történhet a Rendszerleíró adatbázis (Registry) betöltési részének átírásával, de akár egy szkript is intézheti ezt. Nagy antidemokratikusan ;-) beállítható, hogy **milyen USB eszközökön ne fertőzzön**, vagyis a gazdi gépét nem szabad összegányolni. Akár **indulási és végdátumot is beállíthatunk** a fertőzési folyamat szabályozásához.

Elméletileg **egy üzenet ablakot is fel lehet dobni** valamilyen elmés vagy félrevezető üzenettel, ez a feature azonban nálunk látszólag ne működött.

Tetszőleges programokat blokkolhatunk is a checkboxba helyezett pipákkal: példának okáért a Firefox, az Opera, a parancssor, vagy a Regedit eshet áldozatul a manővernek. Mindenesetre látszik, hogy a lokalizációs csapat még nincs a topon: **ők ottan nem beszélni teljesen angol bele oda neki ...**

Ha **már mindenhová pipát tettünk, ami élt és mozgott**, akkor nem marad más hátra, jöhet a várvavárt nagy zöld Generate, és persze az is, hogy anyakönyvezzük az újszülött lényt ezúttal **calc2worm.exe néven**.

A **NOD32 szépen jelzi**, hogy itt valami köbgyök próbálkozik zsebszámológépnek látszó tárgynak látszani;-)

Ha **megvizsgáljuk művünket a VirusTotalon**, azért némileg oldódik a gombóc az ember torkában: nem minden papsajt alapon ennyire könnyen azért nem adják egy vadonatú kártevő készítését.

Mindenesetre **öröm lehet az ürömben**, hogy hasonlóképpen a Shark generátoros tapasztalatokhoz, **a futószalagon készült állatfajtákat** az antivírusok többsége is **futószalagon ismeri fel.**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/536426

Kommentek:

Nincsenek hozzászólások.

Légy résen!

2008.06.25. 18:07 | Csizmazia István [Rambo] | Szólj hozzá!

Nem kell ezt kétszer mondani a kártevők íróinak, biztatás nélkül is tudják. A mai támadások döntő **többsége már valamilyen biztonsági rést kihasználva** igyekszik befészkelni magát rendszerünkbe.

Most a Microsoft Office és Wordpad alkalmazásokhoz bukkant fel olyan preparált dokumentum, amely **egy jelenleg is nyitva álló sebezhetőséget** kihasználva igyekszik megfertőzni a Windows operációs rendszert futtató gépeket, és képes távolról tetszőleges kód lefuttatására. A demonstrációs kódokat Ivan Sanchez publikálta, ezekben rendezetlen listalemek okoznak hibás feldolgozást. A jelenség az Office 2000 és 2003 verziót is érinti, és **az SP2 valamint SP3 csomag telepítése után is** jelen van, a Wordpad pedig a Windows alapvető része, amely minden gépen szerepel.

Várhatóan a javítás megjelenéséig növekedni fog azoknak a weblapoknak a száma, ahol ennek **a résnek a kihasználásával igyekeznek majd kártékony kódokat bejuttatni** a látogatók gépeibe.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/538911

Kommentek:

Nincsenek hozzászólások.

Hülye fejem van és itt vannak a földrengések ;-)

2008.06.26. 12:33 | Csizmazia István [Rambo] | 8 komment

Címkék: spam féreg kártevő exploit nuwar heurisztika

Kinek a pap, kinek a papné. A megtévesztő levelek - bennük a **kártékony kódokkal egyre csak jönnek és jönnek**. Az már csak tálalás kérdése, **kinek mi az érdekes**, ki mikor és miért hágja át mégis az óvatosságot és kattint az izgalmasnak vélt tartalomra.

Hát ezt is megértem, **több különböző forrásból is megerősítették** - többek közt a híres Chrissie Benedick valamint a mindenki által jól ismert és közmegbecsülésnek örvendő Felike Muh, és mindenki jó barátját, Barclay Kordát se felejtsem ki - , hogy **"what a stupid face you have here rambosoft..."** kezdetű becses leveleküt idézzem. Nem tetszik nekik az ábrázatom - nem is értem, miért ;-)

És még mondják, hogy az internet elidegenít: egy frászt, ennyi baráti levél után ez cáfolva. Talán mondani sem kell, hogy a mellékelt Video1.exe nem eltorzult, félig állati, de félig sem emberi orcájú önarcképet mutat, **hanem egy Win32/Nuwar férget** próbál meg letölteni a gépünkre.

A kretén fejét is **magam voltam kénytelen** elkészíteni Cartoonist segítségével. Innen már csak egy lépés az albán vírus;-)

"Üdvözlöm!

Én egy albán vírus vagyok, de a hazámban nagyon elmaradott a technika, ezért magamtól nem tudom tönkretenni a számítógépét.
Kérem, töröljön néhány fontos fájlt a számítógépéről és küldjön tovább más felhasználóknak is.
Köszönöm az együttműködéstét, üdvözlettel:

Albán vírus"

Persze **a kínai földrengések is jó apropót** szolgáltatnak. **Aki kíváncsi, hamar megöregszik, illetve inkább hamar fertőzött lesz a gépe**.

Ha a kínai fölrengés után érdeklődünk, **egy videólejátszó ablaknak látszó** tárggyal szembesülünk: ám ha az egeret fölévisszük vagy a FireBuggal belenézünk, látszik hogy **egy 9-es erősségű csalás keretében a Nuwar.DA féreg Beijing.exe néven próbálkozik letöltődni** a gépünkre.

Bár sem a fenti, sem a mostani állományt nem mutatta ki a VirusTotal szerint a NOD32 - igaz ott még a 2.7-es változat ketyeg - **valós környezetben azonban a program (ESS) szépen megfogta mindkét esetben**. Mindkét fogás jól láthatóan ("valószínűleg...", "módosult") **a heurisztika találata**.

Jó lenne már megérteni mindenkinek, hogy **a spamek nem pusztán az időnket pocsékolják** - bár ezt is teszik - hanem **szinte mindig a biztonságunk ellen indítanak támadást**. Akit valamilyen **témakör érdekel, az ne szedett-vedett kéretlen**, Petro Sanchezek meg Malyomváry Armandók által küldött levelekből, vagy általuk küldött linkekből akarjon tájékozódni.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/540166

Kommentek:

□lgernon 2008.06.27. 10:25:32

Az ESS mellett miért van másik tűzfalad is, István? (spa9.jpg) :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.27. 10:33:07

Szia Algernon!
Jelentem, nincs több tűzfal :-), miből gondolod?
Ha esetleg a kék pajzsról van szó, az a Spyware Terminator ikonja.

Algernon 2008.06.27. 11:27:12

Igazad van, ezt benéztem. :) Csak annyian bántják az eset tűzfalát, hogy gondoltam, kicsit piszkálódom. :)
(Nekem egyébként "bejött" az ESS, de sokan kritizálják, pl. www.matousec.com)

A poszt egyébként nagyon tetszett, ezeket az "internet-dzsungelben" kalandozós írásaidat szeretem.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.27. 12:42:55

Igen, emlékszem, írtam is rá első felindulásomban:
www.pcworld.hu/forum/index.php?showtopic=11583&st=60#
Azért azt remélem én is, hogy a következő tesztben már jobban fog szerepelni :-)

Algernon 2008.06.27. 14:00:16

Addig is ha valaki még nagyobb biztonságban szeretné magát tudni, annak ajánlom az ingyenes, kicsi, s nagyon könnyen kezelhető DSA (Dynamic Security Agent) programot. Tűzfal mellé telepíthető, kiegészíti azt.
Egy leírás róla:
www.privacyware.com/dynamic_security_agent2.html

Autonomous Foe 2008.06.29. 02:41:22

Tiszteletem!
Ez jó, rég találkoztam ilyen dologgal, mint amit Te csinálsz. Én is nemrég sz*ptam be egy nagyon makacs trójait, Avast!, NOd32, McAfee stb. ellenére. Kezdek hozzászokni. Ha esetleg tudnál ajánlani egy freeware címet, hálás lennék....bár ez így elég h*lyén hangzik.....Mármint ezen médiumon keresztül. Mindenesetre további sok sikert, egészséget a bloghoz, hajrá!!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.29. 11:07:39

Szia Autonomous Foe!

Köszi a jókívánságokat :-)

100%-os védelem nincs, de amiket tudnék javasolni:

- ha NOD32-t használsz, (Chip és PCWorld olvasók ingyen kapnak havi kódot hozzá) beállítások: legyen bekapcsolva az AntiStealth, a kiterjesztett heurisztika, a kéretlen alkalmazások keresése, a veszélyes alkalmazások keresése: ezek közül nem minden van ALAPÉRTELMEZETTEN kiválasztva.

- Bármilyen AV-t is használsz, érdemes mellé külön kémirtót is telepíteni, sőt akár többet is: pl. Spyware Terminator, SpyBot SD, Dynamic Security Agent, stb. - ezek mind freewarek otthonra.

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.06.30. 09:11:40

Még egy fegyvertény az ingyenes programokkal szemben a fizetősök mellett: a szakszerű technikai támogatás. Ha valaki NOD32-t használ, és megfertőződik a gépe, a support azonnal segít neki a problémáján. Az ingyenes megoldások használói magukra maradnak a problémáikkal. Ez is egy fontos szempont lehet.

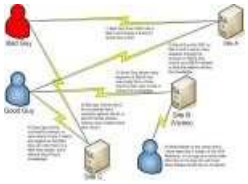
Horgászok a banki oldalakon

2008.06.30. 13:15 | Csizmazia István [Rambo] | 1 komment

Címkék: domén bank támadás xss phishing hsbc adathalász .bank

Eddig sokan úgy vélték, elég egy hitelesített banki belépés előtt egy weboldal valódiságát a https kapcsolathoz tartozó kulcs/lakat **ikon és a tanusítvány puszta meglétével** ellenőrizni. Bár még ennyit sem tesz meg mindenki, úgy tűnik, néha még **ez is lehet édes kevés**.

A HSBC banki oldalak XSS támadhatóságáról adtak hírt nemrégiben. Ez nagyjából annyit tesz, hogy a biztonsági hibák miatt megfelelően kialakított **XSS kódokkal átirányíthatók** a bank DNS adatai. Ilyenkor pedig az ügyfél úgy gépeli be az adatait, hogy szinte semmi esélye észrevenni, **nem is az igazi oldalon jár**. Korábban egyébként már előfordult a Barclays-nél, és Dancho Danchev szerint úgy tűnik, a biztonságért felelős **szakemberek nem veszik elég komolyan** az ilyen típusú támadásokat. Olasz bankok ellen már az év elején igyekeztek az XSS-t felhasználni. Bár ez az eset valószínűleg nem érint magyarországi ügyfeleket, dőreség lenne úgy gondolni, ez **más bankkal és más országban a jövőben nem ismétlődik meg**.



Amit a szakértők javasolnak: rendszeresen **frissítsük** operációs rendszerünket, mindenképpen használjunk **antivírus és kémirtó** programot, a tanúsítványnál ellenőrizzük le annak **lejárati dátumát és a tanusítvány ellenőrző összegét** is. Részesítsük **előnyben a Firefox és Opera** böngészőket, és támogassuk meg gépünk biztonságát egy **komolyabb tűzfal** programmal is. És léteznek külön XSS ellenőrző Firefox pluginek is, érdemes lehet őket kipróbálni.

Egyes vélemények szerint az is félő, hogy **1-2 betűs eltéréssel** egyező domén neveket fognak tömegesen lefoglalni, hogy ezzel is **kihasználhassák a zavaros helyzetet**. Mint ismeretes, a tavalyi évben Mikko Hypponen tett egy olyan javaslatot, amely többek közt a pénzintézetek domain neveire a .bank TLD végződést javasolta. Ezzel **ha mindent nem is lehetne megoldani**, de valószínűleg szintén használna az adathalász támadások elleni védekezésben.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/545703

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.11.06. 06:46:41

Annak idején Mikko Hypponen javasolta. hogy legyen külön .bank domain az adathalász támadások ellen. Ha minden ellen nem is véd, a problémák nagy része ellen hasznos lehetne. Most úgy néz ki, lesz is belőle valami.
www.domainabc.hu/aktualis/domain-tld-newtld-ujvegzodes/1318/

Indexes címről spammelni

2008.06.30. 20:27 | Csizmazia István [Rambo] | 21 komment

Címkék: spam letöltés indexes hajnalka fizetős e mailcím emília

Mi a hasonlóság a sas meg a bakter között? Igen, egy régi viccről van szó, és azoknak van igazuk, akik az alábbi választ adták: "**A sas baromi magasan száll, a baktert ez meg baromira nem érdekli**." Körülbelül ennyi lehet **a kapcsolat Kov Emilía és Nagy Hajnalka között** is: mindketten elmehetnének szerintünk melegebb éghajlatra, legalábbis 10-ből 9 címzett biztosan ezt ajánlja nekik...

Mikor a pofátlan spamekről szó esett, úgy gondoltuk, nehéz felülmúlni, illetve talán **valamilyen belső késztetés révén (lelkiismeret, becsületesség, empátia) esetleg netalán-tán kimegy a divatból** a fizetős letöltési oldalak gerillamarketingje, de a szikár tények azt mutatják, hogy nem ez a helyzet.

Induljunk Nagy Hajnalkával, **aki az ilu25693@index.hu e-mail címről támad be minket kéretlen levelével**, és **válaszol egy olyan kérdésre, amit nem is tettünk fel neki** - valószínűleg költői lehet ez a kérdés ;-)

Nagyobb indulatokat korbácsolhat viszont lelki békénkben Kov Emilía (dia90638@index.hu) - legalábbis az ő kéretlen levelének láttán **felmenőivel kapcsolatban több találgatás bukik ki a földi halandó száján**, amelyekben **rinocéroszokról és varangyosbékáról esik szó**, valamint furcsa nászukról és **az abból született félig állati, de félig sem emberi lényekről**. A Baby megszólítás nem talált és nem is süllyedt, hiszen egyáltalán **nincs szerencsénk ismerni egymást** és csak sajnálni tudjuk, hogy ennek ellenére mégis emlékszik az e-mail címünkre, sőt láthatóan **a legelső címzett neve is megakadt neki a fejében** - lehet hogy komoly mentalista, sőt ezzel az adattal szerintünk **egyenesen gondolatolvasó!**

Rettentő unalmas már ez a **"szióka, milyen volt a buli, ja igen küldöm amit kértél..."** bizalmaskodás, Kávéházi Konrádos bennfenteskedés. Egyszer még lehet valami jópofa, később már fárasztó és szánalmas. Aki pedig olyan elfajzott;-) hogy fizetős letöltést keres, enélkül is talál ilyet tucatjával.

Szóval mindkettőjüknek ezúton üzenjük: **húzz el Baby** és ha egy mód van rá, legközelebb lehetőleg **ne emlékezz a címünkre**, köszike, **jah és majd elfelejtettem**, itt a link, amit kértél a multkor ;-)

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/546574

Kommentek:

nemethv · http://backtotheukblog.wordpress.com 2008.07.01. 01:13:00

Ezeket en is kapom, szerintem az independence v a revolution adta el az emailcimem vkinek :S
Egyebkent a gmail spamszuroje mar egy ideje nalam szuri eleg jol ezeket. (Eddig szerencsere azt hiszem h egyetlen 'normalis' levelem se ment a spambe ezek miatt, de szemmel tartom azert)

Uglee · http://nagydobraverem.blog.hu 2008.07.01. 01:38:00

Nosö.
Ping, ripe.net
A file-ok (legalábbis amit én néztem) lakhelye toy.smsbse.hu
IP: 194.50.101.231
Az IP lakhelye: 1B Telekom Ltd. Hévízgyök
Kontaktszemély:
person: Zoltan Egri
address: 1B Telekom Ltd.
address: Szechenyi u. 43.
address: 2192 Hevizgyork
address: Hungary
phone: +36 20 559 1243
e-mail: ripe@1b.hu
nic-hdl: ZE86-RIPE
mnt-by: ONEB-MNT
remarks: ----------
remarks: Please send all abuse and spam complaints to:
remarks: abuse@1b.hu
remarks: ----------
source: RIPE # Filtered

Ebjúz ímélcímet elárasztani, telefont felhívni, jelezni neki, ha két nap múlva nem tűnik el a cucc, rendőrségen feljelentést tenni az adott információkkal, és Egri Zoltán bátyót is gumibottal seggbe kuratni, lobogtatva a hangfelvételt és az e-mailváltást.

Vagy lehet blogon siránkozni.

dark future · http://www.andocsek.hu 2008.07.01. 01:54:44

Komoly cég lehet...

anti hipi□ □ i□2008.07.01. 02:06:23

Küldenék valamit én is a fent nevezett spammer patkányoknak: img2.tar.hu/refresh/size2/27418302.jpg
:)

algi 2008.07.01. 03:05:49

"este gyere"? Mind a tíz címzett?

Eddig ahányszor létező, magyarországi ember küldött nekem spamot (és nem külföldi bot), és feljelentettem a hírközlési hatóságnál, ott mindig sikerrel jártam.

spam-bejelentes kukac nhh pont hu

(Vajon ide mennyi spam érkezik?)

A bejelentéskor el kell küldeni a saját nevedet, címedet, valamint a spam teljes fejlécét is. Sok sikert!

soseleszekelső 2008.07.01. 07:46:57

Én nemrég totalcar-os címről kaptam...

Cigiző · http://cigi.blog.hu/ 2008.07.01. 08:24:22

Én visszaírok nekik mindig. Ezt: "ha még egy levelet kapok tőled, megbaszom anyádat a ravatalon"
Segít.
;)

Hurrá Torpedó · http://www.youtube.com/watch?v=br-D7UneS0E 2008.07.01. 08:54:07

cigiző:
felesleges visszaírni. ha normlisan csinálják akkor ezek nem is létező e-mail címek.

és is küldhetnék bárkinek bármilyen e-mail címről levelet, pl pamela@anderson.hu-ról is

Perillustris 2008.07.01. 09:09:06

A legnagyobb hiba visszairni barmit is vagy kattintani a linkre, mert azzal siman "ervenyesiti" az ember a mail cimet.

Magnat 2008.07.01. 09:50:31

Hi,

legalább a két spamoldal címét kitörölhetted volna a levelekből, h ne csinálj nekik ingyéreklámot.

OkoskaTo:rp 2008.07.01. 09:52:44

Mi lenne, ha a címzettek mind eleget tennének a felkérésnek, és meglátogatnák személyesen - no nem a levélben szereplő fiktív csajt, hanem az eredeti feladó fickót?

yooccoo 2008.07.01. 09:53:58

hu.spam.wikia.com/wiki/Kateg%C3%B3ria:1B_Telekom-spamek

□aveSlim 2008.07.01. 10:06:25

Az a baj, hogy a feljelentéssel semmit sem érsz. Te hallottál már arról, hogy vkit magyarországon megbüntettek ezért? Még az amcsiknál sincs sok ilyen per...

Annyit lehet tenni, hogy annak az ip-nek a tulajdonosát értesíteni, akiről kiment a spam.

A legjobb az lenne, ha egyszer ki lehetne deríteni, hogy ki használta az adott ip címet..... És megkeresni... És... levágni a pöcsét; anyját felgyújtani, stb.

DaveSlim 2008.07.01. 10:12:25

Még a Coldfusion nyomta igen keményen az elején....
aztán valamiért megszűntek az ilyen spamek...

Mostanában, Szervernet-es ipről, 1B telekomosról jönnek a spamek.
Jah.. és kezdenek átállni a Vodafone-os netről való spamelésre.
Ugyanis a Vodafone az egyetlen, amelyik azt írja vissza nekem mindig, hogy sajnálják, de nem tudnak mit tenni (nem akarnak) és iratkozzak le! :O Nagyon buták még a nethez, hálózatokhoz... ezt meg isírtam nekik :) De hát mit is vár az ember egy GSM szolgáltatótól, aki közben netet is ad...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.01. 10:13:31

Hello Magnat!
Köszi, igazad van, javítottam, no ingyen ingyen reklám

ehhh 2008.07.01. 10:28:56

en azt nem nagyon ertem, hogy protokoll szinten az email miert ad lehetoseget nem letezo cimrol irni. hogy nagy kunszt lenne a egy domain szervertol valo lekerdezeshez kotni a kuldest?

uglee: azt hogy lehet kiderinteni, hogy honnan jon a spam?

illetve ezek a weboldalak vajon teljesen jogszeruen mukodnek? nem hiszem, lehet, hogy a feljelentes nem is a spam miatt kene, hanem a celweboldal ellen. vagy oket meg nehezebb megfogni?

Hurrá Torpedó · http://www.youtube.com/watch?v=br-D7UneS0E 2008.07.01. 12:05:18

ehhh. azért ez nagyon bonyolult lenne.

nekünk pl a céges emailszólgáltatónknak köze nincs a domain, és tárhelyszolgáltatónkhoz. mégis ugyan az a végződés.

illetve pontosítok, mert kell hogy legyen létező e-mail cím amiről kimegy a levél, csak a levél header információi átállíthatóak. szóval levél elmegy, és azt látod xy küldte, de közben az a zy@abc.hu címről lett elküldve. de ez az infó hozzád már nem jut el...

a normálisabb tárhelyeken, vannak olyan paraméterek amiket nem lehet átállítani, így mindenképpen továbbításra kerül az eredeti cím, vagy legalább a szerver infója amiről küldték. de avatatlan szem ezeket azt se tudja hol keresse.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.01. 12:16:46

Itt van két részlet az üzenetforrásokból:

1. levél
Received: from dsl5401C011.pool.t-online.hu [84.1.192.17]
by with HTTP; Mon, 30 Jun 2008 06:52:26 +0200

2. levél
Received: from dsl5401C011.pool.t-online.hu [84.1.192.17]
by with HTTP; Mon, 30 Jun 2008 06:52:41 +0200

Jól láthatóan egy helyről, 15 másdoperces különbséggel jöttek.

ehhh 2008.07.01. 13:29:37

hurratorpedo: ugyertem, ha emilkliensben letrehozok egy felhasznalot, pl zy@abc.hu -t, akkor letoltesnel szol, hogy nincs ilyen pop3 szerver, de ha megadok egy smtp klienst, akkor siman elmegy a level. legfeljebb az ip szamom derulhet ki, nem? nincs mas emilcim, ami kiderulhetne.

Hurrá Torpedó · http://www.youtube.com/watch?v=br-D7UneS0E 2008.07.01. 14:16:26

más elvileg nincs. e-mail cím legalábbis. de ha meglesel outlookban egy levélforrást, vagy a teljes eredeti üzenetetet, akkor a fejléce tele van olyan infóval ami elmegy a levéllel együtt csak alapból nem mutatja meg neked az outlook (sem más levelező). azokból csomó infó leszűrhető.

a spammelők ezért pl php programokkal támadnak, és a futtató szerver pop, és smtp beállításait használják.

Elemér_ · http://nonprofit.info.hu/blog 2008.07.02. 09:24:38

Pár napja minden reggel vár egy újabb internetes "csajom" kedves levele, hogy innen és eztés azt töltsek le. Nagyívben megy a kukába. A spamszűrő nem boldogul vele, hisz magyarul van és többi spam angolul.

A maiak a következő helyről jöttek:
Received: from dsl5401C7D5.pool.t-online.hu [84.1.199.213]
by with HTTP; Wed, 02 Jul 2008 07:21:13 +0200

hogy ez valós-e, azt nem tom.

De sz@rjon sűnt aki küldte.

Szerva itt, SQL injection ott

2008.07.03. 15:32 | Csizmazia István [Rambo] | 1 komment

Értekeztünk már többször is, **mekkora veszélyt jelent**, ha rosszindulatú kódokat tartalmazó bannerhirdetésre kattintunk, illetve hogy milyen gondot okozhat, ha egy nagylátogatottságú portált sikerül megfertőzni. A **sportszerető** fanatikusok most ismét veszélybe kerültek.

Ezúttal **a nemzetközi teniszszövetség**, az ATP (Association of Tennis Professionals) honlapját módosították ismeretlenek úgy az SQL injection technikával úgy, hogy a látogatók észrevétlenül kártevőket: trójai és kémprogramokat töltöttek le a számítógépükre.

Itt nem is annyira nyitott biztonsági rés kihasználása történik, mint inkább **a nem megfelelően biztonságos szerver oldali programozás** miatt nyílik lehetőség az effajta manipulációkra. A megfelelő **vírus- és kémprogram védelem nélküli gépek megfertőződnek**, és felettük átvehető a vezérlés, a támadók tetszőleges kódot futtathatnak rajtuk és becsatlakoztathatják ezeket a botnetes hálózatukba.

A támadás **még júniusban kezdődött és jól is volt időzítve**, mert a még ezekben a napokban is **zajló Wimbledoni torna** miatt kiemelkedően nagy a látogatók száma.

És amíg ráadásul az átlagfelhasználó hajlamos nem frissíteni a böngészőjét, addig **magas labdát ad** az ilyen bűnözőknek. Amit azok stílszerűen fogalmazva nem átallanak majd ezt egy jól irányzott lecsapással pontra váltani.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/551349

Kommentek:

Algernon 2008.07.11. 14:40:20

Mr. AqWeEy elmehet a fenébe. Az egyik kedvenc oldalam:
www.sorlap.hu

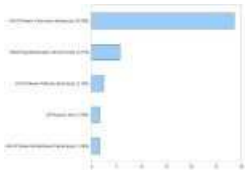
Ó trójai, miért vagy te Virtumonde?

2008.07.07. 16:47 | Csizmazia István [Rambo] | 12 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Míg júniusban a legtöbb fertőzést az **online játékosok adatait gyűjtő vírusok okozták világszerte**, addig **Magyarországon még mindig** a felhasználók által telepített, ingyenes .mp3 **tartalmakat ígérő Virtumonde** családba tartozó károkozók terjednek a leginkább. Következzen a **NOD32 antivírus rendszert gyártó ESET ThreatSense.NET Center felmérése.**

Számos vírusirtó cég közöl statisztikát arra nézve, hogy mely károkozók végzik a legnagyobb pusztítást az interneten. Az **ESET statisztikai rendszere azonban egyedülálló módon képes az egyes országokra lebontott** vírusstatisztika közlésére is, és **nem csupán az e-mailekben terjedő** károkozókról ad átfogó képet, hanem a számítógépet http protokollon keresztül, böngészés közben megfertőzőkről is.



A júniusi adatokból kiderül, hogy **Magyarországon továbbra is a Virtumonde** végzi a legnagyobb pusztítást. Az ingyenes .mp3 tartalmakat és letöltéseket ígérő károkozót a gyanútlan felhasználók saját maguk telepítik számítógépükre. A Virtumonde elsősorban **kéretlen reklámokat jelenít meg a megfertőzött gépeken**, így böngészés, vagy az operációs rendszer használata közben felugró üzenetekkel találkozunk.

Ezalatt **a világban az online játékosok adatait gyűjtő**, a Win32/PSW.OnLineGames családba tartozó károkozók terjednek leginkább, melyek nemzetközi szinten összességében a júniusi fertőzések 13,29%-ért felelősek. A **több mint 30 ismert változatban létező trójai** billentyűzet-figyelő képességgel rendelkezik, és rootkitként rejti el magát a számítógépen. Az online játékokra vonatkozó adatokat – például a belépéshez szükséges felhasználónevet és jelszót – készítőinek továbbítja, akik többek között arra használják a megszerzett információkat, hogy **az online játékokban összegyűjtött virtuális pénzt és a felépített karaktereket valódi pénzzé tegyék**. Egy jól felépített, megfelelő képességekkel rendelkező karakter ugyanis **akár több száz dollárt érhet** meg azon türelmetlen játékosoknak, akik nem kívánnak maguk bajlódni harcosuk vagy varázslójuk tanításával.

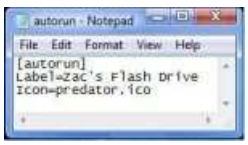
Júniusban az alábbi károkozók terjedtek hazánkban a legnagyobb számban:

1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a júniusi fertőzések között: 28.56%
Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET kategorizálása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben **megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni**. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában (alapértelmezés szerint C:\ Windows\ System32) véletlenszerűen generált névvel fájl(oka)t hoz létre.
A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

2. WMA/TrojanDownloader.Wimad.N trójai
Elterjedtsége a júniusi fertőzések között: 5.61%
Működés: A Wimad.N egy trójai letöltőprogram, amely a Win32/Adware.PlayMP3Z vírust telepíti a PC-re. A kártevő úgy kerül a számítógépre, hogy a felhasználó **figyelmetlenül elfogadja a licencszerződést**, amellyel egyúttal **jóváhagyja a további tartalmak letöltését**. Az Adware programok általában azáltal válnak ingyenessé, hogy cserébe bele kell egyezni, hogy reklámokat jelenítsenek meg a gépünkön.
A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

3. Win32/Adware.AdMedia alkalmazás
Elterjedtsége a júniusi fertőzések között: 2.35%
Működés: Windows rendszereken terjedő **kéretlen reklámprogram**, amely eltéríti illetve **manipulálja az Internet Explorer böngésző** forgalmát. A megtámadott számítógépbe beépülve különböző kártékony DLL állományokat hoz létre, illetve tölt le az internetről, a Registry adatbázisba pedig olyan bejegyzésket készít, amellyel gondoskodik arról, hogy a kártékony kód minden rendszerindításkor automatikusan lefuthasson. Működése során **több különböző kártékony weboldalhoz is megpróbál kapcsolódni**, és a megfertőződött rendszer a tulajdonos tudtán kívül képes más weboldalak ellen indított DoS támadásban is részt venni.
A számítógépre kerülés módja: Trójai programokkal titokban, észrevétlenül települ a gépre.

4. INF/Autorun vírus
Elterjedtsége a júniusi fertőzések között: 1.59%.
Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy **a számítógép működése drasztikusan lelassul**.
A számítógépre kerülés módja: fertőzött adathordozókon (akár .mp3 lejátszókon) terjed.



5. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a júniusi fertőzések között: 1.58%
Működés: Az Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan Registry kulcsot módosít, és **kéretlen reklámokat jelenít meg** az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait és **adatokat gyűjt** ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kliens kereséssel kapcsolatos beállításait és az **alapértelmezett kezdőlapot is**.
A számítógépre kerülés módja: megváltoztatja a böngésző kliens kezdőlapját, reklámok jelennek meg.

Ezek öten adják az összes észlelés **39.69 százalékát**, vagyis a további megközelítőleg 60 százalékon már sok, kisebb arányban előforduló kártevő osztozik.

Bővebb információ a Win32/PSW.OnLineGames **családba tartozó károkozókról** az alábbi linkeken érhető el:
http://www.eset.hu/virus/psw-onlinegames-dnz
http://www.eset.hu/virus/psw-onlinegames-nfn
http://www.eset.hu/virus/psw-onlinegames-nla
http://www.eset.hu/virus/psw-onlinegames-nmy
http://www.eset.hu/virus/psw-onlinegames-nnu

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/557375

Kommentek:

Erőforrás 2008.07.08. 18:04:54

Ez érdekes leírás, és statisztika.
Elolvastam a blogot, de ahogy nézem, ez végig a Nod32-ről szól.
Megnéztem a korábbi írásaidat kedves Rambo.
Két kérdésem lenne:

Miért jöttél el a 2f Kft.-től?
Ha a Nod32 a legjobb víruskereső, ahogy állítják, akkor például ha megfertőződik a gép például a Virtumonde kóddal, akkor miért nem képes eltávolítani?
Nem szeretném piszkálni a Nod32-t, mert nincs tökéletes védelem, de sajnos még az új 3-as verziónál is fennáll, hogy nem távolít el rendesen vírusokat.
És nagyon sok fórumon erősen leírják a Nod32-t. Azt hiszem, nem véletlenül. Egy biztos, az adatbázisa, nagyon gyenge.

Erőforrás 2008.07.08. 18:34:35

Még egy:

A win32/PSW OnlineGames kód nevét honnan vettétek, hogy a Kaspersky-nél Packed.Win32.NSAnti.r ?
Utána kéne nézni, hogy a Kaspersky-nél is szintén OnlineGames-ként szerepel.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.08. 19:34:56

Helló Erőforrás!

Igyekszem sorban válaszolni. 2003 meghívást kaptam a PC World-be online szerkesztőként, és érdekelt, izgatott ez az új feladat. A blog indulásakor írt beköszöntőben vázoltam az eddigi pályafutásomat, ami valóban sokfelé vezetett.
antivirus.blog.hu/2007/09/17/bekoszonto_12

100%-os védelem valóban nincs, szerintem mindent összevéve a profi heurisztikával rendelkező "nagyok", mint az Eset, a Kaspersky hosszú távon jól teljesítenek, még akkor is, ha időnként a megjelenő új változatokból nem is vesznek azonnal mindent észre.

Sok fórumon látom én is a különböző, sőt esetenként szélsőségesen elvakult véleményeket, hitvitákat, flamwart, néha hozzá is szólogatok. Úgy látom, rettentő elszántan dolgoznak a fejlesztők, és ezt én az egyre javuló program zálogának látom.

A vírusok nevét MINDIG a víruslaborban adják. Az elnevezések valóban eléggé kaotaikusan lettek mára, sokan még az eredeti CARO nevezéktani ajánlásokat sem tartják be sajnos. Ezen nem igazán lehet segíteni. Az akkori szabályokról például itt lehet olvasni:
vx.netlux.org/lib/asb01.html

Az Erő legyen veled :-)

Erőforrás 2008.07.09. 08:27:36

Szia Rambo!

Köszönöm a válaszod. Ez korrekt volt.
Abban egyetértünk, hogy tökéletes védelem nincs, és nem is lesz.
A hitvitákat én sem kedvelem, mert egy olyan felhasználónak, aki abszolút ész nélkül nyit meg mindent, és nem ért alapvető dolgokhoz, sosem lesz tökéletes védelme, és mindig kapni fog valami kártevőt. A felhasználói butaság ellen nem véd semmi!
A Nod32-t jó, nagyon jó programnak tartom. Bár én otthon, illetve a cégnél Kaspersky-t használok, használunk. Mivel rendszerinformatikus vagyok, sajnos nálunk olyan programra van szükség, aminek nagyobb az adatbázisa, a sok alkalmazott tudatlansága miatt. A részemről, sosem gondolkoztam úgy, hogy mi a legjobb, és mi nem az. Egy olyan felhasználónak, aki betart bizonyos szabályokat, minimális védelem is elég! Így, a Nod32 is megfelelő védelem. A magam részéről tényleg jó programnak tartom, de ahogy írtam, én azt hiányolom, hogy gyenge az adatbázisa! Ha ezen fejlesztenének, akkor azt gondolom, magasan lehetne a legjobb mind közül.
Viszont, ha van valamilyen internet elérhetőséged, örömmel kooperálnék veled.

Kellemes napot! ☺

UI.: Az Erőforrás informatikai ihletettségű név. ☺ Gondolom a jelentése tiszta. ☺

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.09. 17:11:26

Szia!
Itt találsz hozzám email címet:
www.commodore64.hu

FK 2008.07.10. 23:00:03

Sziasztok!

A statisztika érdekes, ahogy ez az egész kémprogram téma is a NOD32-vel. Már régóta használjuk több helyen is a régi és az új NOD32-t egyaránt, és nagyon jól működik, de önmagában azért nagyon kevés is. Az egyik gépen például Rbotot találtunk, miután az használhatatlanul lelassult, egy másikat meg WinAntivirus fertőzte meg és folyamatosan felugró ablakokkal zaklatott, de a NOD el sem tudta távolítani. Pedig mindkettőn rendszeresen frissített védelem működött, és az egyik gépet ráadásul csak munkára használjuk, még csak nem is nagyon fut rajta böngésző.
Végül mindkét gépet külön kémprogram eltávolítóval tudtam csak megtisztítani (a CounterSpy jött be a legjobban, azóta is ezt használom), ezért szerintem a NOD32 kémprogram eltávolító nélkül csak önámítás. A NOD nagyon jó, és tényleg okos, de hát vírusokon kívül van más is amire figyelni kellene. Aki nem hiszi el, az meg töltse le például a CounterSpy-t egy olyan gépre amit az egész család használ, szánjon rá időt és futtasson le egy teljes keresést, és meg fog lepődni az eredményen.

fav0r 2008.07.11. 09:38:51

Hu, ezzel a virtumondeval nagyon sokat szívok:(Elvileg már letröltem a drágát mivel a nod32 ldalán jelzett fájlok már nincsenek a windows/system32 mappában ill. a precesses között sem, de még mindig előfordul néha, hogy leáll a windows exploler, mikor guglizni próbálok.(
Most SpywareDoctort futtatok, so far so good, de már nem vagyok biztos benne, hogy mindent leszed.
Jelenleg Vista Home Basicem van, de a napokban kapott a gépem pár új hardvert, és lenne egy Vista Home Premium CD-m. Ha most upgradelem a vistámat, akkor ez a kis rohadék átkerülhet a Premium rendszerembe? Csak mert nem akarok mindent letörölni és úgy feltelepíteni a cuccot.
Van valamilyen hatásos (biztos) módszer ennek a vírusnak a leszedésére? Köszi előre is.
üdv, fav0r

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.11. 11:15:16

Helló Ferenc!
Szeretem én is több oldalról megalapozni a biztonságot, a találó hasonlattal élve az sosem baj, ha több zár is van az ajtón. Nálam még 2-3 féle külön kémirtó van a gépen, ami például abban is különbözik egy vírusirtótól, hogy adott esetben bátran belenyúl és töröl a Registryben, míg a vírusirtók általában csak a fertőzött állományt törlik.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.11. 11:21:50

Szia fav0r!
Azt, hogy mi is fut a gépedben, legjobban egy Process Explorerrel lehetne megnézni.
Nem ismerem a Vistát, de azt javaslom, hogy végezz egy teljes keresést (minden opció maxra állítva) a NOD-dal, és kedvenc kémirtó alkalmazásaiddal. Nekem a Spyware Terminator és a SpyBot SD muzsikál. Ha nincsenek gyanús processzek, mindegyeik progi lefut és nem jelez, szerintem kerülhet át. Külön tűzfalról nem irtál, de ha esetleg nem használsz, azt is mindenképpen javaslok, és ez interaktív módban az igazi.

fav0r 2008.07.11. 17:05:39

to Rambo:
a smart sec kétszer is lefutott, a spybot s&d is kb 20x és még vagy 5 antispyware progit töltöttem le és futtattam végig, hiába. Ráküldtem az Avastot is, de az sem tudott mit kezdeni vele.

Mindegy, végül meguntam, lementettem egy SD kártyára a munkáimat és újraraktam a rendszert. A smart sec és az spybot azonnal felkerültek, bár tudom, hogy én voltam a ... és tulajdonképpen én pakoltam fel magamnak a cuccot XD

wmiki · http://apostolimagyarkiralysag.hu/ 2008.07.27. 12:25:04

Hali!

Ismertek olyan virust, ami (azon kívűl, hogy fertőzi és lassítja a gépet) nem engedi elindulni a virusírtó programokat WinXP alatt?
Illetve néhány programot enged (CureIT, MacAfee, ClamAV), de azok viszont nem találják meg.
NOD, VundoFix, meg néhány másik irtó viszont nem tud elindulni, csak bevillan.
Mi lehet ez? És hogyan tudnám leszedni?

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.24. 21:55:50

Már nem csak trójai, de féreg formájában is "élvezhetjük":
biztonsagportal.hu/uj-lenduletet-kapott-reklamgyaros-trojai.html

Az kérem úgy történt, hogy elvesződött...

2008.07.08. 14:39 | Csizmazia István [Rambo] | 2 komment

Címkék: notebook laptop adat titkosítás mentés ellopott noteszgép

Amikor adataink biztonságáról van szó, **hajlamosak vagyunk csak a vírusokra, kémprogramokra leegyszerűsíteni** mindezt. Persze ez is egy nagy szelet a tortából, de számítógépek - például a laptopok - esetében van itt más is.

A hardvert - többek között az különbözteti meg a szoftvertől, hogy **bele lehet rúgni** ;-) De Murphy noteszgépekre adaptált másik törvénye is sokat nyom a latban: "Ha elveszhet, el is veszik. Ha ellophatják, el is lopják."

Korábban is esett már szó kínos és kellemetlen esetekről: Coppola gépének ellopásáról, **különféle kormányzati szervek elkallódott adathordozóiról és noteszgépeiről**, amelyeknek közös jellemzője, hogy a **gép értékének sokszorosát érő adatok** voltak rajtuk. Coppola esetén egyszerű a képlet, ott a saját - persze pótolhatatlan - szellemi terméke, míg a többi esetben **a mi, a jóhiszemű vétlen állampolgárok adatai kerültek** - nos nincs válasz rá, hogy hova is pontosan. Eltűnt, feladták postán, ellopták, elveszett, elvesződött: lehet reménykedni, hogy esetleg talán nem került rossz kezekbe. Ilyenkor ha az illetékesnél rákérdeznek, hogy az érzékeny adatoknál használtak-e egyáltalán valamifajta titkosítást, **a válaszokat - hasonlóan az úrinők válaszaihoz - illik kétkedve fogadni**. Ha azt mondják **igen, az azt jelenti hogy talán**. Ha azt mondják **talán, az azt jelenti hogy nem**. Az is lehet, hogy ha igent mondanak, akkor az illető nem is úrinő vagy mégsem ő az illetékes az adott ügyben :-)

Ez is lehetne Murphy törvény: amit feladnak, az el is veszik ;-)

Ezúttal a Daily Mail volt kénytelen mentegetőzni, mert **alkalmazottak ezreinek adatait tartalmazó laptopot loptak el tőlük**. Ők is **"reménykednek", hogy azóta biztosan leformázták a gépet**, és az adatok nem jutottak illetéktelen kezekbe.

Ha úgy általában **a saját munkánkat mentjük, ez csak az érem egyik oldala**. Ez attól óv meg, hogy a saját munka - amelyet a gyári szoftverekkel, Windowsokkal ellentétben egyik boltban sem vásárolhatunk meg újra - **el ne vesszen**.

Kovács Brigitta most tudja meg, hogy ~~a lotto heti~~ mentés híján mindezt begépelheti újra. Mennyi?!

Az érem másik oldala, hogy a számítógépnek, és a mentésnek is úgy kell a biztonságot szolgálnia, hogy az **ne kerülhessen illetéktelen, rossz kezekbe**. No ez az a folyamat, ahol a legtöbben - és nem csak magánszemélyek, de cégek is - elvéreznek. Arra még csak-csak **rávehetők az emberek, hogy néha CD/DVD lemezre, és USB kulcsra kimásolják** a dolgaikat, de arról már jóval kevesebben gondoskodnak, hogy ezek az adatok **ne legyenek mindenki által olvasható formában** és így veszélyben. Kitől is óvjuk ennyire? Ez lehet kíváncsi kolléga, betörő, tolvaj, de lehet tisztességtelen szervizes alkalmazott is. Vajon átgondolta-e már valaki, milyen kár érheti-érhetné, ha egy csaló szervizes **minden adatát orvul, titokban lemásolná, eladná a konkurrenciának, feltenné az internetre, zsarolna vele**, stb. amíg az javítás alatt van?

Útmutató a "megfelelően erős" jelszó választásához...

i lehet a megoldás? A hétköznap ember szintjén egy elfogadható kompromisszum a **mentések jelszóval védése** - például ZIP, RAR tömörítvényekkel és egy kellemesen erős jelszóval, a számítógépen pedig valamilyen **titkosított partíció használata** a személyes, másokra nem tartozó állományokhoz. Erre egy jól használható program lehet a TrueCrypt, amely mind a Windows, mind a Linux, mind pedig a MacIntosh platformra elérhető, ráadásul **nyílt forráskóddal és ingyen.**

Van egy mondás: **csak olyan információt küldj el emailben, amit akár bárki láthat egy hirdetőtáblán is** - utalva arra, hogy az elektronikus levelezés alapesetben sima szövegként utazik. Erre rímelve **alkossunk mi is** egy új közmondást: **csak azt tartsd a számítógépeden titkosítás nélkül, amit aztán bárki nyugodtan elolvashat** (például ebédszünetben távollétedben valaki belenéz, szervízbe viszed, elveszted, ellopják a gépet, etc.). Isten hozott a való világban!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/557229

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.22. 09:06:09

Itt a menetrendszerű következő angliai eset:
hvg.hu/vilag/20080822_borton_rab_adat_wales.aspx

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.03.24. 18:07:02

Ez érdekes: az eddigiekkel szemben nem a szervizes fedezi fel és jelent a kuncsaft javításra beadott eszközén esetleg található

pornóról, hanem egyenesen ő maga másol fel rá ilyet:
www.technet.hu/telefon/20100324/kemenypornoval_erkezett_a_mobil/

Magilla a vasfüggöny mögött

2008.07.09. 16:49 | Csizmazia István [Rambo] | 4 komment

Címkék: tartalom video amerikai aol cím amazon ip korlátozás proxy virtuális webkártya torpark

Magilla Gorilla lesre indulunk, és bár felkészültünk a nehézségekre, **lesznek nem várt buktatók**, de annyit már most elárulhatunk, végül happy enddel zárul a történet. Úgy látszik, **a ki veszi, ki viszi kérdésre nem is olyan egyszerű** a válasz. És hogy mi köze ennek a számítógépes biztonsághoz? Több szálon is **lesz kapcsolat**, ezt előre megígérhetjük.

Sajnos vagy hál' Istennek, korom miatt (a negyvennyolcadikat taposom) még emlékszem, sőt **szeretettel emlékszem** az olyan régi klasszikus rajzfilemkre, mint a Foxi Maxi, Maci Laci, Rugóláb Seriff vagy Magilla Gorilla. Akkoriban még 40 filléres zsemle, kötelező iskolaköpeny hozzá rövid haj, a trafikban szálra árusított cigi, és még fekete-fehér TV volt, rendszeres hétfői adásszünettel, ezért a gyerekfejjel nézett sorozatok megőrzése szóba sem jöhetett. A jó tíz évvel későbbi ismétlésről pedig - **bár már méregdrágán megjelentek az első videomagnók** - sikerült lemaradnom, hogy közben katonazubbonyban hazafiasan **fogkefével moshassam fel a laktanyában a lépcsőházat** Zalaegerszegen.

Az elveszett fogkefe keresése ;-)

A rajzfilmek szeretete nem csökkent, később aztán kapott egy weboldalt is - amit azóta is jól elhanyagoltam, viszont szépen **megőrizte** a legnagyobb kedvencek, kb. **300 film 4000 feletti képét**, ahol a HTML kódot még Clipper'87 programjaim segítségével **generáltam automatikusan**. Sokszor próbálkoztam **epizódokat letölteni YouTube és egyéb oldalakról**, de nem is nagyon volt - pláne a teljes gyűjtemény -, és a minősége is sokszor csapnivaló volt: vagy Pixel Péter hancúrozott a képen (értsd gyatra felbontású minőség), vagy spanyolul ment a szöveg **angol helyett**, ami számomra valahogy kevésbé szórakoztató :-(

Amerikai-e vagy?

Végül sikerült egy olyan oldalt találni, ahol fent volt a tartalom, de ekkor **jött az arculcsapás**: csak a piszkos kapitalisták gülü szemeinek ;-) engedélyezik ezt, Kelet-Európa nem nézheti. Kellene valami eszköz, amivel IP címet lehetne váltani. Igyekeztem minden furmányt bevetni, néztem Torpark mögül, kipróbáltam a ProxySelt, keresgéltem nyitott, amerikai egyetemek proxy címeit és állítgattam hosszan a böngészőt, plugin hegyeket próbáltam ki, és igen, sikerült **a működést eszméletlenül lelassítani**, viszont makacsul csak **jött az alábbi üzenet: Az ön területén ez a műsor nem engedélyezett**.

Win és Linux juzereknek jól jöhet

B tervként a júliusi Chip magazinban is vázolt **HotSpotShield programját** szemeltem ki, igaz ez **csak Windows és Mac** platformon elérhető. A telepítés elején igyekeztem nem belefutni kéretlen ikonháttér, képernyővédő, etc. programokba, amiből **majd egy tucat tolakodna a gépre**, így a **HSS kivételével mindenre nemet** nyomtam, és indult a rendszer. AOL videó oldal beizzít, Magilla hivogatás ezerrel, de óh minő fájdalom, szanzsén beintenek nekünk ismét. Azért a program nem teljesen haszontalan, csak éppen nekünk most nem segített. Akik a Lost, a 24, vagy egyéb **mostani népszerű sorozatokra** gerjednek, azok a HotSpotShield segítségével Magyarországról is meg tudják nézni az epizódokat például a hulu.com oldalon. Ennek ellenére **egy hideg sört fel tudok ajánlani** annak, aki ezt az AOL videó kérdést mégis megtrükközné valahogy a jövőben ;-)

Itt is lehet tesztelni, hogy minek látszunk

A nem működő torrent linkek böngészése után következik az **mazon webáruház, minden könyvek és filmek anyja**. Oppsz, és tadaaam, kapható is a termék :-) Az ára pedig egyenesen hihetetlen, ötezer valahányszáz forint (40 USD) a négy azaz négy darab DVD lemezt tartalmazó teljes kollekció ára, amiben **már a tengeren túli postázás díja is bennefoglaltatik**. Gyors közvélemény kutatás a baráti körben, vásárolt-e már valaki innen, de még sajna nem. Hát akkor kalandra, illetve biztonságos internetes vásárlásra fel!

Virtuális kártya a virtuális térhez

Ehhez természetesen **nem szeretnénk az "igazi" dombornyomott bankkártyánkat** veszélynek kitenni, ehelyett igényelünk egy külön virtuális webkártyát. Ennek az az előnye, hogy **csak annyi pénz van rajta, amennyit mi előtte ráteszünk**, így nem tudnak túlvonni, ellopni, stb. **Vásárlás előtt 1 perccel odautalok**, megeszi, elfogadja, és ennek a papírkártyának a számát bátran begépelem akárhová, így meg van a tiszta, száraz, biztonságos érzés.

Itt kérünk elnézést a csapnivaló képminőségért, telefonnal készült :-(

Azt már sokszor láttuk, hogy **a bécsi út másik végén (Commodore64, Gorenje, stb.)** és az óceán túlpartján **(USA, Japán pl. a Nikon, Canon, stb. fényképezőgépeknél)** milyen **óriási különbség van az áraknál**. Sokan emiatt vásárolnak inkább külföldi webáruházban, de néha van olyan eset is, amikor valami **ritkaságot, máshol nem kapható terméket** keresünk, mint jelen esetben, akkor pedig muszáj szétnézni a nagyvilágban.

Megrendel, átvesz, örül

A **regisztráció sima ügynek** mutatkozik, a belépés **természetesen SSL felületen** zajlik, amit ha akarunk, az SSL Blacklist pluginnel is csekkolhatunk. **A tanúsítvány** valódinak és érvényesnek látszik, az utolsó akadály is elhárulni látszik a Magilla felé vezető úton. A június 20-án feladott rendelés **körülbelül 3 hét alatt**, gondosan és alaposan csomagolva, sértetlenül szépen megérkezett. A mutatvány közben pedig a **weboldalon végig lehetett követni, hol tart éppen a folyamat**: rendelés feldolgozása, csomagolás, szállítás.

Remélem, a mai könnyfakasztó retro feeling emlékek mellett azért sikerült némi nemű hasznos és a gyakorlatban mások által is használható információkkal szolgálni, vagy ha nem is, legalább szórakoztató volt :-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

- Mai szavunk pedig: keyjacking

□ bejegyzés trackback címe:

http:□□antivirus.blog.hu/api/trackback/id/560234

Kommentek:

ficcske 2009.07.10. 13:40:55

ezek a rajzfilmek nagyon jók voltak annakidején.
Volt az RTL klubon nem olyan rég egy rajzfilm csak sajnos a címét nem tudom. Dinós rajzfilm volt. Mutáns dinókrol szólt.

ficcske 2009.07.10. 13:51:00

Ha valaki tudja a címét akkor, írja meg a címét magyarul és angolul.

ficcske 2009.07.10. 14:16:58

előre is köszi

titan 2010.05.04. 12:40:51

Nemtom azóta nézegetted-e, de az AOL átállt Jútúbra, és nekem trükközés nélkül lejátszotta a keresettet (az izzítós linkre kattintottam előtte)

Rekord: ingyen antivírus 80 kilobájtban

2008.07.10. 00:28 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: ingyen antivírus

Sok zseniális agyú programozó létezik, de a **mostani szerzőnk** Einstein, Bill Gates és Stephen Hawking egyesített szürkeállományával alázza porig a jelen Nortonjait és Kasperskyjeit.

Zsenink fiatal korában biztos 4 KB-os sceene partykat nyert zsinórban, és most **elérkezettnek látta az időt, hogy tudásával önzetlenül szolgálja az emberiséget ebben az elanyagiasult világban**. Kéretlen levélben kínálja fel mesterművét: "Downloda nwo!" A helyesírás órákról viszont szemlátomást hiányzott szegény.

Talán még agykontroll tanfolyamot is végzett, mindenesetre az emberi természettel azért tisztában van. Az **ingyen kulcsszó** sokaknál sajnos még mindig varázsszó.

Az oldalra lépve - **döntésünket meg sem várva, máris indul a letöltés**, és az AntivirusXP2008Installer.exe fájl ugrik elő. Ami egy jólfejlett **Nuwar féreg**...

A VirusTotalban dolgozó 2.7-es nem, de az új NOD32 3.0 **már felismeri a kártevőt**.

Furcsa, hogy a Domaintools-zal nézve focis nevű oldalunkat, az 2008.07.07. én bejegyzett, de **mégis 2002.-től van a "copyright" az oldal alján fenntartva**.

Az pedig végképp érdekes, hogy egy ilyen nevenincs oldal **éppen az □ S□ elnevezéseit és szintaktikáját** használja **a hamis havi top 10-es listában**.

Meg kellene már tanulni, hogy a **nevenincs ingyen programok komoly veszélyt jelenthetnek**, és nem szabad az ilyenekben megbízni. És köszönjük ~~Emese~~ Gub Magnus, **kenje a hajára ezt a trójai letöltő programot!**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/561348

Kommentek:

Nincsenek hozzászólások.

Micsoda? Firefox és Skype? Azonnal letörölni!

2008.07.11. 10:27 | Csizmazia István [Rambo] | Szólj hozzá!

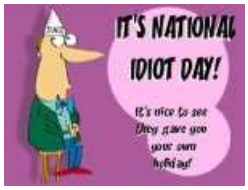
Címkék: szoftver európa eff idiótaság vírusok egyen parlement

Sok **félelmetesen ostoba** dologról lehetett már hallani, és **ez a mostani sem akármilyen**. Imádjuk az olyan ügyintézőket, szervezeteket, bizottságokat, amelyek ilyen semennyire sem átgondolt és empatikus;-) javaslatokkal ügyködnek.

Egyen gépet egyen szoftverrel - lehetne a mottója az Európa Parlament (lehet hogy most büntiből nemecsek ernősen kisbetükkel kéne írni) javaslatának, ahol még azt is meg akarnák szabni, egyes országokban milyen böngésző, milyen VOIP program legyen az engedélyezett. A szakma persze hüledezve figyeli, mikor a hülyeség már Sándor Györgyösen szólva "citerázik" és félve **szurkol, hogy a józan ész azért mégis diadalmaskodjon** a végén.

Mindenki más internetezési szokásokkal, igényekkel, tudás szinttel rendelkezik, és gondoljunk csak arra, milyen kémprogram elleni arzenált használunk a különféle vírusirtók mellett. Ha egyszer csak azt monjdák: minden eddigi program töröl, és mától kezdve mindenhol csak és kizárólag például a McAfee lesz használható, ez pedig kötelező, és slussz, a törvényszegőknek pedig irány a börtön. **Akkor majd a Linux is tilos lesz? És igényeinknek megfelelő saját programot sem írhatunk?**

Túl az ötlet Nagy Testvéres vonatkozásán - előre a lenini úton - egy dolgot azért még mindenképpen érdemes figyelembe venni: aki ismeri az életjáték című kis programocskát, az biztosan tudja, milyen **pusztító lehet a hatás, ha mindenhol egyen rendszereket**, egyen szoftvereket talál. Aki még emlékszik a **2003-as SQL Slammer** pusztítására, azt érti miről van szó. Egy elemző cég későbbi jelentése szerint a megfertőződött SQL szerverek 90 százaléka már **a járvány első tíz percében áldozatul esett**. A homogén kialakítás - például az egységes **bárhová nézek, ott Windows terem -** mindennél jobban **kedvez a vírusok, kártevők** pusztításainak.



Már csak ezért is rettentő nagy ostobaság lenne egy ilyen határozat. A **"Micsoda, a gyermek fiú? Pedig itt az anyakönyvben világosan az áll, hogy lány! Akkor vágjuk le neki!"** típusú hozzáállás helyett inkább az épeszűbb **"Akkor talán javítsuk ki az anyakönyvet!"** megoldás születésében reménykedünk.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/563345

Kommentek:

Nincsenek hozzászólások.

Ez nem diszlexia

2008.07.14. 13:05 | Csizmazia István [Rambo] | 3 komment

Címkék: spam link kód diszlexia kártékony betűcsere

Sokan **kapunk kéretlen leveket**, és az már régóta ismert, hogy a spamszűrők többek közt kulcsszavak szerint is képesek a levelek kiválogatására.

Az ott egy diszlexiás

Nem lehet könnyű az élete egy valódi Rolex ügynöknek vagy a cégük dolgozójának, hiszen ez a szó már annyira le lett járatva a kéretlen levelekkel, hogy szinte nulla az esélye, hogy bármilyen hivatalos levele célhoz érjen. A spam fronton zajló harc egy állandó macska-egér küzdelem, és **elsőként mindig a küldők víritják az új ötleteket**, amire aztán hosszabb-rövidebb késéssel lépni tudnak a biztonsági cégek.

A betűcseréknek emellett **nem csak a szűrőfeltételek kijátszásában** jut szerep - bár ez a fő célja - hanem tudományos megfigyelések szerint **szinte semmilyen érthetőség csökkenéssel nem jár** az olvasó felé. Agyunk úgy működik, hogy automatikusan helyre rakja az ilyen felcserélt karaktereket, nézzük csak meg a Viagar, iVagra, Cailis szavakat tartalmazó leveket.

Tegyünk egy konkrét próbát, ideírunk egy mondatot, és nézzük meg, mennyire zavarja meg a szövegértést a betűk felcserélése, vegyünk egy mondatot az Indexről:

Brá 2001 óat niscn támogatsá a Winwods 3.11-hze, a beágyazott rendszerekzeh mági használták atz. Enenk anozban rövidenes véeg, metr novembetről a Microsotf nme ad ik ötbb licentec a prorgamhzo.

Több delikvenssel is végigolvastattuk a mondatokat, és **azonnal, szinte folyamatosan képesek voltak az eredeti, korrigált és helyes szöveget** olvasni a suta, felcserélt szöveg olvasása közben.

Ez a jelenség azonban tapasztalatunk szerint csak az e-mailekre jellemző, a linkelt **weboldalnál már bizalomcsökkentő lenne** a helyesírási hibákkal tarkított oldal. A kártékony kódokat letöltő oldalaknál - melyek csak igen rövid ideig - órákig, maximum napokig - találhatóak meg egy adott URL címen amúgy is egy fejlesztői kitből, készletből használják a terjesztők, ott pedig a kész weboldal sémán nincs is mit elrontani.

Ami miatt számunkra mindez érdekes lehet, hogy egyre **nő a kártékony kódokat letöltő linkekre mutató spamek száma**, ezért nagyo nem mindegy, mennyire sikerül magunkat ezektől távoltartani.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/567149

Kommentek:

Persze 2008.07.14. 20:03:42

Sajnos ismerjük, SSL FTP és portcsere szükséges, 6000 felé feltenni.

kacsa! 2008.07.21. 22:49:08

Hol lehet azt a "rambosoft" programot letölteni? :) Bizalomgerjesztőnek tűnik...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.22. 10:23:31

Helló kacsa!!
A programot nem lehet letölteni, a C64-es időkben a nicknevem volt :-D
antivirus.blog.hu/media/image/200807/rambosoft.jpg

A tizedik utáni parancsolatok

2008.07.15. 21:46 | Csizmazia István [Rambo] | 2 komment

Címkék: kína földrengés számla feltörés vöröskereszt csaló

Ha valaki **esetleg nem ismeri az első tizet**, legalább lehetne benne annyi jó érzés, hogy olyan alapvető, Rejtői szabályokat betartson, mint hogy "Márta napján ne lopj!", vagy hogy "Kerüld a részeg embert, hogy téged se molesztáljanak hasonló állapotban!" és hasonlók. Hogy az olyan empatikus vezérlőelvekről ne is beszéljünk, mint hogy **gyerekektől, bajbajutott emberektől, óvódából, vagy kórházból rabolni, oda betörni nem ildomos** - ezt az ideillő jó kis kifejezést egyenesen Fülig Jimmytől kölcsönöztük.

Egész pontosan **a szecsuáni földrengéskárosultak számára gyűjtöttek adományokat** egy weboldalon, ám a 23 esztendős Yang Litao **saját magának próbálta meg átirányítani** ezeket a pénzeket. A kínai károsultak javára gyűjtő Vöröskereszt oldalát feltörve, megszerezte az adminisztrátori jelszót, megváltoztatta azt, és a sajátjára állította át a számlaszámot, de **emellett kártevőkkel is megfertőzte** az oldalt. Emiatt később 72 órára le is kellett azt állítani, hogy mentesíteni tudják - ezidő alatt nem is tudtak további felajánlásokat fogadni.

Még **idejében sikerült lefülelni a csalást, még mielőtt nagyobb összegekhez** jutott volna hozzá, és most két év börtönnel honorálták az akcióját.

Semmilyen empátiát nem vagyunk képesek érezni ezzel kapcsolatosan. Egy "vegyük el a gazdagok pénzét a bankokból" akcióban talán még bele lehet vizualizálni esetleg valamiféle Robin Hoodos vadromantikát, de a **bajbajutott emberek számára gyűjtött pénz megcsapolása mélyen szánalmas** cselekedet.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/568826

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.06. 19:46:07

Egy érdekes kezdeményezés: meg lehet nézni a seriff weboldalán, ki ül éppen a börtönben, névvel, cselekménnyel, fotóval.
www.lacrossecounty.org/sheriff/InmateView/Start.aspx

Ugyebár Angliában - nagyon helyesen nem tökölnek holmi személyi jogi maszlaggal, szépen kiteszik az iskolák faliújságára névvel, címmel, fényképpel a pedofilok adatait, hogy kikre kell vigyázni.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.11.27. 17:35:04

Elképesztő videó arról, hogyan vesztik el a házaikat a bedőlt amerikai lakáshitelesek.

Nekem az a legdurvább resz, mikor órák alatt kipakolnak mindent a szemétbe, mielőtt a bank eladná, és közben meg zöldre festik a füvet.
informacio.blogter.hu/299143/legvarak_hitelbol

Malacka hívja Cicamicát, vétel

2008.07.16. 17:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam reklám oldal kéretlen fizetős letöltési

Csak **nem akar vége szakadni** az indexes e-mail címekről induló fizetős letöltési oldalak spam kampányának.

Csak jönnek és **jönnek a "jópofizós" levelek**, a puszik majdnem kifolynak a mailboxokból. Az illetékeseknek úgy tűnik nem érdekük, vagy **nem sikerül lekezelni a problémát**, az oldalak élnek és virulnak, a kéretlen levelek meg halomban érkeznek.

Kész stratégiával rendelkezhetünk már például **az aluljárón keresztül való átkelésre**, ahol aláírásgyűjtés ürügyén, kamu adomány gyűjtés, utazási szokásaink feltérképezése, kéretlen távcső vagy filmfelvevő árusítás, és egyéb okokkal próbálnak meg minket feltartóztatni, de sebaj, az alábbi polóval egyszerűen hárítható a nem kívánt megkeresés.

Ilyen tuti **módszer sajnos a spamfronton nem létezik**, pedig a Csillagszóró hadművelet, Kánikula Kommandó után **itt is lenne egy kis feladat**, amit el lehetne végezni. De miért is?

Még azt az érvelést is szimpatikusabbnak tartjuk, amely az FSF mintájára minden létező szoftvert ingyen akar, bár nyilván ez egy megvalósíthatatlan utópia, de hát higgyen mindenki abban, amiben csak akar. Ha operációs rendszert és hozzávaló programokat szeretne valaki ingyen, ott a sok Linux a distrowatchon. **A média tartalmak biztos, hogy sosem lesznek - legálisan legalábbis - teljes mértékben ingyenesek, mert ez egy üzlet**, a készítők befektetnek, és megtérülést várnak. Az is nyilvánvaló, hogy nem mindenkinek (például diákok) van annyi zsetonja, hogy minden őt érdeklő filmet megvegyen, ha mégis akarja ezeket, hát rázuhan a PirateBayre és ingyen letölti, saját privát használatra ezt jogszerűen meg is teheti. De az, hogy a fizetős warez letöltéseken egyesek még meg is gazdagodjanak, az hosszú távon biztos, hogy **egyik szereplő (felhasználók, gyártók) érdekét sem szolgálja.** Az őket népszerűsítő kéretlen reklám levelekből pedig továbbra sem kérünk.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Nyári tanácsok utazáshoz

□ bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/571263

Kommentek:

Nincsenek hozzászólások.

A trójai mindig kétszer csenget

2008.07.17. 16:16 | Csizmazia István [Rambo] | 1 komment

Címkék: email hamis trójai ups

Az olimpiát **nem csak azért várjuk**, hogy párduc testű atlétáink megmérkőzzenek egymással, hanem drukkolunk amiatt is, hogy a minden létező eseményt, balesetet, ünnepet kihasználó kártevő terjesztőknek lehetőleg ne sikerüljön túl sok embert **a sportesemény kapcsán hamis üzenetekkel, letöltésekkel** becsapniuk. A remény persze meddő, az új trükkök sorra jelennek meg, most egy csomagküldő szolgálattól kaphatunk "értesítést", amelyet megnyitva kellemetlen meglepetésben részesülhetünk. Ügyes - mondhatnánk.

A UPS csomagküldö szolgálat nevében érkező üzenet azt állítja, hogy az általa küldött csomag kézbesíthetetlen volt és **arra kéri a címzettet, hogy nyissa meg a mellékelt számlát, ami valójában egy végrehajtható állomány**, csak éppen Microsoft Word dokumentumnak álcázták. Ez egy olyan trójai program, amely felváltja az eredeti userinit.exe fájlt a Windowsban. Egyes szakértők szerint orosz weboldalakhoz próbál meg csatlakozni, és onnan **további kártékony (rootkit és adware) állományokat** kísérel meg a fertőzött számítógépre letölteni.

A csomagküldö már értesítést tett közzé a weboldalán, hogy **a levelek nem tőle származnak**.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/572099

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.09.02. 09:24:44

Hogy a FedEx sem maradjon ki a szórásból:
www.allheadlinenews.com/articles/7012135991

Emelem és tartom

2008.07.17. 14:06 | Csizmazia István [Rambo] | 6 komment

A póker játék manapság egyre népszerűbb, a tvben is nyomon követhetjük a nagyobb versenyeket, de a Casino Royale James Bond film is **bepillantást engedett** a zöld posztóasztalok világába. A **számok vetélkedése azonban nem csak itt** zajlik.

Jack Bauer az órájára pillant, 2008. június 12., 08:48. A hír "4 millió vírust ismer a Panda" címmel jelent meg.

Tik-Tak-Tik-Tak

Jack Bauer kinyitja egyik kedvenc számítástechnikai hírportálját, és ezt látja:

2008. július 17. "A PandaLabs jelentése szerint a Panda víruslistáján már több mint 13 millió különféle számítógépes kártevő szerepel."

Ezzel **a Guiness Rekordok évkönyvébe is be lehetne kerülni a Harmincöt nap alatti leghatalmasabb vírusismereti adatbázis növekmény kategóriában**, a Kánai mennyegző halszaporítását megszégyenítő mértékben bírnak bővülni a számok. A bő egy hónappal ezelőtti 4 millióhoz képest - ami pedig szintén nem kis szám például az F-Secure 900 ezres értékéhez képest sem - a Moore törvényt meghazudtolva nemhogy duplázódik, hanem szinte osztódással szaporodnak. Kicsit **a régi DOS-os idők számháborúját idézi**, mikor a Turbo Antivírus és társai vetélkedtek, ki bir nagyobb számot mondani.

Nyilván való, hogy nem ez az egyetlen és legfontosabb mérőszáma egy vírusirtónak, a heurisztikus képesség, a proaktivitás például legalább ennyire fontos. Megpróbálok majd különböző gyártók számszerű adatainak utánanézni, addig is **egy viccel zárnék**, ami remélhetőleg minden újszülöttnek új lesz.

A házibulin éppen arról folyik a szó, kinek mekkor a szexuális teljesítő képessége, és a srácok szájából fantasztikus számok röpködnek. Az egyik fiú ijedten hallgatja, majd félrehívja a barátját, és sápadtan azt mondja neki: te én azt hiszem beteg vagyok, itt olyan számok hangzanak el, amiknek én még csak a közelében sem jártam.
Mire a barátja legyint: ne foglalkozz vele, mondd te is! :-)

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/572530

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.17. 15:50:52

Itt találtam egy linket a hír egy lehetséges forrására:
translate.google.com/translate?u=http%3A%2F%2Fblog.pandasecurity.fr%2F&hl=en&ie=UTF8&sl=fr&tl=en

.Andrei (törölt) · http://www.andreiground.com/ 2008.07.25. 00:06:51

/* Azt hiszem bookmarkoltam a blogot :) */

A Panda egy jó dolog :) Aki feltelepíti, az utat nyit a pokolból a felszínre.

Előre leszögezem, hogy nem vagyok Nod-ista, max nudista :)

Mindenki másra esküszik, de mostanában nem tudok olyan ismerőst (amatőr vagy profi), aki ne az Nod, Avast vagy Avclamot használta volna. Pandát senki. Egyszer 4-5 éve futott egy gépemen Panda, mert kíváncsi voltam rá. Ugyanezen időszakban a másik gépen Nod volt. Hagytam történni a dolgokat. A két gépen ugyanazt csináltam nagyjából mindig. Eltelt egy hét, és a Panda már nem érzett, sőt a gép sem. Kb a 30-ik oldalon beszedett valamit, ami aztán elburjánzott és a portscanner félelmetes adatforgalmat mutatott. Majd már be sem bootolt, hanem fekete kép villogó kurzorral :). A Nod meg ketyegett még akkor is, amikor két hete ki volt lőve a firssítési szolgáltatás. Frissítés nélkül másfél hónapog futott a gép, majd néhány alfunkció kikapcsolása után sikerült kinyúvasztanom.

Hasonló tesztet nyomtam Avast, kontra AVG :) Gondolhatod, hogy az AVG mennyire tuti volt :DDDDDDD

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.25. 06:21:49

Szia Andrei!
Itt volt olyan retrospectiv teszt, ami kifejezetten azt nézte, frissítés nélkül mi a pálya:
www.eset.hu/files/dokumentumok/osszehasonlitasok/AV-Comparatives_2006_julius.pdf
másik:
www.eset.hu/files/dokumentumok/osszehasonlitasok/CheckVir_2006_februar.pdf

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.29. 11:02:46

F-Secure hír: itt az egymilliómodik kártevő:
www.sda-asia.com/sda/news/psecom,id,19942,srn,4,nodeid,4,_language,Singapore.html

Algernon 2008.09.24. 10:37:03

Ez a 10 milliós szám sem kicsi...Ráadásul "10 millió kémprogram" szerepel a cikkben, de a kémprogramokon kívül még biztos jó sok reklámprogramot és egyéb kártevőt is tartalmaznia kell az adatbázisnak...
www.biztonsagportal.hu/megujult-fegyver-karokozok-ellen.html

Kíváncsi vagyok, ha virtuális gépen meglátogatnék néhány oldalt a program védelme mellett a stopbadware.org "kínálatából", meddig bírná...Lehet, kipróbálom, s elmesélem.:)

titan 2010.05.04. 16:40:19

10 millió kémprogram, ez azt jelenti, hogy 4 kémprogram egyenként 2,5 millió variánssal tán? :)

Privát MMS képek közprédaként

2008.07.21. 18:37 | Csizmazia István [Rambo] | 9 komment

Címkék: google keresés link mms képek o2 adatszivárgás

A MailChannels blog hívta fel a figyelmet arra, hogy a **magán multimédia üzenetek képeit illetéktelenek is elérhették a weben** keresztül.

A problémát az okozza, hogy egyes készülékek - például az oly népszerű Apple iPhone is - nem képes MMS-ben érekezett képet közvetlenül fogadni. Ehelyett a képre mutató linket mellékelnek az üzenetbez, amelyre rákattintva a böngésző segítségével tudjuk az megtekinteni.

David Cawley postjában megmutatta, hogy lehet egy egyszerű Google kereséssel ilyen jellegő fotókra rátalálni, és **vadidegen emberek - akár bizalmas - MMS képmellékleteit nézegetni**. Mivel az illető **oldal semmilyen autentikációval nem rendelkezett, a Google kereső szépen felindexelte** az ott található fotókat és képeket.

Az eset nyilvánosságra kerülése miatt jelenleg a brit O2 szolgáltató felfüggesztette a webalapú MMS szolgáltatását és a képmellékletek webes megtekintési helyét a probléma teljes kivizsgálásáig.

Ezért a jelzett Google **keresési módszer most nem ad vissza képtalálatokat**. A keresési feltételeket tovább finomítgatva **belefutottunk egy érdekes hibaüzenetbe**:

További érdekesség, hogy az O2 szolgáltató az erről szóló topikot is törölte.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/578544

Kommentek:

Erőforrás 2008.07.21. 21:31:04

Szia Rambo!

Lenne egy kérdésem:
A Worm Win32 GetCode a., vírust a Nod32 milyen néven ismeri fel?

holex · http://fred-basset.blogspot.com 2008.07.22. 08:04:18

OFF

ne használj vírust, akkor nem lesz ilyen gondod. :D virusírtót se használj, mert a vírusok azon keresztül jönnek be a gépedre. :)

ON

a webesalapú MMS, egyébként is egy nagy baromság, csak bosszantó, hogy külön egy linket kell nézegetni, böngészőbe betölteni... ehhh...

iPhone-ra meg ott a SwirlyMMS, ha valaki anyira mms-ben gondolkodik, és nem akar a webes szarral kínlódni.

Terveüdekszi 2008.07.22. 09:55:58

Mi az az MMS?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.22. 10:11:51

Szia Erőforrás!
Sorry, nem tudom. Ha van minta, a VirusTotalon meg lehetne nézni. Mi ismeri fel ezen a néven? Küldenél egy PONTOS, formailag spacek, stb. tekintetében is szabatos féreg nevet?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.22. 10:14:28

Hello Holex!
Ez a vírusok a vírusirtón keresztül jönnek be ez jó, megnevetettél, és vettem a smileyt a végén :-)

A Swirlyt köszi, meg fogom nézni, annál is inkább, mert a családban már van, aki tűkön ülve várja az új iPhonet.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.22. 10:17:32

Helló Terveüdekszi!

Azon tűnődöm, vajon komoly-e a kérdés? :-D
Tudtommal a Macedón Medvék Sportklubja rövidítése ;-)

Egyébiránt a Multimedia Messaging Service, vagyis multimédiás üzenetküldési szolgáltatásnak a kezdőbetűi.

Terveüdekszi 2008.07.22. 10:29:58

Helló Rambo!

A kérdés inkább cinikus volt. Életemben még egyetlen egyet sem küldtem. Viszont kaptam vagy 5-öt, de azokat meg kitöröltem, mert a telefonomat lusta voltam beállítani hogy tudja fogadni. :-)

Erőforrás 2008.07.22. 10:32:51

Rambo!

Az a pőontos neve amit leírtam neked a kommentemben!
A Kaspersky oldalán is ez az elnevezése.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.07.29. 11:06:52

@Erőforrás:
Szia! Valami még sem stimmel a névvel, mert sem a viruslist.comon
www.viruslist.com/en/find?search_mode=virus&words=Worm+Win32+GetCode&x=0&y=0
sem pedig a kaspersky.comon nincs találat :-O
www.kaspersky.com/find?words=Worm+Win32+GetCode&x=0&y=0&search=1

Deface az antivírus oldalon

2008.07.22. 18:11 | Csizmazia István [Rambo] | 18 komment

Címkék: sql kaspersky deface

Kellemetlen **meglepetésben volt része a Kaspersky weboldalának**. SQL injections segítségével **defacelték (van erre jobb magyar szó?) a malájziai oldalt**, valamint a Kaspersky online áruház címoldalán is egy török hacker üzenete virított egy ideig.

Ez természetesen **semmilyen közvetlen kapcsolatban nincs az antivírus programok minőségével**, bár kétségkívül **nem jó reklám**, szerencsétlen üzenetet sugall, ha egy biztonsági cég a saját weboldalát sem tudja megvédeni, akkor hogyan menti meg így majd a világot? A maláj oldal egyébként egy Microsoft IIS szerveren futott, amit átmenetileg le is kapcsoltak.

Sok múlik a weboldal kódjának biztonságán, az oldalt üzemeltetők éberségén, bár sokak szerint **ezen a fronton nincs lehetetlen**, bármit fel lehet törni, csak elegendő idő, erőfeszítés vagy egy ráérő finn ;-) kell hozzá.

A Kaspersky oldalak elcsúfításának **már szinte hagyománya van**, vonzó célpontnak számít, és nem ez volt az első eset. Egész brigádnapló oldal őrzi a különböző - hol román, hol francia - testvéroldalak megpiszkálását.

· 1 trackback

Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/580317

Trackbackek, pingbackek:

Trackback: Propeller **2008.07.23. 07:49:45**

Deface az antivírus oldalonKellemetlen meglepetésben volt része a Kaspersky weboldalának. SQL injections segítségével defacelték (van erre jobb magyar [...]

Kommentek:

Yann Le Pentrec · http://lnk.bz/t7c 2008.07.22. 18:50:53

MS IIS. Extrémsportnak jó...

ChPh · http://edol.hu 2008.07.22. 18:53:07

Pedig a netcraft szerint pont egy ilyen IIS-nek van a legnagyobb uptime-ja

kocka.blog.hu/2008/07/21/legregebbi_mukodo_szerver

Kheller 2008.07.22. 18:56:55

"szerint pont egy ilyen IIS-nek van a legnagyobb uptime-ja"

...és a legkevesebb ismert sebezhetősége. Messze biztonságosabb az apache-nál. SQL injectionnek meg halvány köze sincs a futtató web szerverhez, az az adott oldal programozójának a sara.

gusthy1 · http://kolyokjoga.blogspot.com 2008.07.22. 19:52:57

Kheller, mint tudjuk, az ismert sebezhetőségek száma nem sok összefüggést mutat a biztonságosság szintjével: a sebezhetőségek biztonsági kockázatát is figyelembe kell venni. Igen, egy időben az MS ezzel fényezte magát, hogy hánnyal kevesebb sérülékenysége van. De egy súlyos vulnerability lehet, hogy összeomlasztja az oldalt vagy mondjuk a fél netet, egy kevésbé súlyos meg csak arra jó, hogy valaki fölrakjon egy kép helyett egy másikat.

Kheller 2008.07.22. 20:05:26

gusthy1: a vicces az, hogy az iis kapcsán gyakran majd egy évig semmilyen (értsd el ezalatt: SEMMILYEN) sebezhetősége sem ismert, nézz meg 1-2 statisztikát. Se kicsi, se nagy. Miközben az apache-ot 2 havonta foltozhatod, gyakran nagyon durva hibákkal. A furcsa az, hogy ez tényleg csak az iis-re vonatkozik, a többi komponensben egyáltalán nincs ilyen előnye a ms termékeknek. Talán még az sql server az ami a konkurenciához képest (mind open mind closed source) nagyságrendekkel biztonságosabb, alig kell patchelni.

Kheller 2008.07.22. 20:07:09

nem véletlen, hogy 1-2 éve zuhan az apache részesedése és nő az iis-é. volt idő, hogy majd 2x annyi telepitett apache volt a világon mint iis, ma már alig 10-15% nagyobb csak az apache részesedése.

Naaaaa 2008.07.22. 20:32:40

Nem mellőzném azt a tényt sem, hogy az ismert hibák száma nem egyenlő az összes hibák számával. Le merem fogadni, hogy az IIS-ben több hiba van mint az apacheban, csak mivel nem nyílt a forráskódja, kevesebb publikus hiba van hozzá. Csak a script kiddiek dolga nehezebb.

Kheller 2008.07.22. 20:47:51

"csak mivel nem nyílt a forráskódja, kevesebb publikus hiba van hozzá."

jaj ezt el ne kezdjük...

ezerszer ki lett már fejtve, az iis forrását több ezer független szakértő ellenörzi (shared source program és egyedi felkérések alapján), attól még hogy boldog-boldogtalan nem töltheti le, igy a hackerek se. Nemcsak a script kiddiek dolga nehezebb, hanem mindenkié.

"csak mivel nem nyílt a forráskódja, kevesebb publikus hiba van hozzá."

valószinűleg csúnyán elveszitenéd a fogadást, de mindegy, hinni mindenki azt hisz amit akar, a TÉNYEKEN semmit nem változtat.

iTortent · http://mitortent.hu 2008.07.22. 21:34:11

Sajna az MS-t szidni divat, de egyszer majd csak felnőnek ezek az emberek is...

Sem Mihály 2008.07.22. 21:39:43

Csak mielőtt itt összeszarják magukat egy páran az IIS-től, a cikk arról szól, hogy egy IIS alatt futó oldalt defaceltek. Nem Apache alatt, hanem IIS alatt. Lehet itt statisztikát lobogtatni, elméleteket gyártani a zárt forrás biztonságos voltáról, attól még nem feltétlenül az a baj, ha valamit rendszeresen foltoznak, hanem ha esetleg egy nem detektált, nem publikált hiba miatt később egyszerre borítják be a fél internetet. Az meg, hogy milyen oprendszeren fut a legrégebben futó szerver teljesen érdektelen info, ha nincs miért megborítani, akkor nem is fogja senki.

0xFFFF 2008.07.22. 21:45:50

"ChPh · chph.blog.hu 2008.07.22. 18:53:07
Pedig a netcraft szerint pont egy ilyen IIS-nek van a legnagyobb uptime-ja

kocka.blog.hu/2008/07/21/legregebbi_mukodo_szerver "

Valami azért sántít azzal az uptime-mal....az első két post a hír után:

"Kommentek, trackbackek, visszapingek:
melák 2008.07.21. 18:55:37 fp002.crayfish.net/
No web site is configured at this address.
*muhaha
megbízható 2008.07.21. 19:09:44 "No web site is configured at this address.""

Majd ezután a két post után már ment. Uptime...aha. :)

Kheller 2008.07.22. 22:20:04

Morcog: "a cikk arról szól, hogy egy IIS alatt futó oldalt defaceltek. Nem Apache alatt, hanem IIS alatt"

tovább is kéne olvasni. SQL injection. Innentől futtató webszerverről meg alatta lévő oprendszerről beszélni (mutogatni rá) nem vall túl sok szakértelemre. Már, ha az illető akár csak halványan tudja hogy működik az sql injection.

Árpi 2008.07.22. 23:29:27

Tartok tőle, hogy az IIS térnyerése nem kis mértékben annak is köszönhető, hogy szaporodnak azok a cégvezetők a szervertulajok között, akik nem oprendszeren, hanem windowson nevelkedtek. Akik úgy hoznak döntést, hogy azt hiszik, GUI nélkül a szerver csak múltszázadi lehet, mert parancssort csak DOS alatt láttak még. A rendszergazda meg oldja meg.
Persze rossz weboldalt minden alá lehet írni, ennek semmi köze a webszerverhez.

Celtic 2008.07.23. 08:08:26

Hmm, az IIS nepszerusege azert is nohet, mert .NET ASP oldalak nem mennek apache alatt? Legalabbis Linux/BSD apache alatt...

aqswdefr 2008.07.23. 08:15:50

Ha jol emlekszem, az IIS ternyeresen eleg sokat dobott pl. a godaddy atallasa apache-rol.

Kheller 2008.07.23. 09:07:12

"mert .□ET ASP oldalak nem mennek apache alatt?"

szerintem mennek mono-val, persze csak úgy mint a többi .net komponens esetén az is évekkel le van maradva linuxon.
De az biztos, hogy a .net iszonyatosan terjed, mind web mind általános vállalati fejlesztések terén, ami mondjuk valóban az iis felé döntheti a mérleget, mert sokkal több szolgáltatást, konfigurálási lehetőséget ad alá (pl egy 7-es iis) mint az apache.

"Ha jol emlekszem, az IIS ternyeresen eleg sokat dobott pl. a godaddy atallasa apache-rol"

az csak egy jól behatárolható időbeli pont (2 éve volt talán) ahol tényleg nagyot zuhant az apache részesedése (gyakorlatilag néhány nap alatt), de ha tendenciát nézel ott is jól látszik hogy folyamatosan csökken az apache, az iis pedig nő.

aqswdefr 2008.07.23. 09:54:46

news.netcraft.com/archives/web_server_survey.html
Gondolom ezt nezegetjuk mindketten, hadd lassak a tobbiek is :)

Az IIS-ben eleg furcsa, hogy lepcsozetesen ugral (a godaddy 2006 elejen volt, ott latszik is szepen egy jo nagy lepcsofok), es a lepcsok kozott stagnal. Az apache ehhez kepest sokkal ingadozobb.

Ugyanakkor ez szazalekos abra, es kozben no a szerverek szama is, igy lehet, hogy pl. marcius-aprilis kozott az apache-okbol 1.1 millioval, IIS-ekbol 848 ezerrel lett tobb, csak ez az apache-nak -0.27%-os, az IIS-nek viszont -0.14%-os valtozas.

De persze hajra IIS, meg hajra lighttpd, nginx, stb., eljen a valtozatossag :)

Kheller 2008.07.23. 10:48:19

az apache pont annyira lépcsőzetesen zuhan amennyire lépcsőzetesen emelkedik az iis...
és néha pont ugyanolyan lépcsőzetesen ugrik felfele is az apache. ezügyben nincs különbség.

A % meg már csak igy működik, pont ez benne a jó, hogy kimutatja a valós piacvesztést/növekedést akkor is, ha a számszerűen lehetne döngetni a mellett, hogy ma több szerver van xy-ból mint tegnap, miközben a valóság az, hogy csökken a részesedése.

Social engineering egyenes adásban

2008.07.23. 11:18 | Csizmazia István [Rambo] | 3 komment

Címkék: demo social rambo mitnick engineering

Akik **olvasták Kevin Mitnick könyveit, vagy látták a róla készült filmet**, biztosan megértették a dolog lényegét: megtévesztéssel, hamis szép szavakkal önként és dalolva **adnak át jelszó és egyéb bizalmas céginformációkat** akár egy pár perces telefonbeszélgetés alkalmával.

Mitnick és barátai a múlt szombati Live HOPE konferencián előadásokat és bemutatót tartottak, **hogyan kell alkalmazni az ilyen módszereket**. A publikum előtt még telefonhívásra is sor került, ahol egyikük **a nem létező Utolsó Reménység Segély Alapítvány** (Last Hope Foundation) nevében folytatott telefonbeszélgetést egy Stairbucks alkalmazottal. Arcvonásait - különösen a hívás vége felé - nehéz volt tartania, néha még fel is nyerített a nevetéstől.

Muszáj tudomásul venni, hogy **hiába a technika, a biztonsági programok garmadája, ha a megfelelő emberi hozzáállásban rések mutatkoznak**. Van egy mondás, miszerint "Az egészség nem minden, de a minden is semmi egészség nélkül", hát nagyjából hasonló a szituáció.

A Rambo First Blood Part II. epizódjában, mikor a helikopteres-táborfényképezős küldetésre készítik fel, és amikor azt mondja neki Trautmann ezredes: **ezúttal hagyatkozz a technikára, meg a mostani jó és még jobb fegyvererekről is szó esik**, elhangzik egy jó kis kulcsmondat John szájából: **"én azt hittem, az ész a legjobb fegyver"**.

Úgy tűnik, ez napjainkban sem vesztette el az aktualitását. A mai világban, amikor a kártevők sokkal **inkább a banki adatainkat, jelszavainkat lopják, fürkészik, továbbítják, semmint látványosan fertőznének**, hiába állítunk be vírus- és kémprogragirtót az ajtóba, ha **közben meg az ablakon dobjuk ki, nyújtjuk át** - vagy csak hagyjuk, hogy nyúlkáljanak érte - a bizalmas információkat.

Nem lehet nem észrevenni, hogy dr. Househoz és Jack Bauerhez hasonlóan Mitnick előtt is egy MacBook látható a pulpituson. Visszaevezve a **hazai vizekre**, már érik a napirend a szeptember 20-21-i Hacktivity találkozóra, senki ne hagyja ki!

· 1 trackback

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/581258

Trackbackek, pingbackek:

Trackback: Propeller 2008.07.24. 08:56:25

Social engineering egyenes adásbanMitnick és barátai a múlt szombati Live HOPE konferencián előadásokat és bemutatót tartottak, hogyan kell alkalmazni az ilyen [...]

Kommentek:

.Andrei (törölt) · http://www.andreiground.com/
2008.07.24. 23:53:07

Az SE misztikus, az SE félelmetes, és a legtöbben ezt gondolják. Pedig hiba. Én azt gondolom, hogy bizonyos szintig mindenki Social Engineer a saját érdekében.

Észre kellene venni, hogy Mitnick egy monitor, semmit több. Az a cél, hogy mindenki megbízzon benne, legyen "elismert", majd aztán jól informálja a megfelelő ügynökségeket. A könyvek alapvetően tompítottak. Ha mélyen átrágod magad a két könyvön, akkor le fog esni a dolog. Ráadásul a felhozott mintáknak köze sincs Európához vagy Ázsiához és elferdíti az SE fogalmát.

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.07.25. 06:26:13

Egy korábbi munkahelyemen köremailt küldtem, hogy az AV frissítésig senki ne nézze meg, ha egy Pretty Parkos levelet kap. Félórán belül megjött az új adatbázis, a 400 gépes hálózatban béke honol, de egy helyen mégis fertőzött, Felballagok megnézni, aholis a titkárnéni ezt mondja: "igen, olvastam én a körlevelet, hogy NE, de én azért mégis kíváncsi voltam rá :-)

.Andrei (törölt) · http://www.andreiground.com/
2008.07.25. 10:10:28

Persze, az emberek kíváncsiak és ezt ki lehet használni vagy lehet vele számolni védelmi oldalon. A körlevél amúgy jó dolog, mert "mindenki utál ilyet kapni", de azért "mindenki kíváncsi rá". Az állapotkapcsolók könnyen billenhetnek, csak egy kis izgalmat kell belecsempészni.

A last hope-os dolog kapcsán meg annyit, hogy Amaróka amúgy is a "bizalom szigete", tehát SE szempontból maga a paradicsom. Európában sokkal "dörzsöltebbek" az emberek és más technika kell egy-egy információ kisajtolásához.

Kártevők a blogokban

2008.07.24. 10:52 | Csizmazia István [Rambo] | 1 komment

Címkék: google blog blogger malware kártevő

Azt már mindenki tudja, hogy **az ártó kódok a hétköznapi, legális oldalakat** is veszélyeztetik (pl. SQL injection), sőt ezek mennyisége hihetetlen mértékben növekszik. **Most a blogokkal kapcsolatban** láttak napvilágot érdekes adatok.

Egy korábbi vizsgálat szerint körülbelül napi 16 ezer kártékony weblap keletkezik, vagyis minden ötödik másodpercben jelenik meg egy. **A növekedési ütem az előző, 2007-es évhez képest 300 százalékos**. Most egy friss jelentés szerint **a Google Blogger szolgáltatása felel a kártevők mintegy 2%-áért**. A felmérés szerint népszerű az új, **kártevők kódjára mutató blog bejegyzések** készítése úgyanúgy, mint a már meglévő postokhoz illesztett, **fertőzött tartalomra mutató linkeket tartalmazó kommentek hozzáfűzése**.

A Sophos szakértője **szerint ebben a Blogger webnaplói kiemelten veszélyesebbek** a többi hasonló blogszolgáltatásokhoz képest, **mert a Google kereső azonnal fel is indexeli** azokat.

Nyilvánvalóan itt is **kell(enne) működnie** egy egészséges gyanakvásnak, szelekciónak, hogy mire kattint rá az ember, miben bízik meg, és miben nem. De mint tudjuk, **ember tervez, egér kattint**.

· 1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/582908

Trackbackek, pingbackek:

Trackback: Propeller 2008.07.25. 06:13:33

Kártevők a blogokbanA blogbejegyzésekben és kommentekben egyre növekszik a kártékony kódokra mutató linkek száma

Kommentek:

.Andrei (törölt) http://www.andreiground.com/
2008.07.24. 23:45:24

Persze sok mindenről tehet a blogger-ggl kombó, de ezt a wp alapú trunyát is elvinné a tájfun, ha valaki odafigyelne. És egy kis fertőzdés után aztán lehetne etetni a google-val.

Hamisított Flash frissülés

2008.07.25. 06:00 | Csizmazia István [Rambo] | 2 komment

Címkék: spam flash kártevő kodek lettöltés

Akik **a bulvár műfajt szeretik, azok biztosan fogékonyak** az olyan hírekre, mint például **"Angeline Jolie terhessége hazugság"** - hiszen lám milyen jól néz ki rövid idővel utána, de a tengerentúliakat érdekelheti a **"Hillary Clinton beperli Barack Obamat"** kezdetű értesülés is. Ami akár lehetne igaz is, bár mi eléggé el nem ítélhető módon a CNN-nek ez utóbbit valahogy jobban elhinnénk.

Na persze ha mindez **nem a Bunte vagy a Blikk címlapján szerepel. hanem kéretlen levélben érkezik** a postafiókunkba, tapasztalataink szerint máris **kevés az esélyünk a jóltájékozottságra**, annál több a sansz arra, hogy valamilyen letöltő trójaival próbálkozó weboldalba botlunk.

A kártevős oldalak **gyors változtatásának "hála" az első két hírnél** a install_flash_player_update.exe nevű fájl elérhetősége **már nem is működik**.

Csak a harmadik weboldalon jártunk "sikerrel", onnan **le is töltöttük a flashcodecinstall_13_31.exe** trójai állományt. Érdemes megfigyelni a kamu Flash update ablakot.

Persze a VirusTotal eredményt akár előre borítékolhattuk is volna. A tanulság talán annyi lehet, hogy bár **kifordítom, befordítom, mégis kodek a kodek :-)**

· 1 trackback

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/583115

Trackbackek, pingbackek:

Trackback: Propeller 2008.07.25. 06:35:10

Antivírus blog - Hamisított Flash frissülésA régi kodekletöltős kártevő trükk ezúttal Flash Player köntösben

Kommentek:

.Andrei (törölt) · http://www.andreiground.com/ 2008.07.25. 10:05:36

Ugyanez a trükk csak pepitában, amikor egy video oldal úgy nyit, hogy .exe letöltés vagy plugin telepítés browser alá. :) Szemét trükk, mert sokan bedőlnek neki az áhított video miatt.

Algernon 2008.07.25. 11:39:15

Az utóbbi pár napokban ezek a trójais flash codeces, video.exe-s oldalakra mutató linkek nagyon ellepték a postaládámat. Pár hónapja még minőségi, "optimalizált" víruskákat küldözgettek, amelyeket sokszor még a heurisztika sem ismert fel (pl. a fool's day-es storm codecek), de mostanában inkább a mennyiségben hisznek. Tömegtermelsé, standardizáltság, volumen...Hova tart ez a világ? :))

Olvassunk cikket .EXE formátumban!

2008.07.29. 12:12 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam facebook hülye fbi spammer

Akit a mozdony füstje megcsapott - ez volt a címe az egyik Moldova riportkönyvnek, amelyben **szerepelt egy idézet az egyik dolgozótól**: sajnos sokan lenéznek minket, úgy tartják: "hülye, hülyébb, leghülyébb, rendőr, postás, vasutas". Nos mi úgy véljük, a **"hülye, hülyébb, leghülyébb, spammer" lenne inkább a helyes sorrend**. Meg is mutatjuk, miért.

A legfrissebb - és természetesen kéretlen - levél szerint **az FBI azonnali hozzáférést óhajt a Facebook közösségi oldal adataihoz** - ez aztán az újdonság, mintha ez már rég nem lenne meg neki :-) És persze az üzenet felkínál egy linket is. A levél további érdekessége, hogy a NetSecurity portál sajtólistájára (is?) küldték.

Ez a weboldal hivatott lerántani a leplet a dologról - és most érdemes megkapaszkodni - nem holmi hihető csali Storm kodekként, vagy esetleg olvasható és emészthető formátumú (preparált) DOC formájában, esetleg trükkös dupla kiterjesztésű .JPG.VBS vagy .JPG.EXE állománnyal, hanem csak úgy simán, face-to-face szamurájosan **egy fbi_facebook.exe** Mark Zbikowski féle futtatható EXE fájl képében **adják a "cikket"**.

Ami **persze nem olvasnivalóféle**, a VirusTotalos eredményt pedig becsatoljuk alant, ebből majd kiderül hogy ciki vagy cuki.

Talán elgurulhatott emberünk gyógyszere, ki tudhatja? **Hány épeszű felhasználó gondolna egy futtatható fájlt cikknek vagy hírnek?** Mindenesetre a terjesztőnek ezúton gratulálunk ehhez a ~~zselatinos~~ zseniális ötletéhez ;-)

· 1 trackback

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/589999

Trackbackek, pingbackek:

Trackback: Propeller 2008.07.29. 09:35:24

Antivírus blog - Olvassunk cikket .EXE formátumban!Egy új spam üzenet az FBI kontra Facebook kapcsán még a látszatra sem ad: futtatható állományt kínál olvasnivaló cikként

Kommentek:

Nincsenek hozzászólások.

Ön elkészíti, mi kiegészítjük

2008.07.29. 12:51 | Csizmazia István [Rambo] | 2 komment

Címkék: spam weboldal web storm kártevő kéretlen page landing

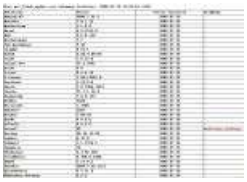
Nem pontosan az Önök kérték, mi teljesítjük mintájára ugyan, de felfutóban a **nagylátogatottságú weboldalak extra landing page**-dzsel való kiegészítésének divatja - persze mindezt **a tulajdonos tudta nélkül**, Önök _NEM_ kérték jeligére ;-)

A munkát persze nem irgalmas szamaritánusok végzik, hanem a kártevőterjesztők olajozottan működő hálózata. A levelek témáját szinte biztosan egy hatalmas adatbázisból tombolázzák ki, most éppen a Nők a pult mögött analógiájára **Az első nő, aki a NFL foci ligába verekedte magát** címmel érkezik. A női nem tisztelete ide, női egyenjogúság oda, erre a hírre itt Európában érezhetően kevesebb az érdeklődés.

Eddig mindennapos a történet, látjuk a kamu flashkodek letöltő oldalt, bedobjuk a fájlt a VirusTotalba - a már unalomig ismert rutinmunka - gondolhatnánk. Ahhoz is hozzászokhattunk, hogy egy **Storm kódot letöltő oldal általában mindössze egyetlen HTML fájlból áll**, amiben a kártékony link szerepel, és a letöltést biztosítja. De...

Ha kitöröljük a mostani weboldal domainje mögül a "checkit.html"-t **és a főoldalt nézzük** meg, igazi működő, ékes **portugál nyelven készült brazil üzleti weboldalt látunk**, ez most éppen egy online oktatással foglalkozó cégé. Igen **valószínű, hogy halvány segédfogalmuk sincs, hogy mire használják fel a cégük domainjét**. Ha nagyon kíváncsiak vagyunk rá, a Google Translate segítségével angolul is ránézhetünk.

További izgalmas körülmény, hogy mivel **esetünkben már el is mozdították vagy elköltöztették az EXE-t**, így a valódi elemzést ezúttal lekéstük. A get_flash_update.exe állomány helyett ugyanis csak egy HTML tartalom tölthető le, amiben jelzik, a kért tartalom már nem áll rendelkezésre az IIS szerveren. De nézzük meg, hogy **ez a belül HTML, EXE fájkiterjesztéssel rendelkező sima szövegállomány mit mutat** a VirusTotalon.



Hüphüphüp, Barba trükk: a Prevx - szerencsére egyedül - a sima HTML kódra jelzi, hogy **szerinte ez egy kártékony szoftver!** Az eseten **felvillanyozódva gyorsan összeütünk egy Hello World!-ot kiíró HTML kódot**, és ezt EXE-nek átnevezve megvizsgáljuk, de arra már nem jön a riadó.

Szóval a lényeg, hogy nem csak magánemberek gépei, nem csak a bothálózat fertőzött géptagjai, hanem **minden valamiképp megfertőzhető oldal veszélyben lehet**. Érdemes ezért **rendszeresen ránézni saját vagy céges webhelyünk statisztikájára**, és ha **a nézettséget esetleg egy olyan aloldal vezeti, amit nem is mi készítettünk**, akkor máris kezdhetjük a nagytakarítást.

· 1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/590733

Trackbackek, pingbackek:

Trackback: Propeller 2008.07.29. 13:52:38

Antivírus blog - Ön elkészíti, mi kiegészítjükFelfutóban a nagylátogatottságú weboldalak illegális, extra landing page-dzsel való kiegészítésének divatja

Kommentek:

Erőforrás 2008.07.29. 16:53:35

Szia Rambo!

Live Messengernél, a fájl átvitel opciónál, a No32 melyik modulját kell beállítani? Tudod, amikor kapok egy fájlt és automatikusan át szeretném vizsgáltatni? Az EGUI nem csinál semmit.

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.07.31. 20:24:07

Szia!
Szerintem ez segíthet neked:
www.eset.eu/knowledge-base/how-to-configure-windows-live-messenger-to-scan-incoming-files
Ha mégsem menne így, a support KUKAC sicontact PONT hu címre írjál, és ott biztosan megoldják a problémát.

Angol állampolgárság csak könnyedén

2008.07.31. 22:14 | Csizmazia István [Rambo] | 3 komment

Címkék: angol rablás chip útlevél azonosító bimoterikus

Az elkövetkező években **ha valaki új személyiségre vagy angol állampolgárságra vágyik**, mostantól könnyen elérheti ezt. Mielőtt mindenki megrohamozná a nagykövetséget, előtte **azért érdemes lesz továbbolvasni**.

Alaposan **megszervezett** támadást intéztek hétfőn egy biztonsági furgon ellen, amely Manchesterből Londonba tartott. Az elkövetők eltérítették a járművet és körülbelül **háromezer eredeti, kitöltetlen** brit útlevelet és vízumot zsákmányoltak, amelyet eredetileg külföldi nagykövetségeknek szántak.

Bár a Külügyminisztérium jelentős biztonsági incidensnek minősítette az esetet, de **azt bizonygatta, az üres dokumentumokat nem fogják tudni használni** a bűnözők a beépített biztonsági chip miatt.

A cáfolattal ellentétben félő, hogy mégiscsak komoly károkat lehet az iratok felhasználásával okozni. Ismeretes, hogy a megbízhatónak tartott RFID chipes útleveleket a **szakértők egy része mégsem tartja annyira biztonságosnak**, például klónozásos másolását már többször is demonstrálták különféle biztonsági konferenciákon.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/595058

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.09. 11:27:47

A Produkáljunk percek alatt rovatunkban:
www.vnunet.com/vnunet/news/2223415/uk-electronic-passports-cloned

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.21. 09:42:47

Ez is vicces, útlevél Bin Ladennek:
www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.06. 13:53:34

Wannabe Elvis Presley? ;-)
hvg.hu/Tudomany/20081006_van_beek_amszterdam_elvis_rfid_hack.aspx

Nem tudja a jobb kéz, mit csinál a bal

2008.07.31. 11:26 | Csizmazia István [Rambo] | 1 komment

Címkék: spam email kártevő nuwar

A kártevő letöltő oldalakra mutató spamek egy idő óta skizofréniában szenvednek.

A készítők megtekerik a generáló program kurbliját, és az **egy adatbázisból máris ontja az érdekesnek szánt leveleket**. Nyári olimpia, a cunami áldozatai, Tibet, Angelina Jolie terhessége, Fernando Alonso balesete - és még hosszan sorolhatnánk, a levélben pedig egy link, ami egy weboldalra mutat, ahol aztán jön az extra kodekletöltésre utaló kamu hibaablak, a kodek EXE pedig a Nuwar féreg egy változata - **így megy ez, ilyen sablonosan**.

A korábbi hosszabb reklámszövegeket, a raszterpontokkal teleszórt képes spameket felváltották az egysoros mondatok egy link kíséretében. Újabban úgy tűnik **valamiféle zavar van a gépezetben** - összecsúsztak a mezők az SQL adatbázisban, esetleg egy elszabadult pointer csörgeti láncát - minden esetre a mostanában érekezett **levelek tárgysora (Subject) és a levéltest szövegében a linkre utaló mondat már köszönő viszonyban sincsenek egymással**. Lehet, hogy **esetleg szándékosan** duplafedelű az e-mail, ha eseteg valaki éppen nem bukik az egyik témára, akkor "van máááááásik" - nem tudni pontosan az okot.

Az ilyen linkek **legtöbbször a Win32/Nuwar féreg** valamelyik változatára mutatnak, ezek közül is létezik olyan változat, amelyik a gép található **biztonsági programok ellen** kísérel meg támadást intézni. A Nuwar.M variáns megpróbálja leállítani azon folyamatokat, mely nevében szerepelnek a következő szótöredékek:anti, avg, avp, blackice, f-pro, firewall, hijack, lockdown, mcafee, msconfig, nav, nod32 rav, reged, Registry Editor, spybot, taskmgr, troja, viru, vsmon, zonea.

A **trójai komponens pedig jelszavakat igyekszik összegűjteni** a megfertőzött számítógépről - szóval ez a Nuwar nem lesz a barátunk, annyi biztos.

Valaki megalkothatna már egy jó kis emblémát a "Ne fürgyé le!" mintájára, **"Ne klikkelj rá!" vagy valami hasonló felirattal** ;-) és majd beajánljuk Tomcat polóboltjába.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben

- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás
- A jelszó érték, vigyázzunk rá

bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/593952

Kommentek:

Scientist · http://deadindian.extra.hu 2008.07.31. 13:51:57

elavult az otthoni virusgyüjteményem

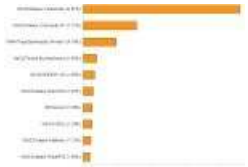
Nyári szabadságon a vírusírók

2008.08.04. 18:28 | Csizmazia István [Rambo] | 9 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az elmúlt **három hónapban gyakorlatilag nem változott** a Magyarországon legtöbb fertőzésért felelős vírusok toplistája, **még mindig a Virtumonde vezet**. Következzen a **NOD32 antivírus rendszert gyártó ESET ThreatSense.NET Center** hazánkra vonatkozó kimutatása.

Számos vírusirtó cég közöl statisztikát arra nézve, hogy mely károkozók végzik a legnagyobb pusztítást az interneten. Az ESET statisztikai rendszere azonban **egyedülálló módon képes az egyes országokra lebontott vírusstatisztika** közlésére is, és nem csupán az e-mailekben terjedő károkozókról ad átfogó képet, hanem a számítógépet http protokollon keresztül, böngészés közben megfertőzőkről is.



Az ESET statisztikai rendszere szerint júliusban az alábbi 10 károkozó terjedt a legnagyobb számban Magyarországon:

1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a júliusi fertőzések között: 22.87%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET kategorizálása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

2. Win32/Adware.Virtumonde.FP alkalmazás
Elterjedtsége a júliusi fertőzések között: 7.77%

Működés: Ez a kártevő szintén a kéretlen alkalmazások táborába tartozik az ESET kategorizálása szerint. Futása közben különféle felnyíló ablakokat jelenít meg. A trójai megkísérel egy távoli szerverhez csatlakozni, és onnan további komponenseket letölteni.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

3. WMA/TrojanDownloader.Wimad.N trójai
Elterjedtsége a júliusi fertőzések között: 4.79%

Működés: A Wimad.N egy trójai letöltőprogram, amely a Win32/Adware.PlayMP3Z vírust telepíti a PC-re. A kártevő úgy kerül a

számítógépre, hogy a felhasználó figyelmetlenül elfogadja a licencszerződést, amellyel egyúttal jóváhagyja a további tartalmak letöltését. Az Adware programok általában azáltal válnak ingyenessé, hogy cserébe bele kell egyezni, hogy reklámokat jelenítsenek meg a gépünkön.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

4. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a júliusi fertőzések között: 1.96%

Működés: Az Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró-adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.

5. Win32/CMDOW.143 alkalmazás
Elterjedtsége a júliusi fertőzések között: 1.68%

Működés: A cmdow.exe állományra sok antivírus program nem jelez, hiszen nem vírusról, hanem egy hacker eszközről van szó. A Cmdow egy olyan parancssori segédprogram, melynek segítségével Windows NT4/2K/XP/2003 rendszereken kilistázhatjuk, átmozgathatjuk, átméretezhetjük, átnevezhetjük, elrejthetjük, vagy ismét láthatóvá tehetjük, minimalizálhatjuk vagy kinagyíthatjuk, helyreállíthatjuk, aktiválhatjuk illetve inaktiválhatjuk, továbbá bezárhatjuk, leállíthatjuk az ablakokat. Az eredeti cmdow alkalmazás egy 31 KB-os végrehajtható fájl, amely nem ír a rendszerleíró-adatbázisba, nem igényel külön telepítést, elég lefuttatni. Eltávolításához elegendő ezt az állományt törölni.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.

6. Win32/Adware.SearchAid alkalmazás
Elterjedtsége a júliusi fertőzések között: 1.47%

Működés: Jellemzően egy olyan alkalmazásról beszélünk, amely a böngészőben felbukkanó kéretlen pop-up hirdetéseket jelenít meg. Különböző szoftverek telepítésénél a licenc szerződés megemlíti a jelenlétét, de ezt sokan nem olvassák el alaposan, hanem automatikusan elfogadják.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.

□ IN□/Autorun vírus
Elterjedtsége a júliusi fertőzések között: 1.30%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár .mp3 lejátszókon) terjed.

8. Win32/VB.EL féreg
Elterjedtsége a júliusi fertőzések között: 1.25%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows rendszerleíró-adatbázisának HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is.

A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez, stb.) csatlakoztatásával terjed.

9. Win32/Adware.AdMedia alkalmazás
Elterjedtsége a júliusi fertőzések között: 1.12%

Működés: Windows rendszereken terjedő kéretlen reklámprogram, amely eltéríti, illetve manipulálja az Internet Explorer böngésző forgalmát. A megtámadott számítógépbe beépülve különböző kártékony .dll állományokat hoz létre, illetve tölt le az internetről, a rendszerleíró-adatbázisba pedig olyan bejegyzéseket készít, melyek segítségével gondoskodik arról, hogy a kártékony kód minden rendszerindításkor automatikusan lefuthasson. Működése során több különböző kártékony weboldalhoz is megpróbál kapcsolódni, és a megfertőződött rendszer a tulajdonos tudtán kívül képes más weboldalak ellen indított DoS támadásban is részt venni.

A számítógépre kerülés módja: Trójai programokkal, észrevétlenül települ a gépre.

10. Win32/Adware.PlayMP3Z alkalmazás
Elterjedtsége a júliusi fertőzések között: 1.00%

Működés: Ez az alkalmazás a kéretlen és felesleges alkalmazások körébe tartozik. Kéretlenül reklámokat jelenít meg, MP3 tartalmakat és lejátszóprogram-komponenseket tölt le. Automatikusan nem képes terjedni, ehhez szüksége van felhasználó közreműködésre is. Az elemzése alapján feltételezhetően Kínából származik.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.

A □liusi toplista 10 szereplője az összes fertőzés 45.21 százalékáért felel, a további, megközelítőleg 55 százalékon már sok, kisebb arányban előforduló kártevő osztozik.

· 1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/600181

Trackbackek, pingbackek:

Trackback: Propeller 2008.08.04. 19:31:00

Antivírus blog – Vírusok, kémprogramok, rootkitek - Nyári szabadságon a vírusírókAz elmúlt három hónapban gyakorlatilag nem változott a Magyarországon legtöbb fertőzésért felelős vírusok toplistája, még [...]

Kommentek:

Gery Greyhound // · http://www.bestofgyurcsany.hu 2008.08.04. 19:49:04

Ez a Virtumonde valami nagyon nagymájer vírus lehet, mert ez az első vírus amit az elmúlt 1-2 évben még nekem is sikerült beszopni. És rendszeresen visszajön, legalábbis a panda naponta nyávog hogy megölte. Hogy lehet véglegesen kiírtani?

==T== 2008.08.04. 20:10:54

NOD 32-vel:)

Fikázó · http://zsarufika.blog.hu/ 2008.08.04. 20:18:53

Gery- nekem a Nod32 supportja segített, érdemes őket választani!

dX 2008.08.04. 21:06:59

az egyetlen ami végleg segített (több helyen):
www.malwarebytes.org/
ingyenes, tud magyarul

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.04. 21:31:15

Hello Gery!
A Virtumondeból nagyon sok változat van, és a készítők is beleadtak apait-anyait, hogy megnehezítsék a biztonsági progik dolgát. Több verziója rootkitet is megpróbál telepíteni a megtámadott gépre.

A Pandához sajnos nem értek ;-) Ha új, 3.0-ás NOD-dal nézed (van 30 napos próbaváltozat), és minden fullra van állítva, elvileg észre kell vennie. Sok esetben a heurisztika találja meg, de nemrég volt egy jelentős Virtumonde és Zlob szignatúra frissítés. Egy próbát szerintem megér, és ha elakadnál, a support KUKAC sicontact PONT hu címen szívesen segítenek neked :-)

Eltiron72 · http://haragszom.blog.hu/ 2008.08.05. 13:52:20

Nos, én is beleszaladtam ugyanebbe- nekem a büdös életbe nem volt még virusom.
Az avg 8.0-t első körben hazavágta. Ajánlották, hogy probálkozzam a Kaspersky-vel- azt már telepíteni sem tudtam. De persze ilyen helyzetekre ott a panda- ami 20 percenként diadalmasan közölte, hogy márpedig neki sikerült kiírtani- kb annyira mint Gyurcsánynak a korrupciót(ha már Gery Greyhound van itt...:))
Happy end nincs: 5 nap kétségbeesett harc után szombaton format c:/.
350 GB-nyi adat hullott el.

HGyöngyi · http://blog.ladyuser.eu 2008.08.20. 09:49:54

Mostanában óvatos duhaj vagyok. Megosztottam a lemezem két partícióra. A C:/-n csak a programok vannak. Ha mindenképpen le kéne formázni, ne essek kétségbe. (Azért persze az archiválási szokásaimon lenne mit javítani :))

Más: Több helyen olvasom, hogy a NOD32 csak megfelelően beállítva tud célt érni. Mindenütt leírják: megfelelően, de sehol nem találok arra ajánlást, hogy mi is lenne az a megfelelően. Legutóbb addig kísérletezgettem, amíg az Internetre sem engedtem ki magam :)))
Biztos előbb-utóbb megtalálnám a Felhasz. Kézikönyvvel karöltve, mit-hogyan, de egyelőre, maradtam "gyári" alapbeállításon.

Tanács? Mire figyeljek, ha mégis beállítgatni jut időm? Köszönöm.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.21. 10:07:06

Szia Göngyi!
Ami szerintem alapból kellhet, ehhez menj el a Beállítások menübe.
Valós idejű védelemnél:
- Anti Stealth technológia engedélyezése
- Kéretlen alkalmazások keresése
- Veszélyes alkalmazások keresése

Ezek a Webhozzáférésvédelemnél (IMON) is legyenek bekapcsolva (emlékeim szerint a Kéretlen és a Veszélyes alapból nincs kiválasztva).

Hasznos még a TreatSense.Net Korai Riasztási Rendszer engedélyezése is, ez a gyanús fájlokat elküldi a laborba.

Jó ötlet, ha logfile készül, van mit nézni a későbbiekben, ha pedig többen használtok egy gépet, védheted a NOD32 beállításokat jelszóval elpiszkálás ellen.

HGyöngyi · http://blog.ladyuser.eu 2008.08.22. 10:21:57

Köszönöm. Átnézegetem a beállításaim.

Csini Nyuszi színrelép

2008.08.06. 14:15 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: flash frissítés szabadság kocka twitter trójai

A Twitter nevű közösségi hálózaton kissé felbolydult az élet, **a kártevő terjesztők a Facebook és a MySpace után ide is befurakodtak**.

Biztonsági **szakértők vették észre**, hogy egy hamis Twitter profil mögé helyezett kamu letöltés a már ismert **Adobe FlashPlayer frissítési trükkel** igyekszik trójait telepíteni az áldozatok Windowst futtató gépére. Persze azt is mondhatnánk, így jár aki **pornográf video linkre kattint**. A fertőzött gépeket pedig igyekeznek saját céljukra - spamterjesztés, jelszó lopás, távoli támadások indítása - felhasználni. Az első vizsgálatok szerint a támadás feltehetően Brazíliából származik, legalábbis a portugál nyelvhasználat alapján erre jutottak a magát Pretty Rabbit, azaz Csini Nyuszinak nevező felhasználó profillapjának átnézése során.

A közösségi hálózatok egyébként azért is lehetnek **veszélyesebbek, mert az ottani, főként fiatalkorú felhasználók automatikusan jobban megbíznak egymásban**, az üzenetekben és linkekben.

Az élet apró örömei rovatunkban büszkén számolhatunk be arról, hogy a Goldenblog 2008 IT kategória győztese, az általunk is nagyra tartott Kocka Blog érdemben hivatkozik ránk, egészen pontosan a felhasználók operációs rendszer használatát firtató szavazási eredményünkre.

A minap a **Nyári szabadságon a vírusírók** címmel jelent meg post, ezért most ezúton szeretnénk az alkalmat gyorsan kihasználni, és bejelenteni, hogy **az antivírus blogot írók;-) is nyári szabadságra indulnak néhány napra**. Aki épp most készül még egy kicsit ideje pihenni, vagy éppen most nyaral, annak **jó pihenést kívánunk, és hamarosan újra jelentkezünk**.

· 1 trackback

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/603493

Trackbackek, pingbackek:

Trackback: Propeller 2008.08.06. 14:22:58

Antivírus blog - Csini Nyuszi színrelépA Twitter nevű közösségi hálózaton kissé felbolydult az élet, a kártevő terjesztők a Facebook és a MySpace után ide is [...]

Kommentek:

Nincsenek hozzászólások.

Hamis CNN, hamis YouTube

2008.08.21. 16:24 | Csizmazia István [Rambo] | 5 komment

Címkék: spam breaking youtube cnn news hamis

Egy jól felvértezett környezetben **szinte ellene kell dolgozni a védelmi programoknak, és háromszor annyi munkára, kattintásra van szükség** ahhoz, hogy a kétes emailekben kapott trójai letöltő linkek mégis becsaphassanak minket. A statisztikák tanúsága szerint **mégis ez történik**.

Nem kis mennyiségben hemzsegtek a CNN álhírszolgáltató levelei a postafiókban, és bár jó hír lehet, hogy **Lolobrigida mégsem lett öngyilkos, George W. Bush mégsem csapta be Tony Blairt**, Lindsay Lohan kebleiről nem is beszélve.

Hogy Paris Hilton börtönbe vonulna, az szinte már hihető, ahogyan az is, hogy akár a Google is indíthatna ingyenes zeneletöltési szolgáltatást Kínában;-) Mondhatjuk, **jó trükk ez a Kiküldött tudósítónk jelenti, Breaking News**, stb. szlogen, és **egységes feladó**.

Manapság ha valaki Adolfo Romano, Gomez Chang, Malyomváry Armando és egyéb nevektől érkező leveleket olvas, annak mellékleteit zaklatja egerével, arra már **szinte sajnálkozva gondolunk**, hogy nem százas fejben, és **vélhetően kevesebb esze van egy hintalónál**. Már szinte várjuk, kinek fog először eszébe jutni Google Alerteket és hasonló sajtószemlézőket hamisítani spamjaivel. **Célzott támadáshoz is jó eszköz lehet ez**, először megnézni az Iwiwen, mi is pontosan az **illető célszemély érdeklődési köre** (autó, fotó, zene, sport, nők, kutyák, stb.), aztán abban a témában megszórni ilyen érdekes hírekkel, levelekkel - persze ekkor szigorúan semmi Viagra, Cialis vagy Rolex - hiszen ez azonnal felkeltené a gyanakvást.

Ha például valaki a weben Gmaillel levelezik, vagy a több platformon is elérhető Thunderbird klienst használja, **több, mint elegendő figyelmeztetést kap** az ilyen csalárd leveleknél.

"A Thunderbird szerint ez az üzenet becsapós lehet" - jön az intés, és ezt nekünk egy külön kattintással kell felülbírálni, elutasítani - hasonlóan a böngészőbeli Finjan, McAfee, Netcraft, stb. figyelmeztetéseknél.

Ugyanez a Google levelezőjében még olajozottabb, ott már nem is látjuk, sőt nem is aktív az ilyen link, hanem **egy piros ablakos mondat szól arról, csaló levelet kaptunk**, felejtsük el.

Hasonló a helyzet akár az Internet Explorer, akár a Firefox esetében, **ha a Siteadvisort használjuk: egy külön kattintással felül kell bírálni a figyelmeztetést**, hogy mégis eljuthassunk oda.

Ezek alapján **sokan valóban megdolgoznak azért, hogy megfertőződhessenek**. Ha még hamis Google Alert nincs is, de **az első hamis YouTube video már megérkezett**.

A lapon a **menüsor linkjei az igazi YouTubera mutatnak**, csak az aktuális mozi linkje próbál egy kártevőt letölteni. Mivel az internetes **forgalom jó nagy részét már videomegosztó oldalak adják**, a jövőben is érdemes lesz figyelni, mire kattintunk.

Kevésbé erotikus élmény lehet egy letöltő trójai programot bekapni...

· **1 trackback**

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/625846

Trackbackek, pingbackek:

Trackback: Propeller 2008.08.21. 16:46:04

Antivírus blog - Hamis CNN, hamis YouTubeHáromszor annyi munkára, kattintásra van szükség ahhoz, hogy a kétes emailekben kapott trójai letöltő linkek mégis [...]

Kommentek:

□ndie 2008.08.21. 20:41:45

Kb 2 hete esett be az első CNN alert, aztán jött az MSNBC is dögivel. Kb 4-5 naponta, mindkét fajtából. Ez 10 levél naponta.
Kb 1 hete beállitottam a Mozilla szüröjét, hogy ha ezek a szavak vannak a tárgyban, akkor Delete from POP3.
Azóta csak a szokásos 8-10 egyéb spamom jön. És mindez egy alig használt, privát mailcimnél.

Törne le a keze az összes buzinak, amelyik spammel.

fraki 2008.08.21. 22:28:07

Andie, használd a gmail spamszűrőjét. Azaz: állíts be egy gmail-fiókot úgy, hogy leszedje a te POP3-adról a leveleket, az átmegy a gmail spamszűrőjén, te pedig a levelezőkliensedben a gmail-fiókról szedd le a leveleket.

Yann Le Pentrec · http://lnk.bz/t7c 2008.08.21. 22:59:27

Én is így állítottam be, ahogy fraki mondja. A nagy többsége a levélszemétnek fennakad...

Till S. Seemann · http://seemann.blog.hu 2008.08.21. 23:29:29

hát... nekem még mindig csak viagra-árus "barátaim" vannak... persze minden egyből pakolja őket spamba (gmail, live)... de azért idegesítő. főleg az, hogy még a nemregisztrálós-vigyázokrá ímél címemre is napi 10 jön...:S

Andie 2008.08.26. 08:13:08

fraki, ez remek ötlet. Meg is nézem. Beállitani eccerü? (egy gyakorló programozónak :)

Ki csinál szódát? Hát a sziPhone!

2008.08.22. 11:33 | Csizmazia István [Rambo] | 3 komment

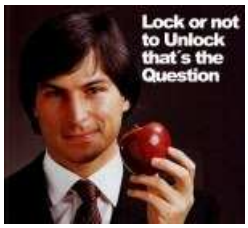
Címkék: biztonság iphone kártevő kémprogram

A jó kis ős Bikini cím arról ugrott be, hogy az értelmes név okán "szifon"-nak becézik az iPhonet. Az esti celebekkel ékesített sorbanállós, visszaszámlálós buli után sokan ma veszik át a hőn várt telefont.

Lehet, hogy a sorbanállók még a dal szövegére is emlékeztek? **"Mindent akarok, de azt most rögtön. Mindent akarok azonnal!"** Mi mindenesetre összeszedtünk pár gondolatot, biztonsági információt **az új tulajdonosoknak**.

Az eladott **iPhone 3G darabok száma már meghaladta a 3 milliót**, az Apple pedig az év végéig összesen 10 millió készülék eladásában reménykedik, ami szinte biztosan teljesül is. De emlékezzünk csak egy pillanatra a vírus és kártevőkészítők szerint, mik is egy vonzó célpont ismérvei? Legyen **az adott platform elterjedve** (jó), **legyen jól dokumentált** (ez már kevésbbé felel meg) és **érje meg a befektetést** (jó, alakul).

Még az év elején jelent meg az első kártevő iPhonera, erről mi is beszámoltunk. Ez egy **hamisított 1.13-as firmware frissítés volt**. Aztán voltak félelmek, miszerint **az Apple megfigyeli a felhasználók** telefonos szokásait, és **továbbítja az Apple szervereire a látogatott weboldalak, emailcímek, hívások adatait.** Nemrégiben pedig **egy hacker észlelte, hogy rendszeresen ellenőrzésre kerülnek a telefonra telepített alkalmazások**, melyek közül távolról központilag is tudnak törölni. Ezt **először tagadták, végül beismerték**. (Lassan kezdenek az MS babérjaira törni).



Először is **bármennyire szeretnénk** ilyen készüléket, legyünk óvatosak ha használtan hirdetés alapján vásárolunk. Profi csalók is kihasználják a népszerűséget, de nem kizárható az előre telepített kémprogram sem. És mellesleg ne higgyünk a reklámoknak! ;-)

Jó ötlet lehet, ha a BlueTooth szolgáltatás csak arra az időre **van bekapcsolva, amikor valóban használjuk is**. Érdemes ezt **rejtett módra** állítani, és ha vásárlás után **a telefon default nevét rögtön megváltoztatjuk** valami egyéni, semleges hangzású névre (pl. NOKIA 1234 ;-), szintén hasznunkra válhat: nincs felhívás keringőre.

A használt **alkalmazások frissítése itt is fontos** szempont lesz - például a Safari böngészőhöz is jelennek meg javítófoltok - rendszeresen tájékozódjunk ezekről, töltsük le és telepítsünk őket biztonságunk érdekében.

Lehetőleg ne használjunk feltört, kétes forrásból származó firmwaret (csak ha muszáj ;-), hiszen elvileg ezekbe is telepíthetnek kémprogramokat.

on t Piszka! - szól az intelem, de az Apple szinte kiprovokálta, hogy a hackerek megismerjék, feltörjék, függetlenítsék a készülékeket. A kérdés, hogy ez a tudás nem kerül-e majd rossz kezekbe is?

Csak **megbízható forrásból származó programokat**, alkalmazásokat, játékokat telepítsünk szintén hasonló okokból. Ezt lesz a legnehezebb betartani, hiszen az ingyenes alkalmazásokon túl mindent vásárolni kell/kellene. Az óvatosságra annál is inkább szükség lehet, mivel itt minden alkalmazás root joggal fut a gépen, emiatt egy trójaival elvileg mindenhez hozzá lehet férni.

Reméljük **a poszt azért senkinek nem vette el a kedvét** attól, hogy a közeljövőben szifon birtokos legyen. Mi mindenesetre figyelni fogunk az eszközzel kapcsolatos biztonsági hírekre, eseményekre **és reménykedünk**, a Safari hibák javításánál megismert tempónál itt majd **gyorsabb reagálásban lesz részünk**...

· 1 trackback

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/627237

Trackbackek, pingbackek:

Trackback: Propeller 2008.08.22. 12:00:41

Antivírus blog - Ki csinál szódát? Hát a sziPhone!Összeszedtünk pár gondolatot, biztonsági információt az új iPhone tulajdonosoknak.

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.24. 09:08:02

Úgy látom, itt is kiemelten fontos lesz a gyors firmware frissítés, illetve születőben a 0day iparág:
www.heise-online.co.uk/security/iPhone-dials-by-remote-control--/news/112023

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.02. 10:52:13

Egy kis érdekesség az iPhone warez témából:
index.hu/tech/net/2009/04/01/kitort_a_haboru_a_warez-itunesok_kozott/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.12. 10:53:57

annak helyek, ahol elég szólni a szülőknek, ideje megvenni a tanszeremet :-D
index.hu/tech/blog/2009/05/12/kotelezo_az_ipod_egy_amerikai_egyetemen/

Trükkös keresés és elcsúfított weboldal

2008.08.25. 17:01 | Csizmazia István [Rambo] | 4 komment

Címkék: google cache sql deface injection

Egy érdekes TheRegister-es cikk említi, hogyan lehet az **olyan fórumokban lévő információkat elolvasni, amihez eredetileg név-jelszó** lenne szükséges.

A dolog **egyáltalán nem új**, valamilyen formában talán mindenki használta már, aki Google segítségével keresett valamit. Előfordul időnként, hogy egy jelszóval védett fórumban lenne a keresett válasz, de a találatra kattintva csak a belépő adatokat kérő ablakot látjuk.

Ilyenkor **néha segít, ha a "Tárolt változat"-ot** választjuk. De van ennél furmányosabb módszer is, ami abból áll, hogy a nem olvasható linket bemásoljuk egy Google keresési ablakba, és **eléje "cache:" szöveget gépeljük**. És tadaam, sok esetben (ha nem is mindig) be is jön az áhított tartalom.

A cikk végén szerepelt még egy weboldal, amit a **gazdája jó idő óta elhanyagol** - magyarán ez azt jelenti, hogy nem nézi sem rendszeresen, se rendszertelenül. És **azt sem veszi-vette észre**, hogy azt illegálisan módosították. Az, hogy az illető itt nem akárki, jelen esetben indiferrens.

Ebből nagyjából azt akartam kihozni, hogy **ha valaki a saját gépén becsülettel frissíti az OS-t és az alkalmazásokat, pedánsan antivírus, tűzfal és kémprogram irtót is használ - az még mindig lehet kevés**, ha a rábízott jószágokat (értsd **saját weboldal, vagy weboldalak) parlagon hagyja heverni** ebek harmincadjára. Jó esetben egy fehérkalapos hacker megírja neki, hogy baj van az oldalán, és ha ideje engedi, javítson. Rosszabb esetben **kéretlen dolgokkal tömik ki** - mint ezt az oldalt is - sőt legrosszabb esetben **kártevők terjesztésére, letöltésére használhatják**.

Ha valakinek weboldala van, nézzen rá időnként (nem törték-e fel, nem babrálták-e meg az SQL adatbázist, stb.). Ha erre **nincs ideje vagy esetleg nem ért hozzá, akkor pedig bízzon meg ezzel valakit**. Ha ezt sem teszi, inkább ne legyen weboldala, mert nem tudja felelősséggel birtokolni, karbantartani. Szlengesen szólva akkor "az már nem az ő weboldala" lesz.

Magyarán, **patyolattiszta számítógéppel rendelkezve is lehetünk kártevő terjesztők**, legyünk hát alaposabbak és figyeljünk jobban ezekre az erőforrásokra is.

1 trackback

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/631931

Trackbackek, pingbackek:

Trackback: Propeller 2008.08.25. 17:36:38

Antivírus blog - Trükkös keresés és elcsúfított weboldalHogyan lehet az olyan fórumokban lévő információkat elolvasni, amihez eredetileg név-jelszó lenne szükséges.

Kommentek:

dark future · http://www.andocsek.hu 2008.08.25. 21:52:59

A weboldalak figyelését lehet automatizálni is, hogy ne kelljen folyton nézegetni. Ellenőrithető pl. a html kód hossza (jellemző módon a nyitóoldalt érdemes figyelni, mert úgyis leginkább azt törik meg), vagy figyelhetők stringek (adott szavak, mondatok eltűnése vagy felbukkanása). A www.netdiag.hu oldalon pl. egy perces figyelési gyakoriság is beállítható, riasztáskor kérhető email vagy sms.

A másik trükk az, hogy időről időre (pl. óránként) egy időzített script vagy batch file valamilyen védett helyről (amihez nincs webes hozzáférés) átmásolja az üzemi területre a html oldalakat (ez statikus oldalaknál bevált).

A feltörők dolgát is meg lehet megnehezíteni, pl. azzal, hogy nem c:-re húzzuk fel a rendszert, hanem más betűre, és a webes mappa sem ott van, ahol a rendszer. Windows esetében érdemes még a cmd-t is átnevezni/áthelyezni (némi kis trükkel, mert azért nem olyan egyszerű :-)).

Tgr 2008.08.25. 22:26:10

A cache-es trükk egész komoly oldalaknál is bejön néha, pl. az experts-exchange-nél jó darabig így lehetett megkerülni a védelmet.

"patyolattiszta számítógéppel rendelkezve is lehetünk kártevő terjesztők"

A fordítottja is igaz: hiába van bombabiztos, mindenféle exploit ellen védett oldalunk, ha a saját gépünkre nem vigyázunk... A minap találkoztam olyan trójaival, ami kiolvassa mindenféle népszerű FTP-kliensek mentett jelszavait, felcsatlakozik az oldalakra, és átírja az ott talált php-fájlokat.

fabatka 2008.08.26. 08:05:12

Ha már a google-t beengedi a lap a védett oldalakra, akkor akár mi is kiadhatjuk magunkat a google robotjának, amihez csupán a böngésző által elküldött user agent-et kell megváltoztatni, amit pl. a firefox-os user agent switcher-el is meg lehet tenni.

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.08.26. 10:32:36

Hello Dark Future!
Köszi az ötleteket, nem is tudtam hogy Andocsekék ilyennel is foglalkoznak.

Pavlovi reflexeink

2008.08.26. 15:32 | Csizmazia István [Rambo] | 5 komment

Címkék: licenc jelszó szerződés figyelmetlenség e mail pavlov phishing

Szinte bizton állíthatjuk: ha valaki **postán, bélyeggel feladott levélben faggatna minket személyes és bizalmas adataink felől, kizárt, hogy válaszolnánk neki**. Esetleg rövid úton elküldenénk a pokolba. Ám ha mindez e-mailben vagy egy weboldal űrlapján történik, mintha rózsaszín köd ereszkedne a többség szeme elé.

Van **ez az ősrégi "adategyeztetéses" beetetés**, phishing ügyekben sem volt ez másként, de persze mindig van új a nap alatt, most éppen egy amerikai egyetemen tolják. Hivatalosnak látszó levélben keresik meg a diákokat, és megkérik, **frissítésképpen ugyan adják már meg nevüket, jelszavukat**. És persze a **nagy számok törvénye alapján volt is**, aki így tett. Vagyis a dolog működik.

Miért nem figyelünk jobban? Ki érti ezt? Hogyan, miért és egyáltalán? Ha már ilyen mélyenszántó talányokat boncolgatunk (ha a vajas kenyér mindig a vajas felére esik, és a macska mindig talpra esik, mi lesz ha a macska hátára kötjük a vajas kenyeret és úgy dobjuk le; avagy ha a repülőgépek fekete doboza mindent kibír, miért nem készítik az egész gépet ebből az anyagból; illetve hogy a hóekevezetők reggel hogyan jutnak el a munkahelyükre?), **nem tanulság nélkül való a Pavlovi kutyákra való utalás**. Ha van **aki Win mellett, vagy után használ Linuxot** (aki esetleg Linux helyett állt át Winre szóljon ;-) és kapkodósan kattintgat az egérrel, eleinte valószínűleg sok szentség-szakramentumozás hagyja el ajkait.

Linux alatt...

... és ugyanez Windows alatt

Két multiplatformos alkalmazáson **be is mutatjuk ennek az okát**. Az egyik az Audacity nevű hangszerkesztő alkalmazás, a másik a szintén ingyenes, tüzes róka névre hallgató böngészőkliens. Ha már sokat használtuk ezeket, és **ha kezünk gyorsabb, mint az eszünk**, könnyen az ellenkezőjét választhatjuk annak, amit eredetileg akartunk :-O Kicsit olyan érzésünk van, mint egy vak kisgyereknek, akinek átrendezték a szobáját.

A gombok helye és sorrendje...

... nem szentírás

Emellett persze vannak a **"miénk a malware, magunknak telepítjük"** mozgalom hívei, és valljuk be, az a fránya licencszerződés véletlenül, vagy **éppenséggel szándékosan olyan hossz□, hogy ehhez képes** a Háború és Béke, valamint a Moby Dick a fehérbálna története Örkény egyperces novellának tűnik.

És aztán van a **"nincs rajtunk füstsz□rős sapka"** esete is, a licenc szerződés már csak azután jön, amikor már rég a gépünkön tombol és csörgeti láncait a kártevő, az Antivirus XP 2008. Persze vegyük észre (ez volt a középiskolai matek órán az egyik kedvenc mondatom:-) **milyen választási lehetőségeket is ad az ablak**, azon felül, hogy becsukási lehetőség egyáltalán sincs rajta?

□1 trackback

□jánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?

□ bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/633757

□rackbackek, pingbackek:

□rackback: Propeller 2008.08.26. 16:05:57

Antivírus blog - Pavlovi reflexeinkSzinte bizton állíthatjuk: ha valaki postán, bélyeggel feladott levélben faggatna minket személyes és bizalmas adataink felől, [...]

□ommentek:

morph 2008.08.26. 22:27:□8

bocsi, de ez nekem tök összefüggéstelen, nem jön le, hogy tulajdonképpen mit is akarsz mondani.

□ogyoo 2008.08.26. 22:38:16

Pavlovi reflex részét még értem, hogy a rutinos rókák csak nyomják a gombot, el se kell olvasniuk, tudják fejből minek hol a helye. De, hogy az adategyeztetős sztori hogy jön ide, azt nemtudom :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.08.26. 23:16:36

Hello Morph és Bogyoo!

dv a blogban :-)

Az volt eredetileg a gondolatom, hogy ez mind valahogy összefügg. Kérnek tőlem valamit (account) és én automatikusan odaadom (nem gondolkodom). Telepítek, licencre kattintok (nem gondlkodom). Megszokásból szoftvert haszbálok, rutinszerűen kattintok (nem gondolkodom). EZ lett volna a vörös fonál, hogy több figyelem, tudatosság kellene.

Az egy gombbal rendelkező licenc ablak meg adja magát, ott (akkor már) mindegy, hogy gondolkodom-e vagy sem.

Péter 2008.08.27. 00:26:10

huh, hát ez a cikk nekem is elég lazán van összeszerkesztve...

atleta.hu · http://www.atleta.hu 2008.08.27. 01:12:8

Tenyleg eleg zagyva igy osszehordva, pedig az egyes gondolatokbol lehetett volna irni ertelmes bejegyzest. Mondjuk a phishingrol.

De amihez hozza akartam szolni: annak, hogy a multiplatform alkalmazasok kicsit maskepp neznek ki a kulonbozo platformok alatt az az oka, hogy alapvetoen az adott platformhoz igazodnak. Nyilvan a windows juzer szamara az lenne a legkenyelmesebb, ha a windows alatt megszokott multiplatform alkalmazasa pont ugyanugy viselkedne linux alatt, ha veletlenul egyszer odaul ele, csak hat nem o a celkozonseg abban az esetben, hanem az atlag linux user, aki viszont megszokta az osszes tobbi linux alkalmazas mukodesenel mondjuk az igen/nem gombok sorrendjet. (Es persze vice versa az alkalmi windows hasznalo esetere.) Ha nem igy lenne, akkor az adott platformon (mundjuk linuxon) a mashonnan attevedo juzer ugyan kenyelmesen erezne magat, a tobbseg viszont utalna az alkalmazast, amiert maskepp viselkedik. Kik vannak tobben? Naugye :).

A platformok kozt ugralas amugy is zavart fog kelteni a fejben, amig mindkettohoz hozza nem szokik az ember (plusz a valtogatashoz!).

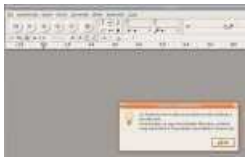
Vírus MP3-ba ágyazva

2008.08.28. 12:12 | Csizmazia István [Rambo] | 1 komment

Címkék: mp3 vírus nod32 wma kártevő

Most egy **olyan kártevőt mutatunk be "Kipróbáltuk" rovatunkban, amely egy MP3 kiterjesztésű állományban terjed**, a média lejátszó pedig neki is ront bőszen. Igaz, **lejátszani nem tudja, de a fertőzést elindatani azt Summa cum Laude igen**. Ez itt nem Unplugged, ha Reloaded! Mostantól érdemes lesz a zenékkel résen lenni!

Az állomány hozzánk ezúttal **"meie_mees_turvamees_1_.mp3" néven érkezett**, és szépen riasztott rá a NOD32. Nosza, felgyűrtük ingujjunkat amúgy Peter Nortonosan, és elkezdtünk vizsgálódni.



Első kísérlet egy **Linux alatti Audacity volt, de hiába vártuk** a felcsendülő ritmusokat a hangszóró felől. Ideje volt egy hexaeditorral is belekukucskálni, és a fájl szerkezet máris rögtön meglepetéssel szolgált: bár zeneállományt látunk, de **szó sincs MP3-ról**. Hanem egy WMA, aza Windows Media Audio szám mosolyog ránk.

Gyalogolva az állomány belsejében máris konstatálhatjuk, a kártevőkészítők furfangos emberek, és okulva az ingyenes vírusírtó 80 kB-ban történetből, **annyi 00 bájtot ragasztottak a kód végéhez, ami nem csak egy átlag MP3 zene hosszának**, de akár az eredeti zeneszám hihető hosszának is a közelében jár.

Át is ülünk gyorsan a Windowsos géphez, de ahhoz hogy audiofil élvezetben részünk lehessen, nyomban **ki kellett kapcsolnunk a valósidejű fájlrendszer védelmet a NOD32-ben**, hogy ne riasszon és ne törölje egyből az állományt. Az előkészületek után a húrok, illetve **a Windows Media Player közé csapunk**.

Először persze megkapjuk a reklamációt - hogy ez itten kéremszépen nem is igazi MP3 - de azért jótékonyan felajánlja a lejátszást. A megjegyzést, miszerint **"a lejátszás váratlan következményekkel járhat"** öszönösen érezzük, sosem kellett még komolyabban venni. Azonban csak **néma csend fogad bennünket**, egy árva hangjegy nem sok, annyi sem árad felénk. Körülbelül tíz másodpercnyi molyolás után aztán megkapjuk a hibaüzenetet:**a fájl nem játszható le.**

(Erről jut eszembe egy kedves történet, volt egy zene és HiFi megszállott barátom, aki nagyon szerette és velem is ő ismertette meg Frank Zappát. Sok szép bakelit albuma volt már - a 70-es évek végén járunk - és mondta, hogy nyáron Angliába megy a család, onnan is hoz majd egy lemezt. Meg is hozta, de pechjére nem számolt Zappa extrém személyiségével és óvatlanul a boltban sem hallgatta meg. Ez volt

az 1979-es Silence című album, kétszer 22 perc tökéletes csend a barázdákba vésve, de az A oldal végén egy hang azért pedánsan bemondta, hogy fordítsuk meg a lemezt :-)

Esetünkben viszont szólásra emelkedik - pedig nem is hívta senki - **az alapértelmezett b□ngésző**, és a Win32/TrojanDownloader.Wimad.N máris orvul tölti le, azaz **csak t□ltene le** egy másik, szintén kártékony **PLAY_MP3.exe állomány**

Szerencsére az IMON webhozzásférésvédelem aktív, és fülöncsípi - más füllel kapcsolatos dolog nem is történik már a postban.

A **WMA fájltípus választása szándékos**, mint natív Windows állományt jól fel lehet használni támadásra (pl. szkriptelni), de mivel az MP3 népszerűbb, így **a trükk része az átnevezés** is.

Gyaníthatóan emelkedni fog az ilyen fertőzések száma, **hatásosnak tűnik**, mind az öntudatos "Én aztán nem használok jusztse vírusirtót" csoport ellen, mind pedig az óvatlan és tudatlan Windows átlagfelhasználók ellen. Mindenesetre továbbra se igyunk mosatlan gyümölcslevet, **zene letöltésnél mindig használjunk antivírus programot, és persze NoScript rulez :-)**

· **1 trackback**

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/637431

Trackbackek, pingbackek:

Trackback: Propeller 2008.08.28. 12:35:26

Antivírus blog - Vírus MP3-ba ágyazvaEgy olyan kártevőt mutatunk be "Kipróbáltuk" rovatunkban, amely egy MP3 kiterjesztésű állományban terjed.

Kommentek:

Csutka 2008.09.02. 17:01:58

zene letöltés? Tessék elbattyogni a boltba és megsoppingolni a CD-t vagy olvasni a kommenteket a mininován/TPB-en ;)

Közösségi oldalból botnet művek

2008.09.08. 12:23 | Csizmazia István [Rambo] | 2 komment

Címkék: kísérlet facebook botnet

Nem minden arany ami fénylik - tartja a mondás. Erre most nagyon jó példa az a kutatók által végzett kísérlet, amellyel **a Facebook portál felhasználóit demonstrációs céllal létrehozott facebotnet háló részeseivé változtatták**. A gyanútlan látogatók - bár kéretlen hálózati forgalomban vettek részt - mindebből az égvilágon semmit nem vettek észre.

A **kutatók által végzett kísérletben** létrehoztak egy hamisított, csali applikációt, amely látszólag a National Geographictól töltött le egy a Nap fotója címre hallgató képet a Facebook tag oldalára. **Az applikáció letöltése azonban nem csak ezt tette, hanem egyéb észrevétlen hálózati kérésekkel "zombigéppé" alakította** a számítógépet, mellyel tetszőleges oldal elleni túlterheléses támadás indítható. Amint a Facebook felhasználó kilépett a közösségi oldalról, lecsatlakozott ugyan a botnet hálóról is, de **a következő belépésnél ismét a részesévé vált**.

A Facebook szóvivője úgy nyilatkozott, nem szükséges nagyobb jelentőséget tulajdonítani a támadásnak, **szerinte egy ilyen, többmillió felhasználóhoz eljutni képes** alkalmazást megvalósítani ennél jóval nagyobb feladat és nem jelent veszélyt, maximum párszáz emberhez juthat el.

A **görögországi kutatók - akik zömében a Computer Science munkatársai** - azonban maguk is meglepődtek, mikor azt észlelték, hogy bár **csak a baráti körben említették a fenti Facebook appletet, mégis mintegy ezer ember töltötte le azt**. A legforgalmasabb időszakban 300 kérés is történt egy óra alatt, az egyik napon pedig a letöltés még a 6 Mbit/másodperc csúcsértéket is elérte. A módszer kétségtelenül jól vizsgázott.

JavaScriptes kódokkal **fűszerezve még ennél is kifinomultabb támadásokat** lehet véghezvinni, és ha azt például valamilyen népszerű alkalmazásba ágyazzák bele - mint például amilyen a Facebookbeli fotó-videó megosztó Super Wall napi több millió felhasználóval - ak **ebből elvileg akár a világ legerősebb botnet hálózat** a is kiépíthető lenne. A dolog arra is tanulság, milyen könnyű az embereket rávenni egy tetszetős program letöltésére.

· 1 trackback

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/653578

Trackbackek, pingbackek:

Trackback: Propeller **2008.09.08. 14:07:39**

Közösségi oldalból botnet művekA Facebook portál felhasználóit demonstrációs céllal egy botnet háló részeseivé változtatták. A gyanútlan látogatók - [...]

Kommentek:

buherator · http://buhera.blog.hu 2008.09.08. 13:57:44

Ööö, sztem ez nem egészen így volt: buhera.blog.hu/2008/09/07/facebot_avagy_az_antiszocialis_halozatok

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.08. 14:23:25

Így jár, aki nem olvas Buhera blogot ;-) Javítottam a pontatlanságokat, köszi.

Köhécselő szivattyú és szeméttelep

2008.09.09. 13:07 | Csizmazia István [Rambo] | 3 komment

Címkék: spam csalás and pump dump

Profi **részvénycsalók nyerték el méltó büntetésüket** Amerikában. A **pump and dump módszerre alapozva** egészítették ki jövedelmüket, most viszont jelentős pénzbüntetéssel és 2 éves börtönbüntetéssel néznek szembe.

A "pump and dump" módszer olyan részvénycsalást jelent, amikor a számítógépes bűnözők a gyors meggazdagodás reményében egyes, főleg kis cégek részvényeiről olyan hamis híreket, ál előrejelzéseket, információkat közölnek (például spam üzenet formájában), amelyből a potenciális befektetők tévesen úgy gondolják, emelkedni fognak a cég papírjai. **A mesterségesen felkeltett érdeklődésnek** a spam kampány végeztével azonban vége szakad, a papírok árai gyorsan leesnek, és a befektetők pedig tönkre mennek. Az ügyletben az a haszon, hogy **a csalók először olcsón, áron alul jutnak ezekhez a részvényekhez, az ideiglenes emelkedéskor pedig busás haszonnal adnak túl rajtuk**, és mire a valóság kiderülne, az igazi befektetők már árnyékra vetődnek.

Bár a módszer első hallásra roppant egyszerűnek és túl direktnek tűnik, valójában **igen kifinomultan lehet befolyásolni a tőzsdék világát hamis híresztelésekkel**. És az ilyen csalások hatékony leleplezéséhez gyakran nemzetközi összefogásra is szükség van, mivel a bizonyítás roppant nehéz. Megfelelő tanulmány lehet a tárgykörben a Tőzsdecápák valamint a Dick és Jane trükkjei című amerikai filmek megtekintése.

A klasszikus módszert megtoldották némi hackeléssel azért, hogy jogosulatlanul hozzáférést szerezhessenek brókercégekhez. A mostani bűnügyben az egyik tettest már kiadták az Egyesült Államoknak, a másik pedig egyelőre egy hongkongi börtönben várja a kiadatást. A becsült kár mintegy 300 ezer dollár volt, amely körülbelül 60 vásárlót és 9 alkuszcéget érintett. Talán nem tévedünk, ha azt gondoljuk erről, ez csak a jéghegy csúcsa.

Már várjuk viszont, hogy első magyar Raiffeisen, Budapest, Erste bankos adathalász támadások után **mikor érkezik meg az első ilyen magyar nyelvű részvényakciós spam**. Ahogy az egyik ilyen phishing levél helyesírási hibáktól hemzsegő (**"visszaélések ellenorizése céljából"**) automatikus nyersfordítással készült, sőt később is voltak efféle próbálkozások, így biztosan lesz majd részünk **"Regyisztráljon ingyenesen, és én tiéd bele oda neki récvényt vegyél, ne fürgyé le ottan"** típusú üzenetekben. Később talán jön esetleg helyesen írt, minőségi magyar próbálkozás is, de ennek - mivel túl kis ország vagyunk - **ebben a számítógépes formában talán még nem jött el az ideje**.

Mit lehetne még ehhez hozzátenni? Szerintünk semmit, maximum annyit, hogy tájékoztatjuk az olvasókat, "piros kalap digitális kulcsokat szegett meg" :-) Ezekután már mindenkinek "leeshet", honnan is jött a post címválasztása...

1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/655217

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.09. 13:30:03

Antivírus blog - Köhécselő szivattyú és szeméttelepProfi részvénycsalók nyerték el méltó büntetésüket Amerikában. A pump and dump módszerre alapozva egészítették ki [...]

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.11. 07:43:54

Ha nem is bűnözőktől, de valami nagy machinátortól is remek példa presented by nagybetűs ÉLET: "Egy hatéves hír majdnem bedöntötte a United Airlines-t"
index.hu/gazdasag/vilag/ualws080911/
Mivel hiszek abban, hogy "érdek a világ ura", a véletlenekben meg kevésbbé, ezért most vagy a Google akart magának gründolni egy olcsó repülőtársaságot ;-), vagy egy valamilyen üzleti konkorrens vitt be egy mélyütést.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.25. 21:52:37

Ez is egy gyöngyszem és egyben rémisztő is, azonnal bemozdul a piac: nem kérdez, nem ellenőriz, hanem bambán és azonnal csökken:
itcafe.hu/hir/steve_jobs_szivroham_alhir_ireport.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.29. 12:46:55

Sajnos nem csak részvényt, de embert is tönkre lehet tenni manipulált álhírekkel:
atv.hu/hircentrum/2008_okt_ragalomhadjarat_hajszolta_ongyilkossagba_a__nemzet_szinesznojet____.html

A tökéletes katona

2008.09.10. 15:01 | Csizmazia István [Rambo] | 11 komment

Címkék: mobil mp3 usb fertőzés eszköz automatikus mentés autorun

Marx szerint **a mennyiség egy idő után minőségbe csap át**, ennek szellemében úgy érezzük, a világszerte használt egyre több USB kulcs, iPod és egyéb MP3 lejátszó, hordozható háttértároló van veszélyben az emberek kezében. Számuk elérte, sőt az utóbbi években meg is haladta **azt a kritikus elterjedtségi szintet**, hogy már megéri férgeket, kártevőket, kémprogramokat fejleszteni rájuk.

A cégeknél sokszor van konkrét szabályzat arra, ki és hogyan használhatja a fénymásolót, hogyan nyomtathat, milyen hálózati meghajtókhoz férhet hozzá, stb. Azonban azt már kevésbbé hatékonyan (vagy sehogyan sem) szabályozzák, hogy a **kisméretű, hordozható eszközöket, kamerás telefonokat, fényképezőgépeket, memória kártyákat, stb. a munkahelyen ki és hogyan használhatja, ez pedig egyre inkább veszélyes lehet**: a számítógép alapból kezeli ezeket vagy azonnal USB tárolóként; vagy más eszközként, de legtöbbször adattárolóként is. A kényelmes autoplay funkció elindítja, lefuttatja az autorun.inf állományban meghatározott kódokat legyen az bármi, és a használt antivírus alkalmazás esetleg nem érzékeli (a nem megfelelő beállítások miatt, vagy pedig vadonatúj kártevő esetén). És itt nem is tértünk most ki az adatvédelmi, adatszivárgási aspektusra.

Még az olyan **ártatlannak látszó dolog is bajt okozhat**, ha nem is másolunk fájlokat, **csupán a mobil eszköz akkumlátorát töltjük fel a számítógép USB csatlakozójáról**. Az autorun vak, nem válogat, nem kérdez, nem gondolkodik, **igazi tökéletes katona: csak végrehajt és mindenre képes**. Randy Abrams egyenesen örültségnek nevezte ezt a featuret, hasonlatában úgy festi le, hogy a Windows felhasználók egy olyan hoki meccs részesei, ahol eltörölték a támadó és védelmi vonalakat, mi vagyunk a kapusok, csak éppen a Microsoft elvette tőlünk az összes maszkot, kesztűt, és egyéb védelmi felszerelést, pluszban extra korongokat tett a jégre, és **azt susogja az ellenfél játékosainak fülébe, hogy csak hajrá fiúk, szórakozzatok jól :□ □**

Persze sokszor és sok helyen tanácsolják az automatikus lejátszás kikapcsolását - ehhez mi is csatlakoztunk - de a kommentek is arról tanúskodtak, hogy ez nem mindig olyan egyszerű feladat. A kézi módszerek mellett egyszerűen lehet az effajta beállításokat ellenőrizni, változtatni, finomhangolni például a TweakUI ingyenes segédprogrammal.

Nemrég olyan fertőzött MP3 állományokról ejtettünk szót, ahol a fertőzött zeneállomány - amely valójában WMA szerkezetű volt, csak a kiterjesztése volt álcázva és egy exploitot tartalmazott - képes volt a lejátszás indításakor megfertőzni a számítógépet, és ezzel újabb, **káros kódok automatikus letöltése indult el**. Nemrég kezdődött egy **új jelenség**, ahol pedig **valódi □ 3 állományok sérültek meg** érthetetlen módon, hogy utána már **csak zajosan és sisteregve lehetett lejátszani**, az állományok vizsgálata gőzerővel folyik. Úgy tűnik, az Autorun probléma mellett hamarosan ez is egy erőteljes új irány lehet, ezért ha már Marxszal kezdtünk, akkor egy módosult Leninnel fejezzük be: a biztonsági programok használatán és az autorun kikapcsolásán felül az adatainkat időszakosan és rendszeresen CD/DVD lemezre **menteni, menteni, menteni...**

· 1 trackback

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/656835

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.10. 15:2□:□2

Antivírus blog - A tökéletes katonaA világszerte használt egyre több USB kulcs, iPod és egyéb MP3 lejátszó, hordozható háttértároló van veszélyben az [...]

Kommentek:

whiteCat 2008.09.10. 20:□0:22

Hát én nem USB-n keresztül hanem a töltővel töltöm fel a telefonom. USB-n keresztül a Win azonnal két cserélhető meghajtóként ismeri fel. Ergo reális lehet a veszély

□urrá Torpedó · http://www.youtube.com/watch□v□ b□ □ UneS0□ 2008.09.10. 20:55:21

nálunk a cégnél csak két ember gépén van engedélyezve az usb. az egyik én vagyok, a másik a fejlesztők főnöke.

ha valakinek alami kínja van kettőnkhöz fordul - pl fényképek feltöltése szerverre, stb.

egyrészt így védekezünk az infóból nem profi felhasználók USB kulcsaitól (ami otthon simán kaphat vírust), másrészt így fontos adatok kiszivárogtatásáak lehetőségét is csökkentjük. (lennének amúgy olyan buzgó emberek akik vinnének haza munkát, félig-teljesen kész műszaki dokumentációkat, stb, ami egy fertőzött otthoni gépről kijuthatna)

ha kell van céges Pendrive, azt lehet csak használni. lehet hogy kicsit túlságosan is paranoásak vagyunk bennt a cégnél, de az ördög sohasem alszik...

□ gany 2008.09.10. 21:32:08

Úgy emlékszem ezt nem Marx, hanem valamelyik ókori görög filozófus mondta.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.10. 22:29:5□

Helló whiteCat és Hurrá Torpedó!

Amiket én láttam saját és cimborák munkahelyein, az kb. a szóban és írásban szabályozott volt, de hát a gyakorlatban mindenki azt csinált, amit akart. Azt másolt le, azt vitt haza, stb. Persze jobb helyeken van profilfigyelő, ami kb annyit tesz, hogy ha valaki a szokásos viselkedéstől eltérően szokatlan és a munkaköréhez nem tartozó hálózati meghajtókon próbálkozik, korábbi szokásától eltérően nagy mennyiségű adatot tölt le, másol át, stb. akkor megy a jelzést titokban a főnöknek, rendszergizdának, és számonkérhető az emberke. Sőt olyan is van - igaz ez már más téma - ami adott kulcszsavakra keres a dolgozó emailjeiben, és nem engedi elküldeni, ha vélémezhető. hogy bizalmas anyagot akar házon kívülre küldeni.

Szóval elvileg sok helyen szabályoznak sok mindent, közben gyakorlatilag meg szabad a pálya.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.10. 22:32:□3

Szia Higany!
Jogos a két pont, bár Marx is írt (plagizélt ;-) ilyet, de Hegel is, és nem kizárt, hogy ő meg az ókoriaktól koppintotta :-)

The □reat □estroyer 2008.09.10. 23:33:10

A szopódás ezzel az egésszel az, hogy a windóznál az autorun egy subprocess, ami az automount része, viszont az automount teszi lehetővé azt, hogy amikor beteszel egy cd-t, vagy bedugsz egy pendrive-ot, akkor annak a filerendszerét tudd olvasni. Sajnos az ikszpében már nem tudsz manuálisan befűzni fizikai meghajtókat a fillerendszerbe, illetve az automountot is csak a registryből tudod kiírtani. Az automatikus lejátszás letiltásával sajnos csak a vírusok egy részét lehet kiszűrni, mivel az csak az autorun.inf-ben meghívott alkalmazások futását tiltja le, de ettől függetlenül maga az autoplay ugyanúgy lefut, tehát, ha a fertőzött script az autorunban van, akkor azt értelmezi is...

□ éter 2008.09.11. 00:13:□1

a legjobb ilyesmi amit mostanában láttam, az egy Sandisk (?) USB kulcs volt, ami hardverből hazudott maga mellé egy CD-ROM-ot, amit se letörölni, se autorun-t letiltani nem tudtál. Amint betetted, már tolta is a reklám szemetet. Előtte meg csodálkozott a fószer, hogy miért ilyen olcsó... nagy nehezen aztán meglett a levakaró progi, de nem volt egyszerű meccs... ja, linuxnak is hazudta a CD-t, igaz az autorun ott nem ment, viszont hiába formáztuk bármi alatt, mivel hardverből nyomta nem lehetett spéci cucc nélkül leszedni.

dark future · http://www.andocsek.hu 2008.09.11. 02:19:50

Hölgyek, urak,

még csak TweakUI sem kell, itt egy "célfegyver":
www.netdiag.hu/autorun_off.zip

Használat: linkre katt, megnyitás, autorun_off.reg-re katt, igen, ok.
5 sec az egész, és máris nem nyílnak meg a ronda dögök maguktól.

Ja, és a fájl garantáltan vírusmentes :-)

□ery □reyhound // · http://www.bestofgyurcsany.hu 2008.09.11. 0□:3□:58

Valakinek mond valamit a Hakaglan.G nevezetű féreg? Nálunk a melóhelyen szépen végigfutott szinte minden gépen, ha bedugsz egy pendrive-ot a fertőzött gépbe, akkor az azon levő minden folderben létrehoz egy [mappaneve].exe fájlt, sárga mappa-ikonnal (gondolom, ha be van kapcsolva az "ismert típusú fájlok kiterjesztésének elrejtése" opció, akkor mappának látszik teljesen) és ha ezt elindítja a gyanútlan júzer, meg is van a baj.

Ráadásul van egy olyan kedves mellékhatása a vírusnak, hogy a fertőzés eltávolítása után is (nod32) a CTRL+ALT+DEL billentyűk lenyomására vagy a regedit futtatásakor "A feladatkezelőt/regisztrációs adatbázis szerkesztőt letiltotta a rendszergazda" hibaüzenet ad. Aranyos.

virkid 2008.09.11. 08:33:29

Érdekes a bejegyzés, de azért én hozzá tennék egy pár megjegyzést.
- Csak azért nem szokták az USB-s kütyüket berakni a gépekbe, hogy villogjanak vele. A Rambo is megjegyezte, hogy jelentősen elterjedt, így már nem státusszimbólum, hanem igen is munkaeszköz. Őszintén ki nem volt már úgy, hogy hazavittem a munkát, ha csak egy doksi, is volt.
- Egy vírusirtó programnak kutya kötelessége megfogni a terjedését, mint ahogy a NOD32 is teszi, és teszi más komoly vírusirtó program is. Kötelező megfognia a káros folyamat indulásakor, és a fájlt is kötelező letörölni, persze ha jól van

beállítva.
- Azt nem tartom informatikusnak, aki nem tudja kikapcsolni, valamilyen eljárással az automatikus indulást. Attól, hogy valaki informatikus, nem kötelező jól programozni is, de ez fordítva is igaz. Én mondjuk a policy szerkesztésével szoktam kikapcsolni.
- A fertőzött média fájlok esetén pedig én is egy klasszikust fogok idézni. Kodály Zoltán: „Csak tiszta forrásból”. Abból, hogy mi a tiszta forrás, azt mindenki döntse el maga! :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.09.11. 15:12:00

Szia Gery!
Itt a féreg leírása, ebben benne vannak a Registry kulcsok is:
www.eset.hu/virus/hakaglan-g
Gyógyításhoz itt van egy lehetséges segédeszköz:
Tweaknow PowerPack
www.tweaknow.com/products.html
De a supportos srácok már várják a jelentkezésedet és részletesen segítenek, ehhez írj a support KUKAC sicontact PONT hu címre.

Obama szexkalandjai

2008.09.11. 17:25 | Csizmazia István [Rambo] | 1 komment

Címkék: spam malware átverés obama trójai

Semmi sem állandó, kivéve a változást. Erre az axiómára máris rábólinthatunk, megfejelve azzal, hogy nem lehet olyan lehetetlenséget kitalálni, amire aztán mégis **ne kattintanának bőszen a túl kíváncsi megfertőzhető számítógéptulajdonosok**.

Michael Jackson és ET közös gyereket szeretne! Hát persze! Ki tette a nyomravezető lószőrt a bárszekrénybe? A jó moszkvai nénikéd! Megette saját lábujját a hűtőszekrénybe zárt csecsemő! Arghhh! Barack Obama szex videója ukrán lányokkal! **A beteges fantáziájú spammelőknek semmi sem szent**, nincs az a blődség, amiben ha fantáziát látnak, **fel ne használnák a kártevők, kémprogramok terjesztésénél.**

Most Obama sex video!!! címmel jár körbe egy levél, nem is kell mondanunk hogy a melléklet még csak véletlenül sem az a videofilm, bár elindul egy felnőtteknek szánt, szemlátomást házi készítésű anyag, annak **semmi köze a szenátorhoz**. Persze közben meg jól **feltelepül egy számítógépes trójai**. Az ukrán lánykákkal folytatott aktus sztori persze **emellett lehet még valami: szándékos lejáratás, hiteltelenítés** (ott mint látjuk, nem elég az, hogy az illető tagadja, aztán mégis emeli a gáz árát ;-) **A legvalószínűbb talán a két ok együtt: kártevők terjesztése (megbízó fizet) és lejárató kampány (másik megbízó is fizet)**, two in one, csak megmosom a hajam, és már indulok is.

Megírhatjuk mi ezerszer is a cikkeinkben, blogjainkban, hogy tegnap, ma mi volt éppen az aktuális álhír, ha ebből rövidlátóan mindig csak az aznapi témát raktározzák el az emberek a fejükben, a módszer általános felismerése helyett. Azt kellene már végre megtanulni, hogy **mindenki meglássa ezekben a csalit, ráérezzen, hogy: "Hohó, itten engem hülyének akarnak nézni, hát ezt nekik!"** és akkor talán kevesebben esnének áldozatul saját butaságuknak és kíváncsiságuknak.

Nagy Feróval szólva: **"Annyi mindent megettem, de van amit a gyomrom nem vesz be, bocsánat, elnézést"**. Már türelmetlenül várom a napot, mikor a többség már így gondolkodik!

· 1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/658829

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.11. 17:37:40

Antivírus blog - Obama szex kalandjaiNem lehet olyan lehetetlenséget kitalálni, amire aztán mégis ne kattintanának bőszen a túl kíváncsi megfertőzhető [...]

Kommentek:

nade 2008.09.11. 21:10:12

:)
És az EMO for Obama megvolt már nektek?
napielet.hu/a_te_napod/post/3366/emo_for_obama

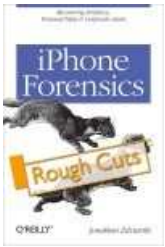
Még csak telepíteni sem kell...

2008.09.12. 16:30 | Csizmazia István [Rambo] | 17 komment

Címkék: apple iphone no screenshot comment titokban zdziarski

... a **kémprogramot az iPhonera, ott van az magától** - állítja egy hacker, **aki Jonathan Zdziarskira hivatkozik.** Ő annak a könyvnek a szerzője, amely "iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets" címmel látott napvilágot.

Az O'Reilly gondozásában megjelent, és nagyjából Törvényszéki Iphone nyomozók: Hogyan állítsunk helyre bizonyítékokat, személyes adatokat és cégvagyont munkacímű kötetben sok érdekeset találhatnak a téma iránt érdeklődök.



Többek közt a **megfigyelései szerint a készülék rendszeresen képernyőmentéseket készít a Home gomb megnyomásakor a felhasználó minden ténykedéséről** cachelési okokból - igaz ezeket aztán később állítólag törli is. Mindenesetre a dolog több mint érdekes, hiszen itt **nem a Home + Kikapcsoló gomb kombinációval elérhető szándékos Screenshot funkcióról van szó**, hanem titokban készülő képernyőmentésekről, erről a jelenségről a tegnapi webcastjában is beszámolt. Reménykedik, hogy az Apple hamarosan felszámolja ezt a privát adataink kezelésével kapcsolatos rést, bár azt is hozzáteszi, hogy **a nyomozóhatóságoknak meg remekül kapóra jön ez a lehetőség**.

Lehet, hogy később vitás esetekben a beépített érzékelőkön kívül ezeket a visszaállított felvételeket is megnézik majd a szervízben, amikor állást kell foglalni a meghibásodással kapcsolatban, hogy garanciális problémáról van-e szó, vagy a felhasználó a felelős? **Korábban is felmerült már kétely** a telefonnal kapcsolatban, akkor azt gyanították a szakértők, hogy továbbítja a látogatott weboldalak, e-mail üzenetek, hívások adatait az Apple szervereire.

Zdziarski neve egyébként onnan lehet ismerős, hogy szintén az ő nevéhez fűződik a **nemrég bemutatott jelszóval védett iPhone feltörése 3 másodperc alatt, vészhívás plusz kétszer Home gomb** című módszer is, ahol aztán az Apple elismerte, valóban működik a dolog, létezik a hiba.

Mindenesetre akinek feltört, jailbreakelt készüléke van, ellenőrizhetné csak úgy kíváncsiságból ezeket a screenshotos dolgokat, illetve az Apple részéről is érdekes lehetne, ha kapnánk egyszer valamiféle hivatalos állásfoglalást.

Bár ez utóbbi ritka madár, a Safari böngésző szőnyegbombázós hibájánál éppúgy mély hallgatásba burkolództak, mint a mostani iTunes 8 és a Vista összeveszésével kapcsolatban: **egyikhez sem fűztek kommentárt**. De hasonló eset volt, amikor a telefonra töltött applikációk távolról való törlési lehetőségét fedezték fel, ott is **eleinte csak no comment volt a reakció**, aztán csak jó sokára ismerték be.

Ide a blogba viszon várjuk a kommenteket pro és kontra, jó lenne ez ügyben tisztán látni.

· 1 trackback

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/660466

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.12. 16:50:16

Antivírus blog - Még csak telepíteni sem kell..... a kémprogramot az iPhonera, ott van az magától - állítja egy hacker, aki Jonathan Zdziarskira hivatkozik.

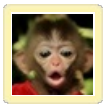
Kommentek:

Daniel W. Mcload 2008.09.12. 19:37:21

Egy szó: hype.
Ha van egy sikeres termék, állítsunk róla bármit, azt jó sok pénzért el tudjuk adni, legyen igaz vagy sem.
Attól, hogy vki megtalált egy hibát egy szoftverben, még semmi nem bizonyítja, hogy összeesküvés elméleteket tud bizonyítani.

Az Élő Legenda (törölt) 2008.09.12. 21:03:53

Azért a marketinghez ért az Apple. Képzeljük el, ha ezeknek csak a fele derülne ki MS szoftverekről. Micsoda felháborodás lenne. Itt meg, sorban állnak Apple cuccokért a bolt előtt.



galicius 2008.09.12. 23:12:22

Azért azt nem kellene elfelejteni,hogy ez a bizonyos kémprogram nem csak az iphonnál működik.Illetve nem is egészen így van.Ugyanis központon keresztül bármelyik telefon lehallgatható.Az,hogy kifejezetten az iphone küld-e az apple szervereire adatokat,nem bizonyított.Mindenesetre egy kis odafigyeléssel kideríthető valamilyen szinten.Előbb-utóbb úgyis kiderül az igazság.

K□rcsány Ferenc · http:□szanalmas.hu/ 2008.09.13. 00:23:56

Az agymosott Macbuziknak mindegy, olyanok mint a Jehova Tanúi.

atleta.hu · http://www.atleta.hu 2008.09.13. 00:50:21

Na ne mar, ez azert viccnek kicsit durva. De dilettantizmusnak is. Az a 'kemkedes', hogy egy program cache-el valamit a sajat eszkozodon (nem szakertok kedveert: sok munkaval osszeallitott adatot egyben eltarol)? Nem, ez nem kemkedes, hanem ahogy irod cache-eles. Hogy ezt 'el lehet lopni'? Hat istenem, _minden_ adatodat el lehet lopni a telefonodrol, ha fizikailag hozzafer valaki - ha csak nincs minden megfeleloen titkositva. De hypePhone-rol leven szo nincsen, hiszen nyilvan nincs benne ilyen funkcio (a konkurens termekekben sincs, ezen kivul nem olyan latavnyos, mint a kinetic scrolling), viszont az SDK-t ismerve nem is lehet ilyesmit fejleszteni ra (Symbianra biztosan lehet, windows mobilera meg szinte biztosan).

De ez mas kerdes. Ahogy Daniel irta: hype. iPhone cimkevel ma mindent el lehet adni, akkor is, ha okorseg. (Lasd meg a lelkesen nyilatkozgato nehany tudost aki szerint nincs glob felmelegedes: ezzel meg ki tud tunni, valtoztatni ugysem tud, erdemi eredmenyt meg ugyszinten nehez lerakni.)

Csak azt nem ertem, hogy te, kedves blogiro minek egeted ezzel magad. Bar eddig minden - az index folapra kilinkelt - mob temad igy sult el ;). Bocs.

ac3^BB 2008.09.13. 01:01:20

fikablog ez is

Dextro (törölt) 2008.09.13. 08:54:27

Atleta,

A honlapotok második sorában a töblet az = többlet.Erre is odafigyelhetnél fikázás közben.(tovább nem is olvastam)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.13. 11:16:42

Szia Élő Legenda!
Lassan már mindenről derül ki valami: MS, Apple, Google (Chrome licenc), remélem végül a Linuxokkal nem fogunk törököt ;-)
Mivel mindenki gyűjti az adatokat rólunk, lassan nem marad mit választani, hogy mostan kérem mi belgák hova is álljunk...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.13. 11:29:09

Szia Atleta!

Először is nem én linkelem a blogot az Index címlapra, néha ajánlom, többször nem, hanem ők teszik ki oda, amit érdekesnek találnak ŐK.

Szerintem nem égetem magam, mivel én beidéztem egy olyan véleményt, amit érdekesnek találtam, másrészt olyannak, amiről jó, ha mindenki tud.

Harmadszor egyelőre még valóban fizikai kontaktus kell az adatlopáshoz, de mi lesz, ha később majd egy exploit csinálja ugyanezt? Miről veszed majd észre? Lesz majd tűzfal a szifonon? És ha lesz is, hogyan kezeli majd ezt egy átlagember?

A globális felmelegedésről egyébként nem tudom mit is gondoljak, a Balcsin töltött egy hét szakadó esőben és 17 fokban nem győzött meg ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.13. 11:35:20

@ Ac3^BB!
Ez nem fikázás, hanem tükröt tartok, ez a világ.

Szerintem egy végiggondolást megér, egyébként nekem is van iPhoneom, hidd el, nem a rosszindulat vagy az irígység beszél belőlem.

Ez a biztonsági szakma erről szól: mi van ha nem úgy használom, ahogy azt eredetileg a gyártók kitaláltak? Mire lenne ez a dolog még másra is kihasználható? Mi lenne ha megbuherálnám ezt és ezt, mi történne? Amíg van aki ilyen kérdéseket feltesz, addig te, én, a szüleid, ismerőseid, az én ismerőseim, akik NEM MIND geekek, bajban lesznek, áldozatok lesznek, hacsak valaki mindig nem figyelmezteti őket, nem írja meg, nem demonstrálja a szándékos vagy véletlen sebezhetőségeket.

atleta.hu · http://www.atleta.hu 2008.09.13. 23:12:31

Dextro: > A honlapotok második sorában a töblet az = többlet.
> Erre is odafigyelhetnél fikázás közben.(tovább nem is olvastam)

Ez mondjuk elegge a legalja szinvonal. Eloszor is, a ceges honlapon nem fikaztunk. Ez meg itt a maganvelemenyem, tehat nem a fikazas kozben irtam el azt az egy szot. Amit irsz, az nem erv. Akar az is lehetne, hogy botranyosan szar a helyesirasom, ettol meg lehet igazam, es erthetek a szakmamhoz. A ket dolog tok fuggetlen egymastol. Ennek ellenere te azt olvasol es addig, amit es ameddig akarsz. Meg szerencse, hogy nem magyar nyelv oktatas, szakforditast vagy epp korrekturazas a cegunk profilja.

A (szakmai) maganvelemenyem meg hadd mondjam mar el ott, ahol akarom es ahol lehet. Persze tudom sokakat zavar az, hogy az internet egy ilyen visszapofazos medium, de ez nagyban hozzajarul ahhoz, hogy konnyebb rola hitelesen tajekozodni.

De azert kosz, hogy szoltal, bar nem ez a legnagyobb problema a weblapunkkal - ha tovabb olvasod, biztos eszrevetted volna, hogy erosen 0.0.1-es valtozatban all meg sajnos a dolog tartalmilag is :).

atleta.hu · http://www.atleta.hu 2008.09.14. 13:23:48

Csizmazia István: Valaszoltam szep hosszan, erre elszallt a sunyiba. Iszonyat jo, hogy - bocs a fikazasert - ennyi ido alatt is keptelenek megcsinalni normalisan a blog.hu mindennel osszekombinalt belepteto rendszeret. Majd he lesz erom, akkor ujra leirom.

atleta.hu · http://www.atleta.hu 2008.09.23. 00:09:49

Na, sok jelentosege nincs, de roviden a kovetkezoket probaltam elmondani a multkor: eloszor is feluletesen fogalmaztam, a fizikai hozzaferesbe beleertettem azt is, ha kodot kepes valaki futtatni az eszkozodon, barmilyen modon. Leven egyfelhasznalos rendszerrol beszelunk, ez igazabol tenyleg ugyanazt jelenti. Tehat nem kell fizikai kontaktus.

A problema lenyege viszont az,hogy ha valaki kepes kodot futtatni (vagy fizikailag hozzaferni) a zajphonodhoz, akkor a legkisebb problemad lesz az, hogy keszult nehany kepernyomentes az utobbi idoben. Eloszor is nyilvan keves keprol van szo, masodszor jo esellyel nem veszed eszre a kartevot, tehat majdnem lenyegtelen, hogy az eszre nem vett idopont elottre is lat. De ha mar sikerul eszrevetlenul adatokat lopkodni a keszulekedrol, akkor ezek a kepek a legkevesbe erdekesek. Sokkal nagyobb gaz a contact listad, jegyzeteid, naptarod (visszamenoleg is), hivas listad (visszamenoleg is), browser cache (esetlegesen meg elo cookie-kkal), SMS-ek, e-mailek, stb. Mi az, amit csak egy ottfelejtett screenshot formajaban szerezhetne meg egy tamado? A browser cache miatt gyakorlatilag nincs ilyen. Es ez a lenyeg, ettol mubalhe a dolog. Semennyire nem csokkenti a rendszer biztonsagat, sem egy esetleges tamadas eseten nem segiti a tamadot olyan informaciokhoz, amikhez amugy nem ferne hozza.

Csak a hypephone-rol mostanaban nagyon divatos beszelni, es ezert mindenki probal mondani valami okosnak latszot. A paraztatasra meg mindig vevok az emberek. Jobban szeretnek parazni es horror sztorikat meselni, mint gondolkodni.

> Szerintem nem égetem magam,

Bocs, az eros fogalmazasert, csak nehezen megy a simulekony fogalmazas, ha sokadszor olvasok ilyen megalapozatlan allitasokat ;).

> mivel én beidéztem egy olyan véleményt, amit érdekesnek találtam,

De azert szerintem tovabbra is felelos vagy, es mint szakember ha idezel valamit a sajat blogodon, akkor ha nem ertesz egyet, akkor jelezned kell, kritikat kell megfogalmaznod. Ellenkezo esetben ugy ertelmezheto (es szerintem ugy is kell ertelmezni),

hogy az egyezik a te velemenyeddel. Nyilvan nem veletlenul publikalod. Sot, ehhez szakembernek sem kell lenni, de szakemberkent ez meg erosebben elojon.

> másrészt olyannak, amiről jó, ha mindenki tud.

Tehat akkor megis egyezik a velemenyeddel, akkor pedig..? :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.23. 09:55:01

Sok minden van részben igazad, köszi a kommentet. Ha időm, erőm engedi, még lehet hogy az emlegetett könyvet is meg fogom venni.

De ha jó életszerű példát akarsz a screenshot mentésre, íme tessék. Egy rendszergazda vagy egy átlagember a tirkos jelszavait, bankkártya pinkódjait valamilyen titkosított formában (Lockbox, etc.) a szifonon tárolja. A kinyitott és olvasható állapotról készül pár "cache mentés" és akkor az ugye ez már nem olyan frankó, mintha csak a Tetris highscore táblája van lefényképezve.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.29. 12:57:17

Még egy apsektus, ez most nem kémpprogram szempontból.
Ha el akarod adni a használt készüléket, és nem lehetsz benne biztos, hány sceencapture készült, hol vannak ezek, nem találja-e meg majd az új gazdi, amint éppen netbankolsz, stb.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.30. 11:47:48

Íme egy lehetséges jó megoldás Buherátortól:
buhera.blog.hu/2008/09/23/aki_kivancsi_hamar_dev_null

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.15. 09:58:13

Használt mobil rulez:
www.privatbankar.hu/html/techtud/it.php?kommentar=26223

Nekem nyolc

2008.09.15. 17:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: apple hiba itunes frissítés vista iphone

A mostani 2.1-es iPhone firmware frissítés mellé kaptuk az **iTunes 8.0 programváltozatot** is, amely **néhány Vista felhasználó életét kékhalállal** keserítette meg.

Az usbaapl.sys és az usbaapl64.sys meghajtó programok okozta problémákra **egy újonnan kiadott iTunes adja a gyógyírt**, ezt az egyszerűség kedvéért úgyanúgy 8.0-snak jelölik.

Az iPhone egyébként sok hasznos funkciót hozott, megjelent a magyar dátumformátum, magyarul beszél a GPS, végre megjött a hosszú ő és ű betű a kalapos ékezetes helyett, jobb akkus és 3G teljesítmény, és **a háromgombos jelszóval lezárt nyitási trükk is a múltté lett.**

Amin kicsit mulattam, az az volt, hogy a PCAdvisor cikkben reklamáltak, hogy miért nem egy újabb iTunes változat készült. Jó, értem én, abban is van logika, hogy két ugyanolyan verziószámú csomag nem jó, ha tartalmában mégis különbözik. Arra viszont nem gondoltak, hogy akkor a Help /Check for Updates ezt a frissítést érzékelné, és nem csak a pár ezer problémás Vista felhasználó, hanem **minden egy - sok millió - felhasználónak feleslegesen újra le kellene töltenie** pl. egy 8.01-es 75 MB méretű csomagot, ami ugye azért mégsem len szerencsés.

· 1 trackback

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/664537

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.15. 17:48:27

Antivírus blog - Nekem nyolcA mostani 2.1-es iPhone firmware frissítés mellé kaptuk az iTunes 8.0 programváltozatot is, amely néhány Vista felhasználó [...]

Kommentek:

Nincsenek hozzászólások.

Mega Mac javítófolt

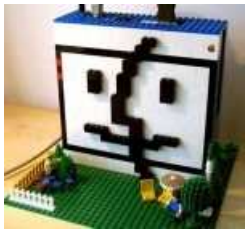
2008.09.16. 11:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: apple patch macintosh

34 különféle biztonsági hiba javítása oldódik meg a legfrissebb patch letöltésével, ezek között egyszerű warning figyelmeztetéstől egészen a távoli kódvégrehajtását lehetővé tevő komoly sérülékenység is volt.

A teljes listában több puffertúlcsordulási, memória mérgezési és egyéb hiba is volt. A **rendszeres javítások letöltése itt is fontos**, hiszen különféle sebezhetőségek szűnnek meg így a rendszerben. Nem szokatlan az ilyen nagy méretű (157 MB) javítócsomagok megjelenése, szinte már szokásosnak számít, hogy egyszerre 20-30-40 probléma együttes megoldását lehet letölteni.

Annak köszönhetően, hogy **a Mac gépek elterjedtsége egyre emelkedik**, az ellene irányuló kártékony trójai és egyéb kódok támadása is várhatóan emelkedni fog a jövőben.



Emiatt itt is érdemes a frissítések automatikus fogadását, illetve azok futtatását miharabb elvégezni.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/665711

Kommentek:

Nincsenek hozzászólások.

Egy éves az antivirus.blog

2008.09.17. 14:23 | Csizmazia István [Rambo] | 5 komment

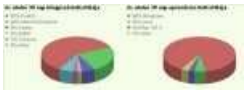
Címkék: blog egy antivirus évesek lettünk

Az idő relatív fogalom, ha kedvesünkkel sétálunk a tengerparton kéz a kézben, szinte repül, míg a fogorvosi rendelőben csiga lassúsággal telnek a másodpercek, ólomlábakon jár. Nem tudom számít-e, de **ez az egy év itt is igen röpke volt ;-)**

Legolvasottabb, best of ever in the first year cikkeink az alábbiak voltak, ötezer feletti látogatószámmal :

Deface az antivírus oldalon
Lehallgatják-e a Skype-ot?
Ha annak idején a szüleid inkább moziba mennek...
Webkamerás kukkolók

És íme, ez az utolsó 30 nap böngészőstatisztikája, jól látszik, bár vannak elvétve Chrome felhasználók is, **a Firefox durván lenyomta a többieket** (én örülök ennek), bár az Operának is erősen szurkolok. Ami viszont az alternatív oprendszereket illeti, sajna itt **még erős Win uralom van 89 százalékkal** - hja kérem, **kell valami közeg, amin a kártevők futnak ;-)**



Jövő ilyenkor tíz százalék feletti Macintosh és 8% körüli Linux adatokat szeretnék majd itt látni :-) Reméljük, a következő évben **még több "átlagfelhasználót" sikerül idecsábítanunk**, mindenesetre témahiányban biztosan nem fogunk szenvedni. Pedig már **jó előre megírtam az utolsónak szánt blogbejegyzést is**, ez egyelőre a fiók aljába lesz süllyesztve: *"Megszűntek a vírusok, férgek, kémprogramok és kártevők, senki nincs veszélyben, a biztonsági szakma képviselői pedig világszerte munkanélkül maradtak, ők a jövőben képeslapok és díszműáruk terjesztésével foglalkoznak majd"*.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/666100

Kommentek:

Algernon 2008.09.17. 16:52:11

Boldog Szülinapot és csak így tovább! :)

□am. □oe · http://www.matchboxmemories.hu 2008.09.17. 18:34:13

Boldog szülinapot!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.17. 20:06:35

Hello Algernon és Sam.Joe!
Köszi szépen :-)

Arikel · http://hogyanfu.blog.hu/ 2008.09.18. 10:29:25

Gratula és boldog szülinapot! :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.18. 15:52:26

Köszi szépen Arikel!
És mindenkinek még, akik emailben gratuláltak :-)

Kényelem VS biztonság

2008.09.17. 13:55 | Csizmazia István [Rambo] | 1 komment

Címkék: biztonság hamis kényelem antivirus

E két ősi kategória örök, **antagonisztikus ellentétben áll egymással**, de komoly **bajok jobbára akkor vannak, ha valahol a kényelem túlságosan nagy teret nyer**, és kiplakátolják, vagy a retinájukba tetováltatják a "Lustaság fél egészség" szlogent.

A "felhasználó" ahol tud, lazít, könnyít, postit-re jelszót irkál, idegennek telefonban megad, stb. Egy friss felmérés szerint folyamatosan **emelkednek a begépelt jelszót kiváltó ujjlenyomat olvasóval felszerelt** számítógépek eladása. Mind az asztali, mind a noteszgépek között nagy népszerűségnek örvendenek az ilyen darabok, a május és július közti időszakban kb. 90 százalékban emelkedett ezek értékesítési aránya.

A biztonsági program kiválasztásánál **utánanézni, rákeresni, nyomozni, olvasni, ismerősnél rákérdezni persze fáradtságosabb**, mint a készségesen ablakban felajánlkozó hamis, kártevőket terjesztő WinAntivirus 2008 ajánlatát elfogadni, még ha a kattintónak fogalma sincs mi ez, de "biztos jó". Ebből **folyamatosan jönnek az egyre újabb csali változatok** Windows AntiVirus, AntiVirus Lab 2009 neveken, sőt újabban a kémprogramellenes harc jegyében már Antispyware Pro XP és WinAntispyware 2008 néven is előbukkant.

Muszáj lenne az **átlagfelhasználónak is valamennyire képbe kerülnie**, és az alapvető óvatosságot, jártasságot elsajátítania, jó lenne, ha vágyna a nagyobb biztonságra - akár a kényelem rovására - ehhez pedig a legjobb útravaló a blog tanulságos jelmondata is lehetne egyben: "**A gravitáció nemismerete nem mentesít a zuhanás alól**".

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/667350

Kommentek:

gothmog 2008.10.21. 21:33:31

Na ja, nézd meg az internet szolgáltatók hirdetéseit. "Csak bedugod, és már szörfözhetsz is" Az ilyenek gépeiből lesz öt percen belül zombi. Senki nem szól a veszélyekről, minek is...
Emiatt a win anti-sokfélenevű aljasság miatt az elmúlt hetekben kb. tíz ilyen júzer only típusú ismerősöm gépét kellett újratelepíteni. (eleinte volt néhány hiábavaló irtási próbálkozásom)
Az én megoldásom xp install integrált sp3-al (nlite-al készül), zone alarm free, avg free, +spybot. (van benne egy ilyen immunize funkció, nem tudom, mennyit ér, de ártani nem árt). Böngészésre Firefox. Levelezésre Thunderbird. -és ezek után dugjuk rá a netre a gépet. Majd update avg, windows. Mellétűzve egy kis magyarázat, hogy mi miért jó, és miért fontos. Zonealarmot kicsit magyarázni kell. Ez eddig még egy fillér plusz pénzbe nem kerül. De mennyivel jobb így mintha meztelen seggel, meg ie6-al netezne a kezdő júzer.

Fertőzött pingvin leselkedik a Windowsra

2008.09.18. 14:04 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: játék iphone panic penguin trojan fertőzött

Ha épp nem sikerül fogást találni az iPhonon (egyelőre), akkor hajrá **előre a bevált recept szerint: a Windowsos gépek** a jól bevált célpont. Az Apple új készülékének népszerűségét mindenesetre sokféleképpen ki lehet használni.

Réges régen, amikor a hülyét még pontos jé-vel írták, voltak a boldog békeidők (C64, Spectrum, BitLet Karácsony, Csokonai, stb.) ahol a vasfüggöny mögött a nyugati utazás is csak a háromévenkénti álom volt 50 dollárral, és utána a maradék pénz visszaváltásával működött. Ha egy szegény átlagmagyar látott egy jó programot a barátjánál, annak rendje és módja szerint **átmásolta magának**, ez volt a BBS: Barátom Barátjának a Szoftvere :-) Legális valuta hiányában sok más lehetősége amúgy sem lett volna.

Aztán kezdődött a PC világ, lehullt a vasfüggöny, utazhattunk, **megtanultuk hogy a szoftvert akár meg is lehet venni**, sőt voltak akik erre rendszeres időközönként különféle furmányos módszerekkel (pl. bilincses plakát) még figyelmeztettek is bennünket. Belekerültek olyan kitételek a Szoftvergazdálkodási útmutatóba, hogy azért (is) **használjunk legális szoftvert, mert "különben vírusfertőzésnek tesszük ki magunkat" :-)**

Azóta sok egyes és nulla lefolyt már az adatkábeleken, és az élet **sok olyan esetet produkált, ahol magán a gyári vadonatúj merevlemezen, USB kulcson, a szoftver eredeti adathordozóján lapult a kártevő**, sőt a mai internetes világban full legális szoftverek birtokában **egy weblap meglátogatásával is** megfertőződhet a gépünk. Most viszont úgy tűnik, a warez egyre gyakrabban adhat táptalajt a kártevő terjesztőknek, **most éppen egy iPhone játék járt így.**

Ha az iPhone programok választékát nézzük, egy nem feltört, és nem jailbreakelt telefon esetében, **akkor csak és kizárólag az iTuneson keresztül töltögethetünk át** dolgokat. Legyen az akár saját fotó, zene - **a Bluetooth szándékos kiherélésével: értsd semmi adatkapcsolat, csak és kizárólag fejlhallgatóra használható** - a többi telefonon megszokott küldözgetés itt sajnos nem működik, marad a központi Apple programmal való letöltés. Szerencsére a csengőhang, kép, video, zene adott saját könyvtárak importálásával feltölthető, de ez már a programok (játékok, alkalmazások) esetében nem működik. Még kivehető memória kártya sincs, amire felmásolva úgy látszana, mintha progit töltöttünk/vásároltunk volna magunknak (ez is szépen ment a régi Symbian alatt).

Az iTunes Store szoftverek esetén ugyan elvileg nyújt egyfajta védettséget is (hasonlóan ellenőrzött és jóváhagyott programok vannak fent, mint a Symbiannál), viszont egy kevés kivételtől (free applications) eltekintve **minden pénzbe kerül**. Jah igen, és a Nagy Testvér bármikor bármit visszahívhat. *(hogy ez a parlamenti képviselőinkre miért nem működik ugyanígy, az korunk egy másik nagy rejtélye, ne is feszegessük ;-)* Vannak persze módszerek, amik megkerülik ezt, segítségükkel beleláthatunk az iPhone fájrendszerébe, feltölthetünk warez játékokat. Egy ilyen feltölthető játék, a **Penguin Panic került elő most egy olyan levélmellékletben szereplő .ZIP állományban, amely egy trójait hordozott magában**, rákattintva pedig Windows alatt megfertőzte a számítógépet. A spam levelek "virtual iPhone games", "take a break" vagy "virtual iPhone toys" tárgysorral érkeztek. Fontos tudni, hogy **sem az iPhone, sem a MacIntosh gép nem fertőződik** meg tőle, a tettesek inkább jól feltételezték, hogy az emberek többsége úgyis Win mellett ül, megéri nekik a trükk. A pingvines alkalmazás egyébként nem is került fel az iTunes hivatalos alkalmazásai közé.

Érdemes tehát óvakodni, ha ilyen **feltört játékokat akarnak ránktukmálni, akár spam emailben, akár weblapon** találkozunk vele. Szinte biztos, hogy a trükköt más kártevőkkel feltöltve a jövőben is fel fogják majd használni. Addig is mindenki használjon szabad szoftvert vagy legális szoftvert, vagy ha mégsem, akkor viszont kérdezze meg orvosát gyógyszerészét, és **csak megbízható hacker programjait töltse le ;-)**

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/669226

Kommentek:

Nincsenek hozzászólások.

Mit tanulhatunk a Sarah Palin esetből?

2008.09.19. 18:06 | Csizmazia István [Rambo] | 5 komment

Címkék: jelszó kérdés biztonsági feltörés palin sarah mailbox

Ha valaki semmilyen irányban (demokrata vagy republikánus) sincs elkötelezve, még akkor is találgathat, kinek a malmára hajtja a vizet egy ilyen postafiók feltörési eset, és mik a tanulságai - mert hogy vannak ilyenek.

Néhányan eleinte talán az email szolgáltatót hibáztatták, de az is teljesen elképzelhető volt, hogy a Yahoo teljességgel ártatlan a dologban. A **republikánus McCain hívek nyilván lejáratókampánynak fogták fel**, és már jelentek is meg olyan találgatások, miszerint egy demokrata párti képviselő fia lenne a lehetséges elkövető. A módszer nem feltörés, nem jelszó találgatás volt, **hanem új jelszó igénylése**. A születési hely és idő megszerzése nem okozott gondot, a **titkos ellenőrző kérdés pedig az volt, hol ismerkedtek meg a férjével**. A dolog érdekessége, hogy erről is beszélt már nyilvánosság előtt - és ez egy középiskola neve volt. **Innentől már meg is volt oldva a dolog.**

A Sophos érdekes párhuzamot vont - és nagy valószínűséggel igaza is van - a korábbi Paris Hilton PDA telefonjával és feltört mailboxával kapcsolatosan. Ott az ismert celeb (brrr, de szörnyű egy szó ez) kedvenc állatának neve volt a jelszó emlékeztető kérdés. Az ismert és kevésbbé ismert embereknek komolyan el kellene gondolkodniuk, **érdemes-e olyan adattal védeni bármit is, amit a búlvárlapok lapok hetente megírnak**, vagy valaki önként kiplakátolja az IWIW-es lapjára. Ez kb. olyan szimpla akadály, mintha Kiszel Tünde jelszava "Donatella" lenne.

Az hogy **milyen jelszót érdemes** választani, már többször is megtárgyaltuk. Vagy ne válasszuk ölebeink, családtagjaink nevét jelszónak, vagy **hívjuk kutyánkat Blöki helyett egyszerűen csak "fFgha/.-(786GGjsoL"-nak ;-)** Ami még feltétlen kiegészítésre szorul, az az **ellenőrző biztonsági kérdés** témája.

Sokszor nincs sok lehetőségünk, csak a rögzített standard kérdések közül tudunk választani: your pet, your first teacher, blabla, etc. De ilyenkor **sem kötelező ám az adott kérdésre vonatkozó választ adni!**

Persze **sok helyen van lehetőség saját kérdést írni** - ezt érdemes is kihasználni - ezekben is alkalmazni lehet a fenti okosságot, ez pedig jócskán **csökkentheti a találgatási lehetőségeket**. Hogy hívják a kedvenc tanárodat? Csütörtök - hangzik a válasz, és ez egy jó válasz. Melyik kórházban születtél? Lekváros palacsinta fahéjjal. **Jó étvágyat hozzá!**

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal

- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/671591

Kommentek:

buherator · http://buhera.blog.hu 2008.09.19. 19:06:42

Már csak azt kell megjegyezni, hogy milyen kérdésre várja a rendszer _valójában_ a választ :)

Itt van még egy érdekes cikk a témában: www.infosecblog.org/2008/08/a-different-approach-to-passwo.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.19. 20:49:08

Szia Buherátor!
Van is egy idevágó Murphy törvény: "Ha elraktároztál valamit a számítógép memóriájában, hogy hova is tetted pontosan, azt raktározd el a saját memóriádban!"
Egyébként ez a volt barátnő sok személyes info birtokában jelszó resetet kér hehe ez tényleg jó :-)
Viszlát holnap a Hacktivityn!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.08. 22:58:01

Na itt a hír a végkifejletről, börtön az e-mail fiók feltöréséért:
itmania.hu/tart/cikk/e/0/25532/1/informatika/Borton_Palin_email_fiokjanak_feltoreseert

R.Gyuri 2010.04.01. 17:21:17

Mindig utáltam ezeket a hülye kérdéseket, sőt biztonsági lyuknak tartottam, lám igazam is volt, baromi okos vagyok.

Főleg azt utálom, hogy többnyire nem lehet ignorálni sem, kvázi köteleznek erre a baromságra. Ilyenkor mérgemben beírom:

Kérdés: lkgjjios ő wtpoe őm ewoqwű őpaw
ősldddáhjfu opaeésiofn,jhj

Válasz: jkécgh blékasd gzgljkmosd h849 76ldbjnvág 87ewug

Ezt találd ki barom...

titan 2010.05.06. 14:37:32

Vazzeee,, te tudod Kiszel Tünde jelszavát? ;P

Hacktivity első nap

2008.09.20. 20:38 | Csizmazia István [Rambo] | 1 komment

Címkék: hacktivity hacker

Van-e magyar hacker társadalom? Különbözik-e és miben a magyar hackerek élete, lehetőségei a külföldi kollégákhoz képest? Jó ember-e a hacker? Mindenre választ adunk a folytatásban.

Úgy látom, a szervezők most **jó érzékkel emelték a gyakorlati bemutatók, workshopok számát** a klasszikus elméleti előadások ellenében, és ez határozottan jót tett a rendezvénynek. Ide **mindenki azért jön, hogy olyasmit láthasson, amit máshol nem** láthat. Azt hiszem, ez az óhaj idén is teljesülhet.

Több kifejezetten **fiatal előadó tartott színvonalas, gyakorlati bemutatót**, és bár valamennyiükön látszott, hogy többé-kevésbbé izgultak, de a lámpaláz okozta előadásbeli gyakorlatlanságuk ellenére **érződött, élvezték a dolgot, szeretik csinálni és magas szinten értenek** ahhoz, amit bemutattak.

Pánczél Zoltán a webservicek hackeléséről, Bucsay Balázs az XSS férgekről, Buherátor a buherator.blog gazdája pedig az SQL injection témakörről mondott el sok érdekeset és **mutatott be különféle trükköket a gyakorlatban is**.

Szakály Tamás a videókártyán történő hashtörés rejtelmeit ismertette, és saját shady crack programjának működését mutatta be, míg Spala Ferenc az Oracle hacking csinját-bínját demonstrálta igen szemléletesen, példákon és bemutatókon keresztül kellemes fanyar humorral átszőve.

Igen jópofa előadást kerekített Sütő János is, ahol a statisztikai spamszűrőkről beszélt, és **konkrét, valós leveleken tesztelve** ismertette a kéretlen levélszemét ellen vívott küzdelem módszerét, trükkjeit, a kiértékelő algoritmus részletes működését.

Minden előadásra így sem sikerült eljutnom, hiszen ezek párhuzamosan zajlottak a kis- és a nagyteremben. **A közönség most is vegyes volt**, a hivatásos biztonsági szakemberektől kezdve a nyilvánosságra nem törekvő, valódi hacker szemléletű emberkéken át az egyszerű kíváncsiskódig minden réteg képviseltette magát.

Mindenképpen érdemes megemlíteni, amit Krasznay Csaba a záró kerekasztal beszélgetésnél is kihangsúlyozott, és nagyon egyetértek a szavaival, hogy **a hackerekre és a hackertársadalomra mint pozitív értékre, kíváncsiság hajtotta újítókra, nyílt eszű kísérletezőkre kell gondoljunk** és fontos, hogy semiképpen ne azonosítsuk őket kártevő terjesztő, pénzt zsákmányoló bűnözőkkel, crackerekkel. Sok esetben éppen a hackerek kíváncsisága óvja meg az átlagember privátszféráját egyes cégek tisztességtelen és rejtett módszerei ellen.

A szögletes alakú kerekasztal mellett Szedlák Ádám moderátor mellett Buherátor, Andrei és Krasznay Csaba ültek, és a közönség is aktívan bekapcsolódott a beszélgetésbe. Szóba került az is, **mennyiben más, vagy szűkebb a mozgástere egy magyar hackernek**. Számukat pontosan nem lehet tudni, de több tucat valóban kiemelkedő képességű hacker is tevékenykedik nálunk, igaz különböző területeken, van aki éppen a Linux kernel fejlesztésében vesz részt, de persze "biztonsági tesztelő" is akad jócskán. Igazából hiányzik a szakmai megbecsülés, a sérülékenységekre való figyelmeztetést sokan ellenségesen fogadják, illetve ezek súlyát tudatlanságuk miatt alábecsülik. Szó esett arról is, hogy sok cég nem bízik az egyébként kiváló magyar biztonsági szakemberekben, és inkább külföldről hívnak etikus hackereket rendszereik teszteléséhez. Buherátor szerint **szakmailag elvileg semmi akadálya nem lenne**, hogy magyar szakemberek Dan Kaminsky DNS sebezhetőséghez hasonlítható sebezhetőségeket fedezzenek fel és tárjanak a nyilvánosság elé, de **az IT szakma és a cégvezetők közömbössége miatt, valamint a kaotikus törvényi megítélés miatt** mindenki inkább a háttérben marad. **Sok multinacionális cég, bank inkább eltitkolja a biztonsági incidenseket**, és lenyeli a károkat - amiket aztán nagy valószínűséggel ránk ügyfelekre hárít tovább, ami **hosszú távon senkinek sem jó**, ebben is jó lenne már előrelépés.

Az **elmulasztott Buhera sörözést szerencsére sikerült helyben bepótolni**, így kétségkívül minden szempontból sikeres nap után vagyunk, illetve a szabadfoglalkozás még ezekben a percekben is zajlik... **Holnap is érdemes jönni**, sőt 14 óra után a belépés már ingyenes lesz.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/673242

Kommentek:

keeroy http://music.blog.hu 2008.09.22. 00:03: 9

Köszi! :)

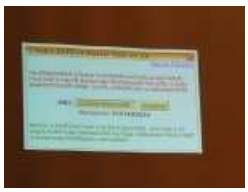
Hacktivity második nap

2008.09.21. 21:20 | Csizmazia István [Rambo] | 8 komment

Címkék: hacktivity hacker

Következzenek a második nap eseményei dióhéjban. Csak ízelítőt tudunk adni, a hangulatot képtelenség így visszaidézni. **Erős nap lett a mai, talán még a tegnapi programoknál is izgalmasabb módszerek, trükkök bukkantak elő** nagyszerű előadóktól. **Törölgethetik a könnyeiket, akik kihagyták**. A jó hír az, hogy lesz jövőre is.

Kissé lefáradtan, de csak összegyűlt a csapat negyed tízre, és elkezdődött a program. Akárcsak tegnap, itt is **sokszor nehéz volt kiválasztani, melyik teremben történik érdekesebb** dolog, de hát nem vagyunk Révész Sándorok, nincs két életünk, muszáj volt egyet kiválasztani. Ezúttal a tegnapi kerekasztal (ami történetesen szögletes volt) egyik résztvevője, **Andrei nyitott egy érdekes social engineering teszt projekttel**. Öt éven át működött egy weboldala, ahol Nokia telefonokat lehetett függetleníteni, ehhez mindössze a IMEI számot és pár adator kellett begépelni, és máris megkapták a látogatók a testreszabott számsort, amit bepötyögve hálózatfüggetlen lett a telefon. A pláne abban volt, hogy a begépelt és önként dalolva megadott adatok (IMEI, telefontípus, szolgáltató neve), a böngészőből lekérdezhető (oprendszer, böngésző, cookie) információkból és az esetlegesen megadott e-mail cím birtokában már **szép adatbázist lehetett építeni az öt év alatt úgy, hogy eközben semmilyen jogszabályt nem sértett**.



Jellemző módon nem csak külföldi, hanem mintegy 800 ezer magyar személyhez köthető kérés is érkezett ez idő alatt, amelyek nem csak magánszemélyektől, hanem esetenként állami hivatalok, minisztériumi internetes környezetből érkeztek. Tanulságos eset és nem tudhatjuk, hol melyik oldal él vissza ezzel **egy olyan korban, ahol például az amerikai állampolgárokat ciageretta, autó és fegyver márkájuk alapján próbálják statisztikai programokkal megjósolni**, ki szavaz majd a demokrata, és ki a republikánus pártra.

Baki Gábort már senkinek nem kell bemutatni, ezúttal egy ritka érdekes demonstrációt tartott, a wifi router sebezhető driverén keresztül és a Metasploit framework segítségével sikerült egy támadást levezényelnie. A három számítógépen párhuzamosan zajló eseményeket inkább a haladó csoportos geekeknek szánta, és ez annyira kifinomult és szellemes volt, hogy végül igen komoly tapssal jutalmazta a nagyérdemű a furmányosan megszerzett local system jogot.

A kisteremben **Szili Dávid beszélt az anonimizáló technikákról**, ahol a névtelen levélküldésről és az anonim böngészésről esett szó az alapoktól a gyakorlati módszerekig, konkrét alkalmazásokig. Szóba került a Tor böngésző, a hasznos anomymous és jap firefox plugin, és **a technika jelenlegi legnagyobb hátránya, az igen jelentős lassúság** is. Jópofaság volt, hogy korábban **egy egyszerű trükkel, a Google Tranlate segítségével, fordítás nélkül (English to English) is anonimizálhattunk**, bár ha azt nézzük, hogy így meg a Google karmaiba hullottak az adataink, nem tudni, jól jártunk-e. A módszer mindenesetre ma már nem működiő képes, bezárták a kiskaput.

Azt el is felejtettem tegnap írni, hogy **minden előadót egy Hacktivity cimkés vörösborral jutalmaztak a szervezők**, így köszönték meg a munkájukat.

Talán szakmailag **a legizgalmasabb előadás következett Major Marcell és Barta Csaba felvezetésében, a fuzzerekről**, vagyis az automatikus sérülékenység detektáló programokról. Meglepő módon ezeknek már közel 20 éves múltjuk van, de a jelentőségük jobbára az utólsó néhány esztendőben nőtt meg, mikor is egy-egy újonnan felfedezett biztonsági rés igen hamar exploit formájában fenyegeti a felhasználókat a javítás elvégzéséig. Az előadók nem csak a technikákat ismertették, hanem **bemutatták saját fejlesztésű Fuzzit és Browser Wave programjaikat**, amelyek igen hatékonynak mutatkoztak, még nulladik napi Safari hibát is sikerült vele detektálni. Talán nem tévedek, ha úgy éreztem, ők aratták a legnagyobb szakmai sikert a közönség körében.

Néhány éve nagy vihart kavartak a mobil kártevők, melyek eleinte inkább csak kísérleti kódok, jópofaságok voltak, de néhányuk már felesleges Bluetooth forgalommal gyors akkulemerítést, kéretlen MMS küldözgetéssel pedig akár anyagi kárt is képesek voltak okozni. A mobil kártevők minden fontos állomását érintve, **konkrét példákkal ismerhettük meg Csiszér Béla előadásából, aki láthatólag nagyon beleásta magát** ebbe a témába. Kiderült, hamarosan ismét szembesülhetünk a 2004 táján tapasztalt kaotikus helyzettel, úgyanis **az új Symbian verzió 2008 júniusi feltörésével ismét lehetőség lesz** tetszőleges, digitálisan nem aláírt programok telepítésére, és ez okozhat majd gondokat.

Egy érdekes könyv is bemutásra került, Dr. Székely Iván társadalmi főinformatikus jelentette be a **"Szabad adatok, védett adatok 2." című kötetet**, amely részben tartalmazza a korábbi előadások témakörét is, és minden érdeklődőnek jó szívvel ajánlják. A mű személyes adatok védelmét megvalósító sajátos informatikai technológiákkal és alkalmazásokkal foglalkozik, amelyek összefoglaló neve Privátszférát Erősítő Technológiák azaz Privacy Enhancing Technologies vagyis röviden PET.

Gulyás Gábor összefoglalta dióhéjban a PET portál eddigi eredményeit, és a közeljövőben várható tanulmányokat, érdekességeket.

A legszórakoztatóbb és legszemléletesebb előadás kategóriában egyhangú pontozással Fóti Marcellnek ítéljük a díjat, aki a Rainbow táblákról mesélt, és illusztrálta, mutatta be az ezzel kapcsolatos érdekességeket, sőt a sokak szemében őskövületnek számító debug programmal egy hashből visszafejtő assembler programot is elővezetett.

A fotók szerint érezhetően **itt gyűlt össze a legtöbb érdeklődő**.

A két nap alatt zajló **Wargame játék eredményhirdetése előtt** már csak egy előadás zajlott, ahol **Földes Ádám beszélt a**

szteganográfiáról, és ennek gyakorlati hasznáról. Érdekes volt hallani, hogy néhány esetben már az is problémát okozhat, ha a rejtett üzenetet ugyan nem tudják megfejteni, de azt már sikerül beazonosítani, hogy valaki valamit rejtve próbált meg tovább küldeni. Vannak országok, ahol ma még ezért is börtön jár.

Minden s**zervezőnek és előadónak ezúton gratulálunk** és köszönjük a munkájukat, és külön köszönet az elvesztett fényképezőgépem megtalálásáért :-) **Viszlát jövőre ugyanitt, ugyanennyi krigli sörrel a kézben!**

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/674576

Kommentek:

keeroy · http://music.blog.hu 2008.09.22. 00:00:55

Kivalo-kivalo!

atleta.hu · http://www.atleta.hu 2008.09.22. 01:19:52

> Néhány éve nagy vihart kavartak a mobil vírusok, melyek eleinte inkább csak
> kísérleti kódok, jópofaságok voltak, de néhányuk már

Foleg, hogy nem voltak. Illetve, hogy hol vannak?

> felesleges Bluetooth forgalommal gyors akkulemerítést, kéretlen
> MMS küldözgetéssel pedig akár anyagi kárt is

Az, hogy irok egy programot, ami a BT-t cseszegeti, meg MMS-t kuldozget, az nem virus, meg csak nem is fereg. Az egy program, ami ezeket csinalja. Virus/fereg onnantol lesz, hogy kepes _onalloan_ terjedni. De ezt te is pontosan tudod.

> A mobil kártevők minden fontos állomását érintve, konkrét példákkal
> ismerhettük meg Csiszér Béla előadásából, aki

Hat ez iszonyat erdekes. En mobil kartevot meg csak eloadason lattam, meg a kulonfele virusirto gyarto/forgalmazo cegek PR cikkeiben. Pedig jo ideje mobil szoftverekkel foglalkozom.

> Kiderült, hamarosan ismét szembesülhetünk a 2004 táján tapasztalt kaotikus
> helyzettel,

Na de mi volt akkor? :) Tegye fel a kezet, aki latott mobil virust vagy ferget. En egyszer lattam _trojait_, de az ellen nem lehet es szerintem nem is kell technologiai szinten vedekezni.

> úgyanis az új Symbian verzió

Ennek ellenere a Symbian megprobalta, es ezzel eleg rosszat tett a (Symbianos) mobil szoftver piacnak. Gyakorlatilag megolik a kis es fuggetlen fejleszteseket. Raadasul faramuci modon az egyebkent sokkal szigorubb kornyezetben futo javas alkalmazasokra meg szigorubb szabalyok ervenyesek. Hiaba irod ala digitalisan, vagy akar hatjod keresztul a nevetsegesen draga JavaCertified eljarason, az alkalmazasod mindig kerdezgetni fog, ha kapcsolodni kell egy szerverhez, es csak hosszas gombnyomogatassal tudja errol lebeszelni a felhasznalo. (Application manager, megkeresed benne az alkalmazast, atallitod egyesevel a jogokat. Ezt tizbol egy juzer fogja megcsinalni, a tobbit elbuktad.)

2008 júniusi feltörésével ismét lehetőség lesz tetszőleges, digitálisan
> nem aláírt programok telepítésére,

Na, errol meg nem olvastam, de hat akkor az tortenik, hogy visszaal a 2004-es allapot, amikor is hol is volt kaosz? :) Valahogy 2001 ota Symbian teloim vannak, es ahogy mondtam nem, hogy nem talalkoztam meg ilyen kartevokkel, de meg csak olyan emberrel sem, aki talalkozott ilyennel. Csak 'szakertoktol' olvastam, hogy mekkor a a baj. Olyan szakertoktol, akik mobilra szerettek volna virusirtot eladni.

> és ez okozhat majd gondokat.

Aha, csak a problema ott van, hogy egy kartevonek nem az alairas ellenorzest kell megkerulnie, hanem valahogy eszrevetlenul be kell jutnia kivulrol a telefonba. Mert ha a felhasznalo telepiti, akkor trojai, az ellen meg szinte semmi nem ved (a Symbianos platform security ilyen alkalmazasa sajnos egy baromsag, es rendkivul kartekony.)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.22. 06:09:27

Hello Keeroy és Atleta!

Jogos a "virus" elnevezéssel kapcsolatos krtika, valóban inkább kártevőt jelent ez. Abban is igazad van, hogy ez "sokkal nagyobb a füstje, mint a lángja" dolog volt, semmint egy világszerte elterjedt valami. Attól hogy a te vagy az én telefonom nem fertőződött meg, ettől még kétségkívül valóban létezett.

Nem lett ez akkora piac semmelyik virusirtó cégnél, tudtommal például az egyik legrégibb játékos, az F-Secure már 1999 óta fejleszt mobil platformokra, de meglepne, ha ebből bármilyen számottevő bevételük származna ;-)

Hasonló okokból felesleges például a Macre írt AV, bármennyire is igyekeznek ezek a cégek népszerűsíteni saját terméküket. Ha slkerül elkerülnöd, hogy te magad trójai vagy rootkitet telepíts, akkor ez ma még felesleges.

A Symbianos progik piaca valóban megsínylette a szogorú szabályozást, állítólag az engedélyezési eljárásban előre be kellett küldeni a konzorciumnak, név szerint milyen függvényeket hívsz meg, és miért :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.22. 10:19:45

Még visszatérve egy röpke pillanatra, a Cabir és a CommWarrior igenis féreg, mert - egy igen utan már - képes terjedni és saját maga másolatát juttatja el egyik készülékről a másikra. Az előadáson említett Lasco pedig egy hús-vér SIS fertőző igazi VÍRUS!

atleta.hu · http://www.atleta.hu 2008.09.22. 12:54:44

Az f-secure iszonyuan nyomta - talan pont 2004-ben -, hogy jonnek a mobil kartevok. Valami PR cikkben meg egy szuper bunkert is mutattak, aminek a lenyege persze egy Faraday kalitka volt, ahol tesztelik ezeket az iszonyat veszelyes kodokat. LOL. Nincs piac, hat megprobalnak teremteni.

Az egy igen utan fertozo ferget azert en nem hivnam feregnek. Raadasul messze nem igaz, hogy egy igen utan fertozne. Aki ezt mondja az vagy hazudik, vagy nem latott meg Symbiant. A bluetooth-on keresztul terjedo fereg ugy nez ki a felhasznalo szemevel - amikor epp jonne befele - hogy eloszor rakerdez a telefon, hogy fogadod-e az uzenetet. Errol mondjuk lattam a youtube-on egy videot, ahol bemutattak, hogy a 9.1-es Symbian alatt ha nemet mondtal, akkor a kerdes egybol ujra felugrott, mert a Cabir a tuloldalon nem adta fel. 9.2-nel mar ha egyszer nemet mondasz, akkor az ugy is marad, akarhanyszor probalkozik a tuloldal.

Na de... onnantol kezdve, hogy igent mondtal, csak annyi tortenik, hogy az inboxodba (ahova az SMSek is jonnek) jon egy SIS file. Neked ezutan meg kell nyinti az uzenetet (egy gombnyomas, ha kijelzi a telo, hogy van uj uzenet, de nekem ugy remlik, hogy el kell maszkalni az inboxba). Aztan az uzenet megnyitasa utan ha jol emlekszem kell megegy gombnyomas, hogy magat a SIS file-t is megnyissa, ebben most nem vagyok biztos (automatikusan nyomkodtam ;)). Utana jon 2-3 kerdes, hogy akarod-e telepiteni, es biztos-e, es ki irta ala, stb.

Tehat valojaban 4-5 gombnyomas, szo nincs veletlenrol, meg egy mellenyomasrol. Tudom, mert fejlesztes es teszteles kozben rengetegszer kellett meg regebben BT-n keresztul felmasolnom es utana telepitenem a cuccot Symbianos telokra. Elmondom, hogy eleg bosszanto volt :). Most mar van alkalmazas, amit ha futtatsz a telefonon, akkor siman kerdezgetes nelkul felnyomja a SIS file-t (fejleszto eszkoz, explict futtatni kell a telefonodon, tehat kivulrol semmit nem ersz vele). Az egyik Symbian hack

pont ezen alapszik, de az pl. csak arra jo, hogy a _sajat_ telodra tudjal alairas nelkul alkalmazast telepiteni.

> igenis féreg, mert - egy igen utan már -

En ezt inkabb trojainak hivom, mert a felhasznalonak explicit telepitenie kell, raadasul ahogy fentebb irtam eleg nehez ezt veletlenul, meg nem tudatosan megtenni.

> A Symbianos progik piaca valóban megsínylette a szogorú szabályozást, állítólag
> az engedélyezési eljárásban előre be kellett küldeni a konzorciumnak, név szerint
> milyen függvényeket hívsz meg, és miért :-)

Semmi ertelme az egesznek. Gondold vegig: irok egy komolyabb alkalmazast, mondjuk nehany tizezer programsor (Symbian eseteben, ahol eleg alacsonyszinten, a C++-nal joval lejjebb kell dolgozni, ez nem nagy kihivas). Aztan elkuldom egy reviewernek, meg meg is vezetem azzal, hogy leirom, hogy mi miert tortenik. Szerinted nehez elrejteni benne nehany tiz/szaz sort, ami olyasmit csinal amit nem kene? Mennyi idot szannak ra nehany szaz dollarert, hogy atnezzek a kodot? Na ennyi ertelme van a symbian signed processzben hinni, ennyire szamit, hogy sikerul-e megkerulni vagy sem. En ugy lattam egyebkent, hogy a hackekkel annyit sikerult elerni, hogy egy kulon (ha jol vettem ki alairt!) alkalmazas segitsegevel a _sajat_ telefnodra utana tudsz telepiteni alairatlan alkalmazasokat.

atleta.hu · http://www.atleta.hu 2008.09.22. 13:11:09

Megneztem ezt a Lasco-t, hat a leirasabol nem egyertelmu, hogy symbianon is fertoz-e. A leiras egyik reszeben az allt, hogy megfertozi az eszkozon talalhato SIS file-okat, amitol ugyan virus lenne, csak hat pont nem annyira jellemzo, hogy a SIS file-ok a symbian eszkozok kozt vandorolnanak, vagyis, hogy az ember SIS (installer) csomagokat tartana a telefonjan, es azt tovabb passzolgatna a haveroknak.

A leiras masik reszeben viszont azt irjak, hogy a SIS fertozest windows alatt koveti el, vagyis a windows-os gepen van egy kulon kartevo, ami az ott levo SIS file-okat fertozi. Ebben egyebkent tobb fantaziat latok, mert gyakorlatilag barmelyik a felhasznalo altal telepiteni szant alkalmazasbol 'tojait' lehet gyartani, a felhasznalo meg siman benezheti a dolgot. Ez igazabol javaval is mukodhet, es talan a leg eletkepesebb (es legjobb ;)) mobil 'virus' otlet, amit eddig lattam. A telorol -telora fertozessel jol lehet paraztatni, csak egyelore nem mukodik. Es ezt mondtam 2004-ben is, es az ido egyelore engem igazol :).

A PCn megfertozni a felhasznalo altal telepiteni szant alkalmazast, vagyis kartekony (de nem tovabb fertozo) kodot nyomni bele az viszont mukodokepes es jo otlet. Siman lehet, hogy a felhasznalok nem veszik eszre a ravaszsagot, mert eleve telepiteni akarjak az adott alkalmazast, es ha ilyenkor visszakerdez a telefon, hogy nincs alairva, hat azt siman tovabbnyomja az ember. Csak hat ez mar nem mobil virus tema, hanem egy mezei PC-s kartevo, ami ugyan mobilon okoz kart, de terjedni PC-n keresztul tud, ezert ott lehjet megfogni.

Ja, es a Symbian fele eszetlen korlatozasokra visszaterve: Blackberryre javaban lehet fejleszteni, a Javas API sokkal tobbet enged, mint a j2me (majdnem annyit, mint a Symbian). Ennek ellenere a korlatozott APIkhoz valo hozzafereshez mindossze egy $20-os (!) kulcsot kell venni, amivel 2147483648-szer lehet alairni. Ez masodpercenkent egy alairast szamolva 68 evig eleg. :)

Szemben a Symbian signed proceduraval, ahol minden valtoztatas eseten fizetheted a dijat, vagy a j2me megoldassal, ahol evi 3-500 USD-t fizetsz az alairokulcsert. Persze ha lejart, akkor telepiteni sem fogjak tudni az alkalmazasod (marmint nem fognak elni az alairassal szerezheto plusz jogok).

Vidi Rita · http://www.hosnok.hu 2008.09.23. 15:14:12

Hát én tényleg törölgetem a könnyeimet...
A következő konferenciára írjátok fel a nevemet a névsorba! Köszi:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.28. 15:40:21

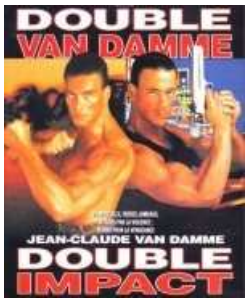
Andrei ifjúi türelmetlenséggel ;-) már mindjárt 5 év után leleplezte magát :-D Íme egy idősebb játékos, aki megfontoltan, nem kapkodva 35 évet várt egy hasonló bejelentésével:
index.hu/tudomany/brittudosok/2009/01/28/nem_letezik_csellohere/

Dupla dinamit

2008.09.22. 12:04 | Csizmazia István [Rambo] | 2 komment

Címkék: suite csomag security smart norton biztonsági nod32 eset symantec lamerek

Ha a Double Impact című mozifilmet nézzük, akkor a "karatéjozós" filmek kedvelőinek biztosan nincs kifogásuk, hogy **egyszerre két példányban láthatják kedvenc Van Dammejukat**. Azonban vannak dolgok, amikből nem olyan izgalmas két egyformát látni.



Nézem a linket, mely a friss Symantec Smart Security nevű csomag megjelenéséről szól, és egyszerűen nem értem. Nincs ezeknek az emberek lelke vagy szeme? Nem nézik a konkurrenciát? **Nem olvasnak újságot, internetet, sajtóközleményeket?** Hogy 2007 októberben már megjelent egy ESET Smart Security nevű komplett biztonsági termék, és **talán mégsem olyan jó ötlet ennek mintájára hajszál pontosan és nyíltan ezt a fantázia nevet adni** a sajátjuknak egy hirdetésben?

Bár ha meg "az érdek a világ ura" szempontjából vizsgálom, még akár tudatos lépésként is elképzelhető: ha egy laikus **bemegy a boltba, hogy vegyen fél kiló Smart Securityt ;-)**, mert eddig csupa jót hallott róla, akkor laza csuklómozdulattal mégis lehet neki a másikat adni a NOD-os helyett, és ez jó üzlet. Nem mellesleg ezzel **a módszerrel akár jól el is lehet harácsolni néhány Google találatot egy másik terméktől**.

Úgy tűnik a sebesség egy idő óta már nem szitokszó náluk. Azt már csak zárójelben jegyzem meg, kíváncsi lennék egy **független, komplett Security Suite tesztre**, hogy **ki milyen sebességgel teljesít AZONOS beállítások mellett.**

Egyszer már beszélgettünk hasonló témáról a Fantázia és ötlet a reklámokban című postban, és most hogy ismét történtek dolgok, kénytelen-kelletlen terítékre került. Remélhetőleg a mostani félreértést **majd békésen tisztázza egymással a két gyártó menedzsmentje**, ki volt az első, mindenesetre **azon biztos nem kell hajba kapniuk a meetingen, hogy mi volt előbb, a tyúk vagy a tojás :-)**. Ám akár direkt volt, akár csak véletlen, szerintem elég sután fest az ilyesmi, kicsit olyan, mint amikor az MS Apple progival készíti az Apple ellenes kampány anyagát :-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/675410

Kommentek:

Algernon 2008.09.22. 15:56:06

"Azt már csak zárójelben jegyzem meg, kíváncsi lennék egy független, komplett Security Suite tesztre, hogy ki milyen sebességgel teljesít AZONOS beállítások mellett."

Az AV-comparatives.org legfrisebb tesztjében vizsgálják a kézi keresések sebességét. Ott a Norton simán győzött.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.22. 17:21:32

Helló!
Igen, azt láttam, de az nem biztonsági csomagok tesztje volt!
Most ezt kezdtem el bújni:
www.passmark.com/ftp/antivirus_09-performance-testing-ed1.pdf

Poénvadászat

2008.09.23. 10:32 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: cd asus rejtvény warez

Gyermekkorom egyik kedvenc újságja az akkori Füles volt, a klasszikus Zorád Ernő és Korcsmáros Pál **képregények mellett mindenféle rejtvény is volt benne**: mi a 19 különbség a két kép között, milyen hétköznapi tárgyat ábrázolnak a következő mikrószkóppal kinagyított tárgyakról készült fotók, és hasonlók. **Most mi is rejtvényezni hívjuk a kedves Olvasót! :-)**

Pár napja jelent meg a hír, amely arról számolt be, hogy bizonyos ASUS noteszgépekhez mellékelt CD lemezeken warez programok, serial számok, és egyéb **"nem szokványos" és kevéssé legális** holmik is megtalálhatók voltak. A cikk arról is beszámolt, hogy a cég annak rendje és módja szerint elnézést kért és **részletes kivizsgálást ígért** - mondjuk sok más lehetősége nem is volt ezen kívül.

A cikkhez mellékelt képet most mi is közreadjuk, élesszemű olvasóinknak adunk egy kis feladatot: **vajon miért tartjuk ezt a képet annyira érdekesnek?**

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/677127

Kommentek:

Nincsenek hozzászólások.

Éljen soká az alapértelmezett jelszó

2008.09.24. 15:38 | Csizmazia István [Rambo] | 1 komment

Címkék: patch jelszó csalás atm default

Sokféle hibát követhet el egy átlagfelhasználó: operációs rendszerébe könnyen kitalálható - ergó szótárban szereplő - jelszót választ, a wifi routerhez nem állít be titkosítást, vagy csak WEP-et, stb. Azonban bármilyen meglepő, **az ATM pénzkiadó automaták üzemeltetői is tudnak nem kicsit hibázni**.

A pénzszerzésnek sokféle módja van, a régi Murphy törvény szerint **mi egy bankrablás egy bankalapításhoz képest ;-)** Sokan csak elhozzák a boltból WiFi routert, kicsomagolják, és az adminisztrációs jelszót nem változtatják meg azonnal, **aztán csodálkoznak, illetve ami még talán rosszabb, észre sem veszik**. Embereink kutakodva a neten, sikeresen hozzáfértek online a Tranax és Triton gyári leírásokhoz.

A két tag ezekben **megtalálta az ATM automaták alapértelmezett gyári jelszavával elérhető rejtett, csak az üzemeltétesnek szánt adminisztrációs menüt**, melyben átprogramozta a gépeket. Ez azt jelentette, hogy bár a gépben 10 és 20 dollárosok voltak, de a menüben úgy írták át, mintha csak egy dollláros bankjegyek lennének.

Így a készpénzfelvételeknél nagyokat tudtak kaszálni, viszonylag csekély lebukási esély mellett. Az volt a dolog sportértéke, hogy nem törték fel a rendszert, nem telepítettek kémprogramot, nem is kellett nem kellett über profinak lenni, **csak "ügyesnek" és ez sikerült nekik**.

Jordan Eske és Nicolas Foster, **mindketten 21 esztendősek**, és némi autós üldözés után immár letartóztatásban, egy Nebraskai cellában várják további sorsukat és a vádemelést. Azért **remélhetőleg a bankok is tanulnak majd az esetből**, és befoltozzák a réseket, na meg a **jelszóválasztási szokásaikon is cizellálnak a jövőben.**

· 1 trackback

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/679244

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.24. 15:54:26

Antivírus blog - Éljen soká az alapértelmezett jelszóSokféle hibát követhet el egy átlagfelhasználó: operációs rendszerébe könnyen kitalálható - ergó szótárban szereplő - [...]

Kommentek:

buherator · http://buhera.blog.hu 2008.09.25. 16:17:02

A dolog pikantériája, hogy a srácok úgy buktak le, hogy többször ugyanoda mentek "nyerőgépezni". Ez persze azért volt lehetséges, mert a károsult az első incidens után sem változtatta meg az alapértelmezett jelszót :)

ITBN 2008 közelről

2008.09.26. 08:28 | Csizmazia István [Rambo] | 7 komment

Címkék: konferencia mom itbn pajzs

Egyszer egy évben előkerülnek az érettségi öltönyök, és komoly tömegek verődnek össze a MOM park mozitermeiben. Az idén azonban **szemlátomást már szűknek bizonyult a helyszín**.

Az Informatikai Biztonság Napján szerencsére a sok reklámszagú bemutató mellett volt pár élvezhetőbb előadás is, **ezekből mazsoláztunk egy csokorra valót**.

Már **pusztán a statisztikák miatt is megérte eljönni**, Sugár Mihály (BellResearch) az IT biztonság helyzetét mutatta be egy friss felmérés alapján, benne külön kiemelve a Top200 vállalatot és a KKV szektort.

Valamilyen vírusirtója szemlátomást majdnem mindenkinek van, de **tűzfal megoldás használata szemlátomást csak a Top200 csoportban** példaértékű.

Gombás László (Symantec) az **adatvesztéssel kapcsolatos előadásában** igyekezett minden részletre kiterjedően ismertetni a problémát és megoldásokat is javasolt ezekre.

A sok mellbevágó adatközül az egyik. A Rambo filmekből idézve, mikor az első részben elindul a hajtóvadászat és mozgósítják a hadsereget, a nemzeti gárdát; a sok katonát látva Trautmann ezredes megjegyzi, **"sok emberből sok halott is lesz"**. Gyaníthatóan az újonnan becsatlakozott számítógépek nagy része odafigyelés, és szakértelem, illetve naprakész védelmi programok híján itt is fertőzött lesz.

Michael Rudrich már **egy "nem létező" szervezettől érkezett ;-)**, hiszen a Secure Computingot alig két nappal ezelőtt vásárolta fel a McAfee.

Előadásában a Web 2.0-val kapcsolatos veszélyekről beszélt, és nekem az tetszett a legjobban, hogy bár elnézést kért osztrák számazása miatti esetlegesen gyenge angolja miatt, ez teljesen **felesleges gesztus volt: tökéletes angolsággal, hibátlan és remekül érthető kiejtéssel** élvezhettük az előadást.

Hamed Khan Angliából érkezett, és **bár az utóbbi időben számos SQL injection témájú bemutatót láthattunk** (Buherátor kollégától is :-), azért ez is élvezetes volt.

Egy webshop piszkálása közben mindkét fél helyzetébe beleképzelhettünk magunkat. Igen szemléletes volt, hogy az SQL hibaüzenetek megzabolázásával ugyan látszólag csökkent a kitacepaózott adatbázis információk mennyisége, de **ez mit sem változtatott a blind módszerrel elérhető további támadási eredményeken**.

Barna Tamás (McAfee) **a bizalmas adatok védelméről** tartotta prezentációját, amelynél a programok csúszása miatt mint a sportversenyeken, rendszeresen beintették neki a még hátralévő percek számát.

Ha az egész nap témáján végighúzodó vékony vörös fonalát kellene megkeresni, az sok fáradságot nem igényelne: **a DLP, azaz a védendő adatok szivárgása elleni küzdelem** lenne az. Vissza utalva Keleti Arthúr (KFKI) előadására, **borzongva láthattuk, hogy a magyar cégek jelentős részében** - és ez alól meglepetésre a Top200 sincs jobb pozícióban - az IT Security feladatokat egy olyan egyéb IT munkatárs látja el, **akinek nem is ez a fő feladata, hanem egyéb munkája mellett látja ezt el**. Ezen a mutatón muszáj lesz változtatni, ha érdemi javulást szeretnénk látni, **különben tálcán kínáljuk fel az adatainkat, adatbázisainkat a támadóknak.**

Hrvoje Dogan (IronPort) a spam háború eddigi mérföldkövei mellett a küzdelem jelenlegi módszereit ismertette, **öröm volt látni a spam evolóció szemléletes példákkal összefoglalt történelmét.**

Az egyik slide egy spamben reklámozott termék terjesztését intéző oldal feltörése utáni állapotba engedett bekukucskálást: nem lódít a statisztika, semmi kétség, **tényleg vannak olyan embernek látszó tárgyak, akik ezektől még vásárolnak is :-(**

Egy különleges ajánlat ismertetése a MessageLabstól. Böröcz Gergely (Filter:max) az egyik leghatékonyabb spamszűrési módot ismertette. **világ legnagyobb levelezési mintájával a szűrők betanítása elképesztően hatékony**. Nekem az volt muris a végén, hogy egyetlenegy kérdésre maradt csak idő a végén, **amely az árról érdeklődött**, azonban a válasz egy diplomatát megszégyenítő szófordulatok után **sem említett egyetlen konkrét számot sem.**

A fejkiszellőztetés közben aztán sikerült két régi ismerőst is "összeereszteni". Krasznay Csaba (Kancellár.hu) és Kristóf Csaba (Biztonság Portál) bár személyesen még nem találkoztak, **hamar megtalálták a közös nevezőt.**

Az előadás angol, a név magyar: Daniel Hetényi a Websense szineiben érkezett, és élvezetes előadást tartott a biztonsági problémákról. Természetesen az adatszivárgás területe innen sem maradhatott ki.

A három teremben párhuzamosan zajó események egyik utolsó előadása Szappanos Gáboré (VirusBuster) volt, amelyben **ezúton is elnézést kért minden Béla nevű embertől a cím miatt ;-)** Tulajdonképpen egy átlagember netezési szokásain keresztül demonstrálta, hogy **milyen mennyiségű kártevő próbálkozik be egy számítógépen** anélkül, hogy a felhasználó extrém szokásokkal veszélyeztetné magát. Aki nem látogat pornográf oldalakat, nem chatel, nem tölt le p2p hálózatokról, az is simán belefuthat szinte bármibe.

· [1 trackback]

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Mai szavunk pedig: keyjacking

bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/682042

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.26. 08:41:08

Antivírus blog - ITBN 2008Egyszer egy évben előkerülnek az érettségi öltönyök, és komoly tömegek verődnek össze a MOM park mozitermeiben. Az idén [...]

Kommentek:

Leni 2008.09.26. 10:19:35

biztosnág kell!

Mindenek felett!

virkid 2008.09.26. 15:44:14

Én is ott voltam az ITBN-en.
Sok jó előadás volt, bár a NOD32-től senki nem adott elő :-))))
Persze a McAfee képviseltette magát. :-)
Kérdésem hozzád, TE elhiszed azokat a számokat, amik elhangzottak Szappanos Gábor előadásán? Szerintem egy kicsit nagyobb számokat adott meg. Véleményed?
Én nem tapasztaltam ekkora kockázatott még, bár az 5-6 perces első támadást már teszteltem, és valós.
És mintha azt is elfelejtette volna közölni, hogy mióta van e-mail címe, és hova szokta megadni. + milyen e-mail címe van...
Kicsit sok volt a program, így már nem emlékszem, ki fejtette ki, hogy bizonyos e-mail címeket gyakrabban bombáznak.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.26. 19:33:09

Helló Virkid!
Na milyen kár, hogy nem futottunk össze!
Ezen én is elgondolkodtam, ha jól gondolom, ez egy már meglévő cim volt. A számok ezért lehettek ekkorák, és biztos nem írt még hozzá egy nullát csak azért, hogy rémisztőbb legyen :-) Egy vadonatúj user vadonaúj email címével nyilván nem ilyen mértékben történik mindez.

Volt régebben tRF-nek (Spányik Balázs, PC World) egy topikja a fórumban, ahol a másik véglet jött elő: nem telepített rezidens cuccokat, de hetente leellenőrizte a netezős gépét, és állítása szerint hónapokig nem talált semmilyen kártevőt. Nekem ez is kissé hihetetennek tűnt :-O

Az igazság szerintem valahol a kettő között lehet, érdemes feltenni az alapszoftvereket, és aztán még így is benyalhatunk olyan rootkitet, amit csak tegnap fejlesztettek ki.

Az én tapasztalataim közelebb vannak - ha nem is ilyen eltúlzott mértékben - Szapiéhoz: telepítettem már úgy Wint, hogy

véletlenül a végére hagytam az AV-t, és ez a kb negyedóra-félóra netkapcsolat is elég volt ahhoz, hogy egy Blaster bepofátlankodjon, és bootolgassa a gépet.

virkid 2008.09.27. 00:41:25

Helló!!!

Az első támadás időpontjával nem is volt probléma, sőt valamelyik angol szaklapom olvastam ennél rosszabbatt is. Nekem a többi számmal volt probléma, bár lehet hogy én nézem szebbnek a világot a a valóságnál. Ahogy rémlik a megadott adatok csak 20-30%-al voltak többek, persze csak úgy, hogy a lélektani határ föllött legyenek, csak egy kicsivel. Lehet, hogy tévedek, de 110 körüli heti spam-et adott meg. Nekem ennyit még nem sikerült, bár van olyan e-mail cimem ami lassan 10 éves, és minden "szürke" helyen azt adom meg. Elvileg fel fogják rakni az előadások anyagát a hivatalos lapra rakni, akkor ha gondolod folytathatjuk... Az egyes adatok elemzését.

Szerencsére nekem már "csak" a vírusvédelem marad, így ha valamelyik telepítő elfelejt szólni, akkor csak a lenovo büvös f11-ét tanácsolom. :-) Szerencsére, a mi hálozatunk zártsága és folyamatos felügyelete miatt kb. 4 éve volt utoljára, hogy egy ilyet kértem, bár akkor IBM-es F11 volt. És akkor amúgy is kergettem a szépemlékű oror vírust osztó gépet.

Vidi Rita · http://www.hosnok.hu 2008.09.27. 08:47:35

Azt szeretném kérdezni, Tőletek, tapasztaltaktól, hogy miért pont ősz a információbiztonság időszaka itthon?
Hacktivity, ITBN szinte egymás sarkában. Utána meg semmi?

Jól tudom, hogy külföldön rendszeresen vannak ilyenek?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.27. 11:03:15

@Virkid:
Jah, igen, itt azért nem alacsony számok szerepeltek valóban. Példaként mondhatom a saját (minden címre egybe nézve) esetem, kb. 30-60 a napi, a kedvesem gépén viszont 80-110. Ezek kb 3-4 emailcímet jelentenek, ezek közül neki is, és nekem is kint van egy állandóra weboldalon, vagyis begyűjthették.

Én ezeken már annyira nem bosszankodom, nagyobb a bajom, ha külföldre levelezek, mert azok jobban elkeverednek a spamek között, és nagyítóval kell elővarázsolni.

Sőt kicist el is szégyelltem magam, hogy ilyen piti spam panaszaim vannak, mert reggel jöttem hazafelé a futásból, és akkor mondta a rádió, hogy Türkmenisztánban MOST, 2008-ban hoztak rendeletet arról, hogy tilos a kínzás a börtönben, és többé nem engedélyezett az embereken való orvosi kísérlet.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.27. 11:08:13

@Rita:
A nyár az uborkaszezon mindenütt, bár amint hallom, hogy a multiknál lassan más szabadságra sem engedik az embereket, így akár július-augusztusban is lehetne bármilyen konferencia. Az ősz az igazi szezon, viszont azt gondolom neked sem kell mondani, hogy kis ország kis konferencia, nagy ország nagy és sok konferencia :-D Pénz kérdés, ez van.

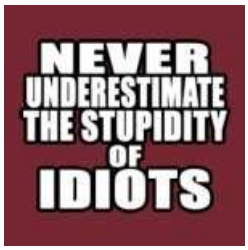
Valamilyen jó kis hacker konfra elmennék egyszer - látni, mit tudnak a fiatalok -, és még életemben nem voltam egy CEBIT-en se, egyszer egy olyat is megnéznék :-)

Van lejjebb - sajnos

2008.09.26. 08:59 | Csizmazia István [Rambo] | 4 komment

Címkék: spam arghhh

Írtunk már pofátlan spamekről, kellemetlen alakokról, **szellemileg szerényen bútorozott humanoidok** e-mail üzeneteiről, kéretlen és idióta véglények reklámjairól, de **úgy tűnik a határt folyamatosan sikerül a béka alá mozgatni.**



Íme egy mai spam termés **No Comment** című rovatunkban, csak erős idegzetűeknek.

· 1 trackback

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/682338

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.26. 09:12:10

Antivírus blog - Van lejjebb - sajnosÍrtunk már pofátlan spamekről, kellemetlen alakokról, szellemileg szerényen bútorozott humanoidok e-mail üzeneteiről, [...]

Kommentek:

Vidi Rita · http://www.hosnok.hu 2008.09.26. 18:10:51

:DDDDDDDDDDDDDDDDDDDDDDDDDDDDD

kínomban röhögök basszus:)))

Ez már művészet...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.26. 19:35:29

Szia!
Én sírok ;-) És még van, aki korábban hiányolta a magyar nyelvű spameket!

pongyolapitypang 2008.09.28. 21:49:30

Istvan, toled privat uzenetben lehet kerdezni?
p

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.28. 22:59:51

Szia!
Itt találsz e-mail címet:
www.commodore64.hu

Én és én meg az adathalász

2008.09.29. 16:12 | Csizmazia István [Rambo] | 1 komment

Címkék: csalás ellen phishing monitorozás asc

Egy **új szolgáltatás mutatkozott be az adathalászat, illetve a személyiséglopások elleni küzdelem frontján**. Ha előfizetünk rá, **széles körben monitorozzák az internet sötét bugyrait**, és figyelmeztetést kaphatunk, ha adatainkat valahol pénzért kínálják.

Az ASC, vagyis Affinion Security Center korábban főként bankoknak és pénzintézeteknek kínálta tevékenységeit, de most elérkezettnek látta az időt **az egyszerű internet felhasználó ügyfelek felé is nyitni**, az USA-ban egyelőre egyedüliként. A vállalat **hackerfórumokat, IRC szobákat, és egyéb helyszíneket fog ellenőrizni**, és ha a kuncsaft neve, számlájának adatai itt bármilyen formában megjelennek, **azonnali értesítést küld** a megrendelő számára, hogy haladéktalanul intézkedni tudjon.

Az adatainkat persze **nem csak mi veszíthetjük el óvatlanul**, vagy biztonsági programok használata hiányában, hanem **elveszíthetik (és el is vesztik) azokat azok a cégek is, akikkel kapcsolatban állunk** - gondoljunk csak a sorozatos Brit botrányokra. A végeredmény szempontjából szinte mindegy is, hogyan történik a dolog, a lehetőség viszont most adott mindenkinek, aki a havi 15 USD-t, azaz mai áron nézve nagyjából 2500 HUF összeget rászánja, egy szalmaszálat adjon magának.

A nagy kérdés persze az, hogy az ellopott banki hozzáférések birtokában **mi fog előbb megtörténni**: jönnek az értesítések, hogy valaki vadul csapolja a számlánkat vagy az internetes adatok között bukkan fel az accountunk még idejében. Viszont **személyiséglopás esetén kétségkívül lehet kézzelfogható haszna**, mielőtt a "másik én" autót bérel, hitelt vesz fel, feleségül veszi Irént vagy egyösszegben kiveszi előlünk a nyugdíjalapunkat.

· 1 trackback

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/687450

Trackbackek, pingbackek:

Trackback: Propeller 2008.09.29. 16:21:49

Antivírus blog - Én és én meg az adathalászEgy új szolgáltatás mutatkozott be az adathalász illetve személyiséglopások frontján. Ha előfizetünk rá, széles körben [...]

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.31. 12:37:59

19 ezer hitelkártya titkos adataira talált a Google
www.penzcentrum.hu/cikk/1016968/1/19_ezer_hitelkartya_titkos_adataira_talalt_a_google

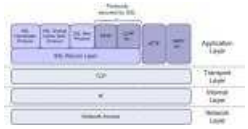
Utazzon velünk!

2008.09.30. 14:44 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: ssl biztonság text fejlesztés account clear tanúsítvány érvényes

Utazni szinte mindenki szeret. Ez a fele még nem is hangzik olyan rosszul, hurrá, irány a napfényes Kalifornia! De **ha ez az utazás a nevünkre és jelszavunkra vonatkozik, és ráadásul clear textben az interneten** történik - hát elmegy a kedvünk az egésztől.

Egy tegnapi cikkben egy kanadai programozó éppen arról panaszkodik, hogy a Yahoo rendszert kiegészítő Zimbra a levelezőszerver IMAP-on keresztüli elérésekor ilyen, **szabadon olvasható szövegként küldözgeti a szerencsétlen felhasználók accountját**. Mondjuk az illető talán nem a legszerencsésebb helyre postolta a panaszát - a Zimbra fórumába - ehelyett inkább érdemesebb lett volna e-mailben a fejlesztőknek, bár abban is van persze igazság, hogy **ha van egy kis nyilvánosság**, akkor váratlan sebességgel, teljes mellszélességgel rámozdul a különben lomha gépezet. Emellett a Yahoo szóvivője is ígéretet tett arra, hogy ellenőrzik a problémát.



Néha szinte megsajnálom Rózsahegyi Zsoltot, aki rendületlenül előd ásokat, sajtótájékoztatókat tart, és kissé szélmalomharcra emlékeztető módon **erőfeszítéseket tesz az elektronikus tanúsítványok ügyében**. Ha **mindenhol lenne SSL, ha sehol nem fogadnák el az érvénytelen, lejárt vagy sajátként aláírt tanusítványt**, akkor vagy azonnal megállna az élet, de inkább egy picit jobb lenne tőle a világ, ha nem is gyógyír ez mindenre.

És talán még az olyan inci-fincidensek is elkerülhetők lennének ;-), ami ma sajnos nem igazán.

Szóval **nemcsak pogácsákat kellene majszolni** legott az ilyen ITBN-eken, hanem az illetékeseknek végre konzekvenciákat levonni, és vadul sietve belerobogni a várvavárt fejlesztésekbe, SSL for President, biztonságos belépést mindenhova, meg hasonlók (például ha lassan is, de az IWIW-nek végre sikerült 8-ról 20-ra emelni a jelszóhosszt ;-) hogy végre valahára **történjen már egy kis előrelépés az ÁTLAGFELHASZNÁLÓ biztonságában** is.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/688607

Kommentek:

Nincsenek hozzászólások.

Miért érdemes NOD32-t használni?

2008.10.01. 15:22 | Csizmazia István [Rambo] | 4 komment

Címkék: reklám film mozi rajzfilm klip nod32 sebesség

Reklámok ma már mindenütt vannak, sokszor **egészen elképesztő helyeken és formában** bukkannak elő. **Az orosz NOD32 disztribútor** (LETA) egy igen ütős reklámmal igyekszik népszerűsíteni az ESET víruskeresőjét, fiatalok figyeljetek :-)

Tehát miért is érdemes ezt használni? **Hát mert anyukánk is ezt ajánlja ;-)** Sok komment és magyarázat nem kell hozzá, a sebesség fő szerepet kap itt is - hát akkor lássuk a medvét :-)

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/689240

Kommentek:

sanya18 · http://www.erepmarket.com 2008.10.06. 23:51:43

ez nagyon lol :D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.13. 14:15:49

Egy Indexes post, hogy a PCW februári biztonsági csomagok nagyteszten a leggyorsabb és a PC World ajánlata "plecsnit" kapott az ESS ;-)
index.hu/info/2009/02/11/a_leggyorsabb_virusirto/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.29. 09:25:50

Itt egy másik jópofaság, ezt most Kasperskys:
www.youtube.com/watch?v=oSxPEEhhKg8

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.28. 13:47:12

Eugene újabb filmje, karate fanoknak kötelező :-)
bit.ly/JJHnL

Aki keres, az talál

2008.10.02. 11:30 | Csizmazia István [Rambo] | 2 komment

Címkék: keresés torrent csalás warez

A mai internetes világban **még egy műszaki antitalentumnak sem okoz gondot, hogy valamit megtaláljon**. Ha például egy szoftvert szeretnénk letölteni, **weblapok, FTP tárhelyek valamint torrent oldalak százai állnak haptákban**.

Biztosan sokan ismerik azt a szokást, amikor a kártevő terjesztők **elgépelésre számítva tucatjával foglalják le** a bankok, hivatalok, pénzintézetek, intézmenyek neveihez megtévesztően hasonló, 1-2 betű eltéréssel rendelkező domaineket. Ez esetben éppen a tévesztésre, elütésre, hibára építenek, de mint **a hiba, mint a véletlen csodás eszköze, sokszor értékes felfedezésekre is vezet**, ehhez elég egy tábla csokit vinni a laborba, majd felfedezni a mikrosütőt ;-)

Szóval **az elgépelés játszotta itt is a főszerepet** - és bár egy ehhez hasonlatos esetről már értekeztünk egyszer - annyira vicces, és talán elgondkodtató is egyben, hogy **nem bírtuk ki ráadás nélkül a témában :-)**

Ezúttal az Extratorrent nevű kereső borzolta fel a kedélyünket, éppen egy kártékony szoftvert próbáltunk felkutatni, és **a mellégépelés ellenére mégis azt jelezte, hogy megtalálta**. Nocsak, vérszemet kapva rögvest közelebbhúzodtunk a monitorhoz és válogatott eszeveszett baromságokat kezdünk a keresőmezőbe írni, **de nem volt olyan, ami meg ne lett volna az Extra torrent gyűjteményében**. "Anyád hogy van V:100.100" - ez is meg van neki, még hozzá CD rippelt változatban is, sőt keygen is van hozzá. Most vagy eljött a Kánaán, vagy valaki szórakozik velünk. Nosza vigyünk hát végig egy teljes keresést, talán nem tévedünk nagyot, ha a következő nevű szoftvert vélelmezhetően még éppen nem fejlesztették ki ;-)

Mégis ott van a polcon, mi ezúttal a full verzióra gerjedünk, hátha freeware és ingyen adják, **nem piszkoljuk be a kezünket holmi keygenekkel ;-)**

Érdekes módon a keresett dolog többek Korda György Aranyalbumán, és Kurtág György MP3-as gyűjtemény csomagjában is szerepel, hát akkor hajrá előre, zsetonunkat ezúttal az Aranyalbum mellett tesszük le, bár szívünkben erős a kétely, hogy keresésünk tárgya a csomagban vajha benne lesz.

A végkifejlet persze **a szokásos kamuzás**, random terheltségű szerverek a nagyvilágban - Párizs, Róma, NewYork, London, stb. Azért kiválasztunk egy kevésbbé foglaltat, játsszuk végig a játékot, értjük mi a tréfát (csak nem szeretjük ;-) Egyébként bármelyi ág, bármelyik tételét, bármelyik letöltési szerveren kiválaszva ugyanazt az eredményt kapjuk. Kicsit olyan, mint a kurblit megtekerve a Celeb Carrier Creator program.

El is indul a letöltési procedúra, mennek az animációk, már szinte célbaértünk, hogy boldog "Baromarcú féllábú bárgyú puputeve" tulajdonosok lehessünk, amikor egyszercsak váratlanul...

... hibaüzenet jöve elénk: **Csak regisztrált juzer uraknak only**, egyszerű látogatók kiméljenek. Vigasztalhatatlanok vagyunk, szomorkás félmosollyal orcánkon törölgetjük a mély csalódás okozta krokodilkönnyeinket, hüp-hüp, köszönjük Emese.

Mellesleg, hogy a jog eszközeivel mit lehet egy ilyen csaló oldallal tenni, gőzöm sincs, de talán ott is meg lehetne próbálni valamit ügyködni. És itt jönne a mondanivaló lényege. A **kártevők nagy része már ma is ellenőrizetlen programcsomagokkal, letöltésekkel terjed**, mi magunk telepítjük, és a trójai trükkök idővel kedveltek lettek/lesznek az alternatív platformokon is (Mac, Linux, iPhones, stb.) Ha **van elég balek, aki nem létező kodeket installál**, hogy lásson valami érdekes mozit, **előbb-utóbb szeretne majd ingyen játékot, okos utilityt, akármit**, és bőszen kattint, letölt, telepít bármit.

És talán hamarosan lesz majd olyan letöltési oldal - láthatjuk, hogy a Mybittorrent mellett egyre több ilyen idióta minden keresést látszólag alázatosan kiszolgáló weblap keletkezik -, **ahol nem a fityiszt fogják mutogatni**, és mélyen szánalmas "members only" riogatással elhessegetni bennünket, **hanem kedvesen fel is ajánlanak bármilyen (létező vagy nem létező) szoftver nevében egy letöltést**, amit aztán lefuttatva **érkeznek majd a kártevők rogyásig** a naív felhasználók gépeire.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/690469

Kommentek:

WUT (törölt) 2008.10.19. 11:33:12

azaz: a lemezcégek, filmstúdiók, szoftvergyártók, és (mostanában már) a könyvkiadók legnagyobb problémáját, a mindent illegálisan letöltögető, torrent-hálózatokat tömegesen használó fogyasztókat idővel, fokozatosan el fogja rettenteni az a sok szemét, ami a gépükre kerül..

eleve mindennel szemben gyanakodni kell, ami "ingyen" kínálja magát. semmi sincs ingyen.

cett · http://cettblogja.blogspot.com 2008.11.04. 23:42:31

Thx. a trackback-et!

Nem bízzák a véletlenre

2008.10.06. 17:50 | Csizmazia István [Rambo] | 1 komment

Címkék: google spam letöltés trends véletlen tudatos kártevők

Perhaps accident - így kezdődik a Szent Lajos király hídja, amiről viszont most mi fogunk beszélni, az **biztosan nem véletlenül történik, sőt.**

Két érdekesség is feltűnt a napokban, az egyik az, hogy korábban sokat irkáltunk már olyan spamekről, melyek **minden ünnepet, eseményt, katasztrófát igyekeznek felhasználni** a kártevők terjesztéséhez. Most Dancho Danchev érdekes észrevételét olvashatjuk arról, hogy egyre profibbak már: **a Google Trends alapján választják ki, mi az a hír, esemény, amit fel lehet használni a levelekben**. Valószínűleg megszaporodik majd a bankok csődjéről, adóságrendező hitellehetőségekről, stb. szóló levelek száma, és ezekután már nem csak vaktában, véletlenszerűen osztják a matériát, hanem igencsak tudományosan. Ami még újdonság, hogy ezeket a híreket aztán **különféle csalárd blogokban is felhasználják úgy, mintha a hozzászólásokhoz videó felvételek linkjét melléknék**, ezek persze nem is filmekre, hanem kártevőkre mutatnak. Az ilyen manipulációkkal próbálnak a bűnözők - és azt tippeljük sikerrel - javítani a saját esélyeiken.

A **másik dolog egy új típusú spam**, ami természetesen egy kártevőt letöltő oldalra mutat. **Emlékszel még rám - kérdezi egy női név**, és a viharosabb előéletű férfitársak kétségek közt kezdenek vergődni. Szerencsére a "jólelkű" Jenna még fotót is mellékelt magáról, na milyen formátumban? Nem JPG, nem PNG, nem GIF, nem BMP, sosem találnák ki, inkább elárulom: EXE.

Szerencsére a **NOD32 Statik motorjának heurisztikája** szépen elkapja, ámbár a new_fotos.exe nevű állomány igen trükkös új variáns lehet, mert kikapcsolt vírusirtó mellett letöltve és utána a VirusTotalon vizsgálva már nem kapunk találatot - igaz itt még a 2.7-es parancsori modul dolgozik.

Vagy az exbarátnők neveit kell jól memorizálni, vagy naprakész vírusvédelmet kell használni, **persze a kettő ötvözete sem rossz választás ;-)**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/699749

Kommentek:

gothmog 2008.10.18. 15:37:34

gmailben lehet .exe-t küldeni? nekem -igaz nem ma volt- még bezippelve se hagyta, hogy akármi futtathatót küldjek, azt hittem ez még így van...

A trójaiak továbbra is kapuk előtt

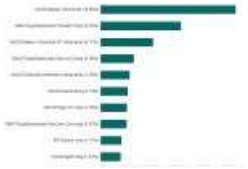
2008.10.07. 11:58 | Csizmazia István [Rambo] | 3 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Sok minden állhat a kapuk előtt: Hannibál, esetleg Hannibál Lecter, Bill Gates, vagy egy sor kuka, vendégek, egy bűvös kocka, Dr. Del Medico Imre, Nyilas Misi, netán Rúgóláb seriff személyesen. Az ESET múlt havi kártevő statisztikája alapján úgy tűnik, **a magyarországi kapuk előtt ;-) főként a trójaiak tolongtak a legnagyobb számban**.

Az ESET statisztikája szerint hónapok óta **nem változott jelentősen** a Magyarországon pusztító kártevők toplistája. A legtöbb fertőzést folyamatosan az okozza, hogy a felhasználók **figyelmetlenül, vagy valamilyen ingyenes tartalom reményében** hasznos szoftvereknek álcázott kártevőket telepítenek számítógépükre.

Szeptemberben 5 trójai is bekerült a TOP10-es listába. Ezek a kártevők – a görög regékből eredő nevükhöz híven – **olyan programok, melyek valami mást csinálnak, mint amit gondolnánk róluk**. Fájlokat törölnek, felülírják a merevlemezt, vagy távoli hozzáférést biztosítanak a rendszerhez a támadónak. A klasszikus trójai általában tartalmaz egy billentyűleütés-naplózót (keylogger) is, amelyet készítői játéknak vagy valamilyen hasznos segédprogramnak álcáznak, számos azonban nem kémkedik „mindössze” kéretlen reklámokat jelenít meg a számítógépen.



A trójaiak ilyen mértékű terjedése persze érthető, hiszen ki ne szeretne egy praktikus kis segédeszközt, egy ingyenes játékot, vagy egy hasznosnak látszó programocskát? Azonban **a kártevők készítői alaposan visszaélnek a bizalmunkkal, és arról is gondoskodnak, hogy a felfedezés után csak nagyon nehezen lehessen eltávolítani azt számítógépről**. A trójaiak így **sokszor több száz állományt és Registry bejegyzést hoznak létre az operációs rendszerben**, melyek segítségével gondoskodnak arról, hogy a gép újraindítása után újra és újra vissza tudják magukat másolni.

Érdemes tehát ügyelni arra, milyen segédprogramokat telepítünk a számítógépünkre. Különösen érdemes óvatosnak lenni olyankor, ha az adott alkalmazást ismeretlen gyártó készítette. Ilyenkor **próbáljunk rákeresni a program nevére az interneten**, és ha azt látjuk, hogy más felhasználók elégedetlenek vele - **minden bejegyzés a "How to remove..." kifejezéssel kezdődik :-)** - inkább tegyünk le a használatáról.

Az antivírusgyártók egyébként óvakodnak attól, hogy a lista 5. helyén álló My Web Search Toolbarhoz hasonló programokat vírusnak minősítsék. A hasonló kártékony szoftverek gyártói ugyanis **sokszor legális cégek mögé bújva beperlik a vírusirtó programok készítőit**, mondván, hogy akadályozzák üzletmenetük folytatását. Az ESET ezért döntött úgy például, hogy termékeiben a kéretlen alkalmazások keresését a felhasználónak magának kell beállítania. Ezt a funkciót tehát érdemes aktiválnunk a vírusirtó telepítése során. Így beállítva **a NOD32 nem is engedi letölteni illetve futtatni az ilyen kétes és felesleges programokat**, de azt tudomásul kell venni, hogy a felhasználók megtévesztésével, és így aktív közreműködésével terjedő károkozók ellen egyetlen vírusirtó sem nyújt tökéletes védelmet.

Végül következzen **a magyarországi toplista. Az ESET statisztikai rendszere szerint szeptemberben** az alábbi 10 károkozó terjedt a legnagyobb számban:

1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a szeptemberi fertőzések között: 10,66%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET kategorizálása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

2. Win32/TrojanDownloader.Wimad.N trójai
Elterjedtsége a szeptemberi fertőzések között: 6,32%

Működés: A Wimad.N egy trójai letöltőprogram, amely a Win32/Adware.PlayMP3Z vírust telepíti a PC-re. A kártevő úgy kerül a számítógépre, hogy a felhasználó figyelmetlenül elfogadja a licencszerződést, amellyel egyúttal jóváhagyja a további tartalmak letöltését. Az Adware programok általában azáltal válnak ingyenessé, hogy cserébe bele kell egyezni, hogy reklámokat jelenítsenek meg a gépünkön.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-wimad-n

3. Win32/Adware.Virtumonde.FP alkalmazás
Elterjedtsége a szeptemberi fertőzések között: 4,11%

Működés: Ez a kártevő szintén a kéretlen alkalmazások táborába tartozik az ESET kategorizálása szerint. Futása közben különféle felnyíló ablakokat jelenít meg. A trójai megkísérel egy távoli szerverhez csatlakozni, és onnan további komponenseket letölteni.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde-fp

4. Win32/TrojanDownloader.Swizzor.D trójai
Elterjedtsége a szeptemberi fertőzések között: 2,58%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat töltöget le és telepít. A Swizzor.D terjedéséhez a hiszékenységet is kihasználja: olyan programokba szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a „csomagban". Ha a Documents and Settings\User\Application mappán belül találunk egy „DVDAUDIO" könyvtárat, az is árulkodó jel lehet.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-d

5. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a szeptemberi fertőzések között: 2,26%

Működés: Az Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró-adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/toolbar-mywebsearch**

6. Win32/Autorun féreg
Elterjedtsége a szeptemberi fertőzések között: 2,10%

Működés: A Win32/Autorun egyfajta gyűjtőneve a Windows rendszerek alatti autorun típusú automatikus programfuttató fájlt használó kórokozóknak. A kártevő az INF/Autorun egy variánsa, de nem az autorun.inf, hanem a hasonló funkciókat ellátó autorun.exe fájlt fertőzi meg. A baj bekövetkezésének egyik jele, hogy a számítógép működése drasztikusan lelassul. Míg az INF/Autorun a szöveges konfigurációs állományokat támadja meg és írja át, a Win32/Autorun csoport alatt azokat a végrehajtható állományokat értjük, amiket az autorun.inf betölt, elindít és lefuttat.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: **http://www.eset.hu/virus/autorun**

7. Win32/Wigon.CK trójai
Elterjedtsége a szeptemberi fertőzések között: 2,03%

Működés: A Win32/Wigon trójai kártevő család a számítógépre jutva különböző fájlokat hoz létre a Windows\System32 alkönyvtárban, ezek egyike a WinCtrl32.dll. Ezek segítségével készít el további kártékony állományokat a helyi gép TEMP mappájában, és eközben a rendszerleíró adatbázisban is módosításokat végez. A bejegyzések segítségével eléri, hogy a fertőzött DLL állomány törlése utáni rendszerindításkor az ismét visszakerülhessen. Tevékenysége során elindít egy szervizfolyamatot is a fertőzött gép memóriájában.

A számítógépre kerülés módja: a felhasználó maga telepíti
Bővebb információ: **http://www.eset.hu/virus/wigon-ck**

8. W□ A/TrojanDownloader.GetCodec.Gen trójai
Elterjedtsége a szeptemberi fertőzések között: 2,02%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki .letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files \ VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben, és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: .A felhasználó maga telepíti..
Bővebb információ: **http://www.eset.hu/virus/trojandownloader-getcodec-gen**

9. INF/Autorun vírus
Elterjedtsége a szeptemberi fertőzések között: 1,61%

Működés: INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár .mp3 lejátszókon) terjed.
Bővebb információ: **http://www.eset.hu/virus/autorun**

10. Win32/Agent trójai
Elterjedtsége a szeptemberi fertőzések között: 1,53%

Működés: Ezzel a gyűjtőnévvel azokat rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti
Bővebb információ: **http://www.eset.hu/virus/agent**

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/700787

□ommentek:

□ orgó □ uki 2008.10.1□. 17:5□:50

Kedves István!

Tudom, ez nem a segélykérő blog, de miután fél napja próbálok valamilyen módon megszabadulni egy trójaitól, így (végső) elkeseredésemben ide írok.
Természetesen a NOD32 megtalálja és a naplóban az alábbi bejegyzés jelenik meg:

C:\WINDOWS\system32\ljJCtstQ.dll - módosult Win32/Adware.Virtumonde.NCD alkalmazás - törléssel megtisztítva (a következő újraindítás után) - karanténba helyezve [1,2]

A probléma ezután kezdődik. Ugyanis újraindítás után sem törli. Megpróbáltam törölni az intéző, illetve a Total Commander segítségével is, de írásvédett a fájl, így nem engedi. Akkor sem tudom megtenni, ha csökkentett módban indítom az XP-t, átnevezni sem tudom a fájlt. Esetleg valami tipp? Köszönöm!

Csizmazia István [Rambo] □http://antivirus.blog.hu 2008.10.1□. 15:05:2□

Szia Morgó Muki!

Ilyenkor segíthet az UnDLL
www.softpedia.com/get/Antivirus/UnDLL.shtml

vagy az Unlocker alkalmazás
ccollomb.free.fr/unlocker/

amely programokat pontosan ezekre a helyzetekre fejlesztették ki. Remélem, ezekkel sikerül megoldani a problémát.

□ orgó □ uki 2008.10.1□. 1□:00:35

Köszönöm! Időközben az unlockerrel már megoldottam. Ellenben fellépett egy újabb probléma, amivel viszont nem tudok mit kezdeni, bár nem tudom, mennyiben kapcsolódik a vírus témához. A win XP-m kikapcsolta az automatikus frissítést és nem engedi visszakapcsolni. Egy Hiba: 1058-as üzenet társaságában abbahagyja a próbálkozást és semmilyen módon nem tudom megoldani. Windows support jó tanácsai sem segítenek. Legutoljára a Rendszerleíró adatbázis szerkesztőjét kellett széttúrnom a tanácsira, de meg sem találtam azt a szakaszt, amit keresnem kellett. Egészen egyszerűen nincs ott. Lehet, újra kell telepítenem a windowst is.

Totális ellenőrzést terveznek a britek

2008.10.08. 17:02 | Csizmazia István [Rambo] | 1 komment

Címkék: big ellenőrzés brother mi5

Magánszemélyek teljeskörű internetforgalmát, minden forgalmazott elektronikus levelet és SMS üzenetet ellenőrizne a Kormányzati Hírközpont (GCHQ, Government Communications Headquarters) és tárolnák is ezeket a benyújtott tervezet szerint.

A **terrorveszélyre hivatkozva kezdeményezték** a kiszélesített felügyeletet. Az MI5 jelenleg csak jóval szűkebb körben, és speciális felhatalmazás alapján tud ellenőrizni, de ez a tervezet megadná a lehetőséget minden állampolgár teljeskörű kontrollálására. A javaslat **komoly felzúdulást keltett** jogvédő körökben, és **az emberi jogok durva megsértésének tartják** - nem tudunk ezzel nem egyetérteni.

Szerintük nem szabadna a korábbi gyakorlattól eltérően - ahol külön ügyészségi felhatalmazásra egy adott személyi kör egy adott időszakát vizsgálhatták csak át - a minden és mindenki ellen irányuló Nagy Testvér vonal irányába elmozdulni.

Mindenesetre **a feladat technikailag sem lenne kicsi**: 18 millió szélessávú internetelőfizetést érintene, évi 57 milliárd SMS és 3 milliárd e-mail üzenet átnézését jelenti, a megvalósítási projektre pedig **12 milliárd fontot szánnának**.

Aztán persze az is jó kérdés lehet, hogy egy fertőzött botnetes gép esetében - amely a tulajdonos tudta nélkül mondjuk jól megDDoS-olja (Istenem, ez milyen szép kifejezés ;-) az MI5 weboldalát, ki lesz majd ténylegesen felelőségre vonva?

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/703366

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.02.02. 22:32:37

Azért a finneknél is vannak érdekes fejlemények:
hirek.prim.hu/cikk/71332/

Gyárilag fertőzött Asus EEE PC-k

2008.10.09. 14:14 | Csizmazia István [Rambo] | 3 komment

Címkék: pc hardver japán asus fertőzött eee gyári

Lassan érdemes lesz egy saját rovatot indítanunk **"fertőzött gyári hardverek a polcokon"** címmel. Most az XP-s, Intel Atomos, 80 GB merevlemezzel szállított **Asus mini számítógépek okoztak kellemetlen meglepetést**.

A **PCAdvisor értesülése szerint Japánban kerültek forgalomba** kártevővel fertőzött merevlemezzel felszerelt Asus EEE mini PC-k. A Recycled.exe állományban rejtőző féreg a D: partición található, és **elindítása esetén azonnal továbbküldi magát a C: meghajtóra**, valamint minden rendelkezésre álló USB kötetre is. A Symantec előzetes információi szerint az Autorun.inf fájl manipulálásával történik meg a fertőzés.

Az Asus szóvivői egyelőre nem erősítették meg, illetve nem tájékoztattak arról, hogy más országokba (például az Egyesült Királyság) szállított termékek is érintettek lehetnek-e.

Az hiszem, lassan már **nem is az lesz a kérdés**, hány percet bír egy számítógép vírusirtó nélkül a netre kapcsolva, hanem hogy - a Mission Impossible TV sorozathoz hasonlóan - hány percünk lesz ellenőrizni és hatástalanítani a gyári csomag kibontása esetén a vásárolt eszközt;-) **Mert ami egyszer történik, az véletlen; ami kétszer, az egybeesés; de ami háromszor is, az már összeesküvés :-D**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/704951

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.13. 16:39:44

Kezelik a problémát:
www.reghardware.co.uk/2008/10/13/asus_japan_virus_response/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.21. 08:23:27

Lassan minden gyári gépnél gombóc lesz az ember torkában :-O
blogs.zdnet.com/security/?p=2203

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.29. 11:22:50

Itt is van egy Samsung képkeret gyárilag előtelepített kártevővel:
www.samsung.com/us/support/news/supportNewsAlerts.do?spp_news_seq=761

Boldogok a lelki szegények...

2008.10.10. 11:18 | Csizmazia István [Rambo] | 13 komment

Címkék: spam hoax álhír idióták

... mert övék a mennyek országa állítólag. Sok olyan spam esik be a postaládába, **amelynek nem is a feladójáról, hanem számtalan _TOVÁBBKÜLDŐJÉRŐL_ azt gondoljuk, ilyen ember egyszerűen nincs**. Sajnos azonban mégis van. Szellemileg szerényen bútorozott rovatunk következik.

Jó pár éve ment a Petrocelli sorozat, sokra nem emlékszem belőle, de az a mondat megragadt, amikor valakinek ezt mondja: "Apám arra tanított: Fiam **csak akkor vívjál szellemi párbajt, ha az ellenfél nem fegyvertelen!**". Hát ha most is ennek szellemében járunk el, akkor abszolúte nem tehetünk semmit.

Forward a négyzeten, sőt a köbön!

A Beatrice "Minek él az olyan" című dala zsong a fülünkbe...

Egyszerűen érthetetlen a dolog, mitől ilyen ragadós a példa ...

Bill Gates majd e-mail küldésért fizet nekünk, mert neki sok pénze van, na persze!

Az kifejezetten szomorú, hogy **vannak még emberek, akik ezeket az álhíreket még elhiszik**. **De a még szomorúbb az, hogy habozás nélkül minden ismerősük e-mail címét közprédaként odadobják bárkinek**. Innentől számítógépes kultúráról, a privátszféra védelméről

beszélni már igencsak nehéz :-(

Azért hogy mégis jó szájízzel záruljon ez a post, egy örökzöld Hoax ismertetőt mellékelünk a végére :-D

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/704619

Kommentek:

movhu 2008.10.10. 12:11

Az alapmű:

yikes.tolna.net/hoax

Illetve egy szájbarágós:

mover.blog.hu/2008/01/13/a_hoax_ol_butit_es_nyomorba_dont

törölt felhasználó törölt 2008.10.10. 12:15

Régen volt egy nagyszerű intézmény, amit úgy hívtak Taigetosz.
De tényleg... Az még, hogy egy 10 éves emós továbbküldözgeti belefér, majd kinövi. De hogy 30-40 éves emberek. És ne mondja senki, hogy azért mert nem ért hozzá, mert ehhez nem informatikai jártasság kell, hanem alapvető emberi ész/logika, amit az iskolában sem oktatnak. De még ha először továbbküldi, aztán felhívják a figyelmét rá, hogy miért nem érdemes és ezek után ugyanúgy továbbküldi, akkor az tényleg darwini eset.

És az a legrosszabb az egészben, hogy a normális ember kénytelen egy külön e-mail címet csinálni, amit a továbbköldözgetős embereknek ad meg, mert az értelemszerű, hogy barátokat olyanokat keres, akiknek 50 fölött van az IQ-ja és nem teszik ki őt spamáradatoknak, de a munkatársait, osztálytársait, rokonait nem válogathatja meg, észt meg még senkinek sem sikerült tölcsérrel tölteni, ha nincs meg benne az ösztön ennek befogadására.

balint 2008.10.10. 18:38

Kedvencem:
www.makingpages.org/pagemaker/humor/badtimes.html

Csizmazia István [Rambo] · http: antivirus.blog.hu 2008.10.11. 1 :2 : 1

Szia Movhu :-)
Igen, az alapmű szerzőjét van szerencsém személyesen is ismerni, egy számítógépes klubba jártunk anno decibel ;.-)
Köszi a "szájbarágós" verzióért.

Csizmazia István [Rambo] · http: antivirus.blog.hu 2008.10.11. 1 :35:40

Helló Penge!
A Taigetosz megoldás azért talán erős, előbb mondanék halálos ítéletet az erőszakos cselekményeket, nemi erőszakot elkövetőkre, pedofilokra, stb. persze érthető az indulat ezekkel a "az embernek látszó tárgyakkal" szemben is :-)

Az igazság sajnos a második bekezdésedben van: muszáj konspirálni, eldobható címeket vagy ideiglenes mukinyulas címeket fenntartani, hogy a szemetet legalább valamennyire távoltartsuk.

A probléma gyökere szerintem két dologban gyökerezik.
1. Azok, akik spammelnek, semmilyen szinten nem érdekli, hogy mit okoz másoknak.
2. Azok a legidegesítőbb felhasználók, akiknek HIÁBA magyarázol el bármit, újra és újra elkövetik UGYANAZT a hibát.

Mivel mindkét típusból rengeteg az utánpótlás, a spammentes szép jövő dolgában kissé pesszimista vagyok ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.11. 19:39:44

Szia Balint96!
Ezt még nem ismertem, de hasonlít arra, mikor azzal fenyeget az új vírus, hogy "összecseréli a fogkrémes tubust a cipőkrémessel" :-D

Fabled 2008.10.12. 22:40:26

viszont a címzettlistát bent hagyni nem szép dolog

balint96 2008.10.13. 14:50:26

Ja igen elfelejtettem írni hogy nem igazi hoax(bár volt valami ilyesmi hogy ezt is elkezdték terjeszteni), hanem a goodtimes paródiája: en.wikipedia.org/wiki/Goodtimes_virus
És vmi olyasmi című könyvben hogy:"Internetbiztonság belülről:Amit a hackerek titkolnak", asszem benne van a magyar verziója.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.13. 16:43:46

Hello Mir!
Próbálom én kerülni a feszültséget, de mindent nem lehet ;-)
Szerinted mennyire lenne hiteles olyan cikk, amelyben sok kis fekete teglalap nez farkas szemet egy nagy fekete teglalappal?
A címeket pont ezért megblur-öltem egy kicsit, egyébkent pedig ez úgyis egy kép, vagyis nincs copy-paste, egy spammernek be kellene gépelni, amit úgysem fog megtenni.

gothmog 2008.10.18. 15:26:54

jó, a tajgetoszról spammelőket ledobálni erős.

Akkor mi lenne, ha csak a számítógépüket b*sznánk le onnan? csak egy ötlet... ;)
Nagy kedvenceim a pps fájlba tömörített, szépnek gondolt fotók, szar minőségben, valamilyen "Évszázados közhelyeink"-című kötetből összeollózott "bölcsességgel. Szar zenével. Meg általában minden pps-es okosság, a "Mars ugyanakkorának fog látszani, mint a hold"-ig bezárólag.
Nem tudom mennyire iq-függő ez egyébként, kaptam én már ilyet állítólag főiskolát végzett mérnökembertől is. Vagy akkor a diploma sem iq-függő.

Csizmazia István [Rambo] · http:□antivirus.blog.hu 200□.03.26. 12:32:41

Szinte hihetetlen, hogy ilyen még történhet 40 évvel a Holdra szállás után :-O
www.kisalfold.hu/kitekinto/embereket_ol_egy_sms_egyiptomban/2092751/
uk.news.yahoo.com/18/20090325/twl-egypt-tries-to-hang-up-on-killer-sms-3cd7efd.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.26. 12:55:47

Még az jutott eszembe, hogy egyszer olvastam egy jó kis mondást: "Ha az újságban a szalagcím végén kérdőjel szerepel, a válasz csak NEM lehet".

Embereket gyilkol egy egyiptomi mobilüzenet?
www.zoom.hu/bulvar/embereket-gyilkol-egy-mobiluzenet-43602.html?ref=hk

titan 2010.05.07. 12:12:06

Két dolog végtelen...

Sírni lenne kedve az embernek

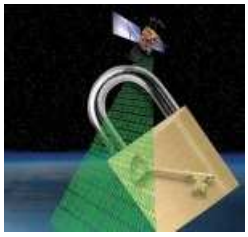
2008.10.13. 17:50 | Csizmazia István [Rambo] | 2 komment

Címkék: adatok titkosítás britek noteszgép ellopás elvesztik

Úgy tűnik, **ami a briteknél zajlik**, az már valóban nem mindennapi. Újabb elvesztett táska, újabb elvesztett laptop, újabb elvesztett ügyfél adatok. **Érdemes lenne külön biztosítót alapítani a problémára, vagy az epsomi derby fogadások mellett erre is kellene tételeket felvenni: mikor lesz a következő elvesztés és melyik hivatal lesz érintve**.

A Vnunet elég szűkszavúan csak úgy fogalmaz, hogy a Deloitte egyik munkatársától ellopták a kézitáskáját, **melyben egy olyan noteszgép volt, amin 100 ezer aktív dolgozó nyugdíjakkal és nyugdíjalapjaival kapcsolatos személyes adata** szerepelt, benne biztosítási azonosítószámok és fizetési adatok.

A TheRegister cikke már 150 ezer dolgozó adatáról ír, és itt már a Deloitte hivatalos közleményét is ismertetik. A **lopás még szeptemberben történt** a nyílt utcán, és igyekeznek mindenkit megnyugtatni, hogy sem lakcímeket, sem banki adatokat nem tartalmazott a számítógép és az eset után azonnal bejelentést is tettek a rendőrségen. Ettől persze még az adatok sorsa továbbra is bizonytalan.



Állításuk szerint - mert ami a jelszóval védett operációst rendszert illeti, az inkább LOL ;-) - elkódolt adatokról van szó. Hogy valóban így volt-e, nem tudni, **mindenesetre nem merik már a hasonló esetkben azt nyilatkozni, hogy egyáltalán nem volt titkosítás, mert akkor hihetetlen haragot vonnának a fejükre**. Ennyi szerencsétlen véletlen egy országon belül azért már mellbevágó.

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/711785

Trackbackek, pingbackek:

Trackback: Propeller 2008.10.13. 18:05:12

Antivírus blog - Sírni lenne kedve az embernekÚgy tűnik, ami a briteknél zajlik, az már valóban nem mindennapi. Újabb elvesztett táska, újabb elvesztett laptop, újabb [...]

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.07. 21:07:46

rdekesség a németeknél:
www.piacesprofit.hu/?r=22381

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.21. 12:09:10

Van már, amiben eredményesen készülünk utólérni a briteket ;-)
index.hu/bulvar/2009/04/21/szemelyes_adatok_a_szemettelepen/

Támadható a Gmail belépés

2008.10.14. 07:31 | Csizmazia István [Rambo] | 11 komment

Címkék: hiba gmail phishing frame flow injection

Egy frissiben megjelent cikk azt mutatja be, hogy egy etikus hacker szerint **lehetséges anonim módon megszerezni Gmailes accountunkat**.

Adrian Pastor (GNU Citizen) közre is adta azt a kísérleti kódot, mellyel egy úgynevezett **Frame Injection Flow** segítségével az eredeti webcím helyett egy **manipuláltat tud elhelyezni a targeturl mezőben** egy biztonsági hibának köszönhetően. Idén áprilisban már volt egy hasonló lehetőségről szó Aviv Raff részéről, az akkori lehetőség a "cross-domain web-application sharing security design flaw" nevet kapta a keresztségben. Ez a mostani erre is rátesz egy lapáttal, és egy harmadik félhez tartozó trükkös weboldallal - **amely legitim címet mutat az address sorban, esetünkben ez most a mail.google.com** - a támadó kényelmesen megszerzi az információt mindenféles XSS manipuláció vagy a szerverbe való behatolás nélkül.

Sokan vannak, akik teljes levelezésüket a Gmaillel valósítják meg, sőt cégek nagy számban is átálltak kényelmi okokból. **Remélhetőleg a prezentáció volt olyan érdemi a Google számára** is, hogy Guiness Rekordok Évkönyvébe illő sebességgel javít és kiküszöböl, mielőtt a trükkös csalók tömegesen hamis belépőoldalakat állítanak fel.

Mi meg **addig is felírhatjuk százszor a táblára**: Nincsenek biztonságos weblapok, Nincsenek biztonságos weblapok, Nincsenek ...

· 1 trackback

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/712757

Trackbackek, pingbackek:

Trackback: Propeller **2008.10.14. 07:38:31**

Antivírus blog - Támadható a Gmail belépésEgy frissiben megjelent cikk azt mutatja be, hogy egy etikus hacker szerint lehetséges anonim módon megszerezni Gmailes accountunkat.

Kommentek:

Hurrá Torpedó · http://www.youtube.com/watch?v=br-D7UneS0E 2008.10.14. 12:56:41

hát előbb szerzi meg az átlag user adatait a hi5, mint egy egy hacker banda.

egyébként a legtöbb bejelentkezős weboldal (=99%) login adatai megszerezhetők a céljuzer gépének hálózati forgalmának figyelésével.

Kara kán · http://karakan.blog.hu 2008.10.14. 13:42:42

Én azt nem értem, hogy a Microfos, amely webböngészőtől elkezdve minden beépített már az oprendszerébe, miért nem tesz bele rendes vírusirtót és tűzfalat is?

Különben a Gmail még mindig biztonságosabb, mint a saját pécéről futó levelezőprogi.

szilárdan... · http://www.flickr.com/photos/haazee 2008.10.14. 13:54:09

Epikurosz: mert sértené a versenytörvényt (haha...)

szilárdan... · http://www.flickr.com/photos/haazee 2008.10.14. 13:57:46

Egyébként nem teljesen értem ezt a támadhatóságot...
Ha be akarok lépni a gmail-re, akkor beírom az URL-t (www.gmail.com) vagy rábökök a könyvjelzőmre.
Ezt tudják "meghekkelni"? Egyéb helyről meg ugye az ember nem mászik rá a levelezőrendszerére...

Anna, a műkörmös · http://mukormos.blog.hu 2008.10.14. 14:06:43

Gmailhez egy kis plusz biztonság:

Beállítások/Böngészőkapcsolat/Kötelező a https használata

Silly 2008.10.14. 14:23:19

szilárdan:

ha nem érted másold be ezt a linket a brózerodba:

mail.google.com/imgres?imgurl=http://SecureGoogleMail&imgrefurl=%68%74%74%70%3a%2f%2f%73%6e%69%70%75%72%6c%2e%63%6f%6d/482f3

ha így sem, akkor ne is akard megérteni...

Alec 2008.10.14. 14:35:52

Silly: szerintem szilárdan pontosan értette a módszert csak nem akarta elhinni, hogy van olyan hülye aki mondjuk egy levélben küldött linkre kattintva lép be a gmailbe

szilárdan... · http://www.flickr.com/photos/haazee 2008.10.14. 15:46:20

Alec: 1:0 ;)

fraki 2008.10.14. 16:02:24

Legyen inkább 1:0,5, mert az url-ek ellenőrzését gyakran csak szemrevételezéssel nézzük, és ha látjuk, hogy a domain rendben van, akkor kattintunk.

Anna, a műkörmös · http://mukormos.blog.hu 2008.10.14. 16:16:03

Igen, ha a webcím eleje stimmel, megbízik benne az ember.

szilárdan... · http://www.flickr.com/photos/haazee 2008.10.14. 17:29:43

fraki: ha a postaládámra vagyok kíváncsi, akkor nem klikkelgetek ide-oda, hanem fix, biztonságos helyről veszem az URL-t.
Ha meg rákattintok egy linkre, majd válaszként kapok egy gmail login képernyőt... hát erősen elgondolkodom rajta, hogy a feladót hová küldjem... (ismeretlen címről érkező mélt el sem olvasok)

Baráti tűzben

2008.10.16. 14:51 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: positive avg zonealarm false vakriasztás

Semmiképpen nem jó az, ha ember embernek farkasa, de az sem, ha **az egyik antivírus program riaszt a másik antivírus program telepítőcsomagjára**. Hofival szólva: "amikor az egyik marxista lövi a másik marxistát, akkor hohó gyerekek, álljunk csak meg, azért ennyire nem olcsó a lőszer ;-)"

A keddi napon kisebb incidens történt az AVG háza táján, vírusvédelmi programjuk téves vakriasztást (false positive) okozott a Zonealarm egyik állományára (zlsSetup_70_483_000_en[1].exe), és abban **látszólag Trojan Agent r.CX kártevőt** detektált. A ZA fórumokban azonnal megszaporodtak a panaszkodó bejegyzések, ám a Grisoft nem kommentálta az eseményeket.

A CheckPoint azonnal kapcsolatbalépett a céggel és sikeresen elérte, hogy **órákon belül kiadják a javított adatbázisfrissítést**, amely már mentes volt a hibától.

Az AVG-nek nem ez volt a legemlékezetesebb balesete, idén **júniusban fedezték fel, hogy a LinkScanner tévesen felpörgette fel és ezzel meghamisította a weboldalak látogatási statisztikáit**, amellyel igen nagy kalamajkát okozott.

· 1 trackback

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/716592

Trackbackek, pingbackek:

Trackback: Propeller 2008.10.16. 14:54:31

Antivírus blog - Dog eat dogSemmiképpen nem jó az, ha ember embernek farkasa, de az sem, ha az egyik antivírus program riaszt a másik

antivírus program [...]

Kommentek:

Nincsenek hozzászólások.

Valóban kicsi az új Norton ISecurity telepítője?

2008.10.16. 07:15 | Csizmazia István [Rambo] | 7 komment

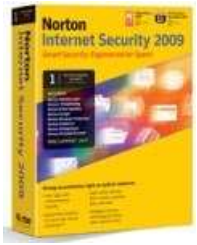
Címkék: teszt kis kísérlet méret trükk norton gyors eset ess symantec telepítési

Vitatható eszközhöz nyúltak a Symantec fejlesztői telepítési idő felgyorsításánál. Csak a kezüket figyeljük.

Nem vitás, hogy minél gyorsabb egy antivírus, annál jobb nekünk. **Nem szeretjük hosszas telepítgetéssel tölteni időnket**, és azt is utáljuk, ha a gépet munka közben pont a vírusirtó lassítja le. Tudják ezt a Symantec szakemberei is, **ezért mindent megtettek, hogy az új Norton Internet Security már gyors legyen**.

Mind a világszintű, mind a hazai sajtó elismeréssel nyilatkozik az új Norton termékek gyorsaságáról, kicsi telepítési méretéről. A Symantec vírusirtója **néhány évvel ezelőtt még lassúságáról volt hírhedt**, most azonban úgy tűnik, megtáltosodott. Olvassuk a Norton Internet Security 2009 varázslatos sebességéről szólóTechline-os cikket, melyben áradoznak arról, hogy "**Csodák márpedig vannak**". A látszat szerint a Norton tehát szárnyra kapott, és ez úgy tűnik **felkeltette a szintén a gyorsasága miatt elismert NOD32 vírusirtó fejlesztőinek** figyelmét. Az ESET szakemberei úgy döntöttek, maguk is megvizsgálják a Symantec új termékének telepítési méreteit. Tartsunk hát velük egy kis kirándulásra, ígérjük izgalmas és tanulságos lesz.

Egy internet biztonsági csomag telepítési mérete - ebben aztán nincs vita - annál jobb, minél kisebb. Mivel a Norton 2009 **még az ESS csomagnál is kisebb volt, ez felkeltette három ESET-es munkatárs**: Andrea Kokavcova, Aryeh Goretsky és David Harley figyelmét, akik **elkezdtek kísérletezni a programmal**.



A saját **laborjukban a Passmark teszt szerinti méréseket végeztek egy Windows Vista operációs rendszer alapértelmezett** beállításaival, majd később egy Windows XP is a pástra lépett. A Passmark módszer nem triviális módon méri a telepítési méretet, hanem a telepítés utáni lefoglalt lemezterületből vonja ki a telepítés előtti lefoglalt lemezterületet, vagyis nem egyszerűen a letölthető telepítőcsomagot nézi.

A kísérlet előtt még muszáj egy picit visszanyúlni a Windows rendszerek egy speciális jellemzőjéhez. Mint ismeretes, a Rendszer visszaállítás (System Restore) funkció szolgál arra, hogy **probléma esetén egy korábbi visszaállítási ponthoz (Restore Point) visszatérhessünk**. A funkciónak persze ára van - mint mindennek az életben - a helyi számítógépen kell tárolni ezeket a pillanatfelvételeket és **ami esetünkben még érdekes lesz: ez nagyban befolyásolja a telepítési méreteket is.**

Hüp-hüp-hüp Barba trükk!

Egyenlő pályák, egyenlő esélyek, én biciklivel megyek :-)
Jöttek tehát a tesztek, Vista és XP rendszereken egyaránt, és ezen belül kétféleképpen is: a System Restore be- illetve kikapcsolt állapotában. A táblázatból jól látható, hogy a Symantec **technikailag titokban kikerüli** a visszaállítást, és **ezzel sikerül neki minden egyes esetben ugyanazt az eredmény produkálnia.** Igaz, ha manuálisan létrehozunk Vistán egy rendszervisszaállítási pontot, akkor a NIS2009 Passmark mérési módszere is 445 MB-os méretet mutat.

WIN Version	*System Restore*	*ESET Size*	*Norton Size*	*Comments*
Vista	ON	368MB	145MB	Same settings and results as Passmark
Vista	OFF	68MB	145MB	Installation sizes without Restore Points.
XP	ON	96MB	145MB	XP equivalent to Passmark settings
XP	OFF	68MB	145MB	Installation sizes without Restore Points.

Az elvégzett kísérletből **az ESET munkatársai szerint egyértelműen kiderül, hogy "Csodák márpedig tényleg vannak". Az új program megkerüli a rendszer System Restore funkcióját csak azért, hogy kisebb telepítési méretet mutasson**, illetve talán hogy ezzel is gyorsabb legyen a telepítés! Ez pedig - ha erre semmilyen előzetes figyelmeztetés nem történik - egyértelműen **biztonsági kockázatot jelent** a felhasználók számára.

Minden tiszteletünk a Symanteces fejlesztőké, és célunk nem a kákán is csomót keresés volt. Ennek ellenére az ilyen kaliberű dolgokról nem szabad hallgatni, valamint nem engedhető meg az sem, hogy **az átlagfelhasználó megtévesztésével és gépének tudta nélküli veszélyeztetésével ilyen vitatható manőverekkel** operáljanak a piac szereplői az egymás elleni harc jegyében.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/714186

Kommentek:

oonline 2008.10.17. 16:48:45

Személy szerint nekem ez nem rossz pont a nortonnál. ahogy feltelepítem az XP-t a rendszervisszaállítást szinte azonnal kikapcsolom, elvégre is, ha vírus kerül a gépre, onnan folyton visszakerül, másrészt, én próbáltam vele visszaállítani dolgot, nem sikerült. Ez az egész cikk is kicsit olyan "használj Nodot, a norton sz*r"" szagú, persze ezzel nem akarok sértegetni senkit, csak egy vélemény.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.17. 19:29:15

Szia Dante01!

Üdv a blogban :-)

Kifejezettem nem célom a zsigerből jövő "fikázás", remélem erre az eddigi működésemmel nem is adtam okot. Úgy éreztem, ez a bejegyzés többről szól, minthogy valaki az A vagy a B terméket használja, szereti.

Nekem ez a varázslatosan felgyorsult telepítés kissé hihetetlen volt - és lám, született is rá egy logikus magyarázat.

Nyilván az őszinteség sokat segített volna a dolgon, akár meg sem születik az ESET-es srácok postja, ehhez szerintem csak annyi kellett volna, hogy mindezt ELŐRE közlik a nagyérdemű vásárlóval pl. rányomtatva a dobozra a figyelmeztetést.

FK 2008.10.19. 16:20:03

Ez mekkora szarrágás! Azt hittem végre egy értelmes cikket olvashatok antivírusokról (ha már antivírus blog), de nem csak hülyeség az egész.

Hol van itt szó a sebességről? Ha mindenki dícséri az új Nortont, akkor valószínűleg meg van az oka, annak kéne utánajárni, nem pedig ilyenen kiakadni. Még hogy az átlagfelhasználót veszélyezteti az, hogy feltelepíti a megvásárolt vírusirtót, és írják rá a dobozra hogy ez mennyire veszélyes??!

Ez igazán szánalmas, és semmi köze nincs ahhoz, hogy mivel lett gyorsabb vagy jobb a Norton, csak arról szól, hogy senki más ne mondja azt, hogy gyors, mert biza csak a NOD32 lehet gyors. Szánalmasok vagytok.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.19. 19:16:29

Kedves Ferenc!

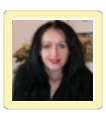
Szerintem félreértetted a dolgot. Ez most a TELEPÍTÉS sebességéről szól. És ha MINDEN (*.*) program átfolyik a bekapcsolt System Restore-on, de a NIS2009 pedig nem, akkor ezzel NEM LEHET dicsekedve összehasonlítani a többi, hagyományos módon települő program sebességéhez képest, nem fair.

Ami pedig a veszélyt illeti, nézz utána, mennyi Registry bejegyzést borít rá a gépedre. Anélkül, hogy szóltak volna, nincs rá lehetőséged, hogy mégis visszatérj a telepítés előtti állapora, hacsak kézzel nem készítettel visszaállítási pontot. Ha erre figyelmeztettek volna ELŐRE, már nincs ez a felvetés.

Keresésben pedig természetesen más is lehet gyors, zajlik a verseny folyamatosan, és ez így van jól.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.20. 09:02:53

Annyiban azért igazad adok kommentelőknek, hogy a cím félreérthető volt, ezért javítottam "Valóban kicsi az új Norton ISecurity telepítője?"-re.



Vidi Rita · http://www.hosnok.hu 2008.10.21. 10:42:57

Egyébként nekem erről az jutott eszembe, hogy marhára nem érdekel, milyen gyorsan települ fel valami. Nyilván, ha sumák módon gyorsítanak, az érdekel, és szeretnék tudni róla.
Amit viszont nap mint nap tapasztalok, az az, hogy bármiről is állnak át az ügyfelek nod-ra vagy ESS-re, állandóan tátva marad a szájuk, hogy: Rita, létezik, hogy begyorsult a gépem?

Naná, hogy létezik, hiszen ritka az ilyen progi, ami állandóan fut és közben észre sem lehet venni. A riválisokra nem ez a jellemző.

Egyébként a nod32 a leggyorsabb és legkevésbé erőforrásigényes védelmi szoftver, és ezt sikeresen el is ültették a fejekben. Innentől kezdve bárki jön azzal, hogy: Hé, most már a miénk is gyors", arról, a marketing törvényei szerint az jut eszébe a felhasználóknak: "aha, MOST MÁR gyors? akkor eddig joggal tartották CSAK az eset termékeket gyorsnak?"

Ezt a pozíciót sosem fogják elvenni a nodtól, nyugalom, próbálkozhatnak akármivel:)
A nod a gyors vírusirtó, a nod a csúcstartó vírusirtó.

Más szavakat kell bitorolniuk, igaz, hogy azoknak már nem lesz semmi értelme. Mert az, hogy biztonságos, az az alap egy védelmi szoftvernél.

Colos 2008.11.01. 08:17:08

Nos, ha már itt járunk, én meg beszélek a NOD32 gyorsaságáról.
A NOD32 egy antivírus, és semmi más. A Norton Antivírus pedig egy antivirus+antispyware. Ha felteszel egy NOD-ot, akkor kell mellé még egy Antispyware is, és csak így lesz egyenértékű a NAV -al. Viszont a két védelmi szoftver jobban belassítja a gépet, mint ha csak egy NAV lenne rajta.

Az azért megjegyzem, hogy nem vagyok NOD32 ellenes, az a program a maga nemében tényleg a legjobb! De a NAV -al a beépített antispyware miatt nem lehet összehasonlítani.

A hosszú élet titka

2008.10.17. 18:43 | Csizmazia István [Rambo] | 2 komment

Címkék: facebook gyilkosság

Ne hazudjunk soha a közösségi portálon, és **ne titkoljuk el, ha házasságban élünk**, mert akár az életünkkel fizethetünk érte.

Egy friss hír szerint letartóztattak egy angliai férfit, aki megölte feleségét. Állítása szerint **az bosszantotta fel, hogy alig pár nappal széltköltözésük után a felesége máris szinglire módosította adatlapját** a Facebook közösségi oldalon.

Az eset még február 18-án történt, akkor az **ittas és kábítószer hatása alatt álló** férj odahajtott a felesége otthonához, és egy konyhakéssel, valamint egy húsvágóbárddal **halálosan megsebesítette az éppen alvó asszonyt**. Tettért 14 év börtönbüntetést róttak ki rá.

Tanulság? Legalábbis a Facebookon ne tegyünk ilyet, az IWIW-ről, illetve egyéb hazai oldalakról és annak veszélyeiről nincsenek adataink ;-)

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/718809

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.24. 08:56:15

Ez is érdekes, sőt a kommentek néha nagyon ott vannak :-) Sajnos biztos lesznek sokan, akik "lelkiismeretesen" minden mezőt kitöltenek magukról, és aztán pedig majd csodálkoznak :-O
emtv.blog.hu/2009/03/23/iwiw_tul_szemelyes

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.05. 10:56:39

Jah igen, és a hatóságok rendszeresen olvas(hat)ják:
nol.hu/archivum/egy_rossz_kattintas_a_facebookon__leleplezte_magat_a_csaladi_potlekkal_csalo_no

Túl sok adatot tárolnak rólunk...

2008.10.20. 09:00 | Csizmazia István [Rambo] | 4 komment

Címkék: adat nyilvántartás gondatlanság

A különböző **cégek, hivatalok kissé átestek a ló túloldalára**: elképesztő mennyiségű személyes adatunkat őrzik - és ki tudja mennyire jól; tartják nyilván - és ki tudja meddig és milyen körülmények között.

Alig néhány hete, hogy **18 hónapról 9-re csökkentette az adatmegőrzés időtartamát a Google kereső**. Ilyenkor az IP címekkel egyetemben - vagyis beazonosíthatóan - megőrződik az internetes ténykedésünk. Az **EU-s szervezetek eredetileg 6 hónapos periódust szerettek volna** elérni, továbbá az is kérdésként merült fel, személyes adat-e az IP cím és be kellene-e szerezni ennek tárolásához a felhasználó beleegyezését. Ha ott van mellette az időpont, akkor nem is kérdés a kérdés.

Vannak aztán olyan jellegű szabályozások, amik eléggé neccesek a **jogállam kontra terror elleni küzdelem** csatájában, például Nagy-Britanniában teljes elektronikus ellenőrzési rendszert készülnek bevezetni. Már szinte félve gondolunk a szigetországban túl gyakori noteszgép és adathordozó elvesztésekre, ahol **sok esetben csak "behazudják" azt, hogy az kikerült adatok titkosítva voltak**. Bár az is igaz, ha az eszköz végül a bűnözők kezébe kerül, ők jó eséllyel értenek hozzá vagy találnak olyan szakembert, aki jó pénzért kinyeri az adatokat - ebből a szempontból mégis a "nemelvesztés" lenne a legmegnyugtatóbb.

Ezek után már szinte meg sem lepődünk, ha ugyanitt **olyan rendelkezés bevezetésére készülnek**, hogy **minden mobiltelefon vásárláskor kötelezően regisztrálnák a személyi adatokat**, csak ezzel a feltétellel lehetne telefonhoz jutni.

Magyarországon is gyűlnek az adatok, elég arra gondolni, ha például valaki **lakásvásárláshoz hitelt vesz fel, mennyi személyes, banki adatot kérnek be**, és ha esetleg a konstrukció még **életbiztosítást is tartalmaz, akkor az összes orvosi adat is bekerül** ezek mellé. És persze nálunk soha nem is lehetett a mobiltelefon vásárlást személyi igazolvány fénymásolás nélkül megúszni.

Összességében sokan gondolják úgy, túl sok adatot tárolnak rólunk és ezek az adatok sokszor nincsenek megfelelően kezelve. Például ha valaki vásárol valamit, de ehhez kezesre van szüksége, az adott boltban nem csak az ő, de a kezes személyes adatai is tárolásra kerülnek. Az adatokat később talán összesítve beküldik a központjukba is. Sok esetben pedig bankkártya adatokat is bekérnek, és az ezekkel megspékelt **adatbázis elvesztése már komoly aggodalmakra adhat okot**. Ráadásul ha ezek az adatbázisok valamilyen módon esetleg az internetről is hozzáférhetőek, akkor pedig az SQL támadások miatt kerülhetnek illetéktelen kezekbe - és ezt akár észre sem veszik azonnal. Emiatt ezen a területen folyamatosan egyre újabb fenyegetések várhatók.

Az biztos, hogy **a felelősség sincs ezzel kapcsolatosan kidolgozva**, itt kellenének olyan változások, amelyek **fokozott gondosságra kényszerítenék a cégeket**, természetesen **az esetleges mulasztások megfelelő szankcionálása mellett. Amíg ez nincs így, maximum reménykedni lehet.** És addig hiába védjük a saját gépeinket vírusirtóval, tűzfallal, kémprogram elleni alkalmazással, adataink titkosításával, hiába ellenőrizzük pedánsan a banki belépésnél a tanúsítvány érvényességét: **ha máshol másvalaki is elveszti azt, ami a miénk, ami rólunk szól.**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/722105

Kommentek:

törölt-felhasználó (törölt) 2008.10.20. 10:45:29

"olyan rendelkezés bevezetésére készülnek, hogy minden mobiltelefon vásárláskor kötelezően regisztrálnák a személyi adatokat"

Ez félig-meddig itt Magyarországon is így van. Bármikor telefont vettem, az volt a feltétele, hogy legalább 18 éves legyek, legyen személyigazolványom és ebből kiírtak olyan adatokat, mint név, lakcím, személyigazolványszám, meg ha jól emlékszem anyám neve...stb. Mondjuk ez szolgáltatónál volt, ahol a SIM is jött a telefonnal, de mivel a legtöbb telefon a repülős üzemmódon meg segélykérésen kívül nem sokra használható SIM nélkül, így mindegy, hogy ahhoz kérik-e az adatokat, vagy a SIM-hez, úgyis célszerű hozzá SIM-et is venni.

Egyébként én már pár éve ezt is megjósoltam, hogy ha nem megy szép szóval (RFID chip), akkor szépen lassan hátulról fogják ugyanezt elérni. Egyre több telefonban lesz GPS, mivel még az Antarktiszról is előkerítenek.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.22. 11:46:54

Nem személyes adat az IP cím, bravo :-O
itcafe.hu/hir/ip-cim_nem_szemelyes_adat.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.23. 14:03:43

És még mondják, hogy ne legyen az ember paranoiás:
index.hu/tech/net/gog0120/
Reszkessen mindenki, aki a "holttest elásása a kertben könnyen és gyorsan", illetve "hamis bombariadó esetleges következményei dolgozatírási időpontban" címszavakra keresett mostanában

Csizmazia István [Rambo] · http:□a□ntivirus.blog.hu
2009.01.23. 14:07:20

Na egy szmájlit akartam még a végére tenni, az lemaradt, íme:
;-)

Herbal Király, ausztrál király vágtat fakó lován

2008.10.21. 15:43 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam botnet internetpol

Néhány napja nagy fogásuk volt a hatóságoknak, a **HerbalKing nevű spamterjesztő hálózat** fejét, a 26 esztendős Lance Atkinsont és csapatát sikerült elfogniuk. Becslések szerint **10 milliárd levél ment ki naponta a mintegy 35 ezer gépből** álló botnet hálózatukból.

A letartóztatás **sajnos nem** hozta meg azt az áhított eredményt, hogy azóta hihetelen mértékben **lecsökkent volna a kéretlen levelek száma**. Ahogy a letartóztatott drogdealerek esetében, már másnap ketten is a helyére állnak, és a hajó megy. Az olvasók közül **van, akit ez érdekel** és nagyjából van is fogalma, hogy mi és miért történik - persze nem a pénzügyi vonatkozásokra gondolunk most, mert az egyértelmű - hanem hogy technikailag hogyan lesz a számítógépből botnet tag. És persze a zöm azt is tudja, körülbelül mit kell tennie ahhoz, hogy ne tartozzunk közéjük.

Nem ördöngősség a dolog, de **a másik és jóval nagyobb csoportnak - akiket mindez nem érdekel** és halvány segédfogalma sincs, miért, hogyan és egyáltalán - lenne inkább teendője ezzel, sajnos nem is futtat a gépén antivírust és kémirtót, még ingyenes programokat sem. Pedig **körülbelül ugyanakkora IQ-t igényelne a dolog**, mint egy tankolás, a hűtőfolyadék utántöltése, csúszós úton való ellenkormányzás vagy egy kerékcsere defekt után. Ha valakinek van jogosítványa, akkor ezekkel elvileg mind tisztában kell(ene) lennie.

Hasonlóképpen **a számítógép is igényel valamennyi odafigyelést, és megbosszulja magát, ha valaki legalább a minimumot nem adja bele** a saját oldaláról: rendesen indítja és állítja le a rendszert, rendszeresen menti a saját munkáit külső adathordozóra, frissíti a operációs rendszerét, használ valamiféle antivírust, kémirtirtót és tűzfalat. Ez utóbbiak mind tudnak automatikus üzemmódban működni - tehát **senkinek nem kell gurunak lennie ahhoz, hogy ezek valamilyen legalább alapszinten fussanak** a gépén.

És mégis - a számok azt mutatják, **van elegendő számú tudatlan és/vagy lusta ember, akik egyáltalán nem használnak** biztonsági programokat, és emiatt a botnetpásztorok hihetetlen vagyonokra tesznek szert. Nem véletlenek az ilyen esetekben kirótt csillagászati bírságok - persze van ebben némi elrettentés is - de elég körbenézni a Spamhaus ROKSO centerében, és rögtön átjön, hogy ezek az emberek nem a küszöböt rágják. A mostani vizsgálatnál is befagyasztották a banda nem jelentéktelen bankszámláját.

Egyszer **évekkel ezelőtt Eugene Kaspersky javasolta, hogy az autós jogosítványhoz hasonlóan** a számítógépes felhasználóknak is **legyen kötelező egy minimum tudást megszerezni és igazolni**, de a dologból nem lett semmi, akkor nem igazán tűnt senki túl lelkesnek ettől.

Egy mostani ötlet talán mégis elindíthat valamit, melyben Mikko Hypponen azt javasolja, hogy legyen egyfajta nemzetközi Internetpol, a **kiemelt internetes csalási ügyekben** tevékenykedhetne. Erre igazából szükség is lenne, hiszen a **komoly, maffiaszerű működés mia** ezek a kémprogramterjesztéssel, és egyéb számítógépes bűncselekményekkel foglalkozó szervezetek szinte minden esetben nemzetköziek, és **remekül navigálják szervereiket, központjukat aszerint**, hogy egyes országokban tevékenységük még nem ütközik törvényekbe.

Azt **persze senki ne gondolja**, hogy az "ez is rendőr - az is rendőr" párhuzam miatt, egy ilyen Internetpol azzal fog foglalkozni, hogy minden felhasználó rendesen védje a gépét. **A gyilkossági nyomozó sosem fog rászólni a fegyelmezetlen gyalogosra, hogy ne piroson menjen át**. Ha már valaki megfertőződött, szerencsére van megoldás: ez a metamorfózis nem egyirányú, a számítógép mentesítése (esetleges Windows újratelepítése ;-) után visszaállhat a normális működés - igaz a sok ellopott adat ekkor már a "kutyáké". A jelszócserék és banki változtatások után viszont jól működik a "saját káron tanul az okos" módszer, alaposan és mélyen bevésődve ;-)

Ahhoz, **hogy ne romoljon tovább a hétköznapi emberek megkárosítási aránya**, a "halászati szövetkezeteket", kártevő terjesztőket, botnet pásztorokat mindenképpen szükséges lenne ipari méretekben levadászni, de legalábbis **komolyan elkezdeni a nagytakarítást**.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Tízből öt kártevő hátsóajtót nyit
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/724447

Kommentek:

Nincsenek hozzászólások.

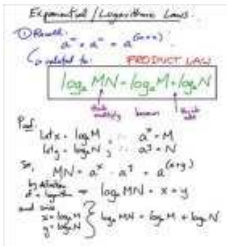
És akkor a logaritmussal egyszerűsítünk...

2008.10.22. 16:29 | Csizmazia István [Rambo] | 1 komment

Címkék: spam statisztika botnet emelkedés kártevő

Egyik kedvenc élményem a középiskolás matematika órán volt, amikor leányzó a táblánál **az egyenlet kétoldalát kívánta ilyetén módon emberformájúbbra alakítani**. Mi most viszont **az exponenciális növekedésről ejtünk néhány szót**, mert a kártevők terjedése világviszonylatban sajnos ilyen meredeken emelkedik :-(

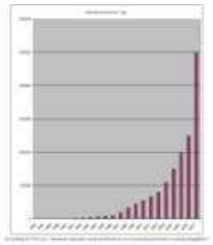
A ScanSafe friss tanulmánya szerint a vállalatok egyre növekvő veszélyben vannak az alkalmazottaik figyelmetlen letöltései miatt. Az energetikai iparban például 189 százalékos emelkedést figyeltek meg a webalapú kártevőknél, és jellemzően **egyes területeken ennél is magasabb értékek szerepeltek.** Volt, ahol a rosszindulató kódok száma **az idei év januári mennyiségéhez képest 500 százalékos** volt.



Ez persze annak is köszönhető, hogy már nem magányos harcosok küldözgetik ezeket, hanem **szofisztikált bűnszervezetek főállású profi programozókat alkalmaznak**, akik napi munkájuk során teszik egyre tökéletesebbé a kártevőket, illetve készítenek egyre újabb változatokat. A növekedés a statisztikák szerint augusztusban és szeptemberben kicsit "megpihent", hogy aztán az év végére még meredekebb görbét alakítson ki magának.

Ugyancsak kedden tették közzé a MessageLabs jelentését, melyben az adathalász támadások számáról is találunk adatokat. Ezek is egyre emelkedő tendenciát mutatnak, és a terítési napokon több tízezer ilyen spamlevél is kiküldésre kerül, amelyeket egyre többször igyekeznek **minél célzottabban** eljuttatni.

Ha **egyszer itt arról lesz bejegyzés, hogy lineárisan, sőt explonenciálisan, vagy akár logaritmikusan csökken a kártékony kódok mennyisége** a világhálón, akkor érdemes lesz majd ellenőrizni jó blogban járunk-e vagy egyszerűen csekkolni a naptárt, **nincs-e véletlenül április 1**.



Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/726175

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.04.30. 11:34:10

Egy érdekes poszt a Homárról, a szolgáltatónak meg nem válaszolt email miatt a böngészőben minden oldalnál egy s.php ugat be szanzsén:
homar.blog.hu/2009/04/30/az_externet_letiljta_az_internetet_ha_nem_valaszolsz

A kedvenc kommentem pedig ez volt :-)
"ennél már csak az a jobb, mikor még tyilifonosbetárcsázósratyifoschpuNpa netem volt, és 1ccer csak nem működött:(
hívtam az ügyfélszolg-ot, hogy vasz iz dasz páJa???? mondták, hogy egy hónap saram van előző évről, és kikaTsolták...
kérdezem: értesítő, valami, kapjam be, he????
küldtünk ma ímÉt, nem olvasta???
hogy a zanyádba olvastam volna, mikor kikapcsoltatok?????"

Botnet társam, óh mondd, akarsz-e lenni?

2008.10.27. 13:08 | Csizmazia István [Rambo] | 16 komment

Címkék: windows lamer wga kalóz exploit

A technika, a trükkös kártékony kódok egy dolog, **a felhasználók nemtörődömsége és bugyutasága** pedig egy másik - de ez utóbbi kétségkívül **a leggyakoribb oka annak, amiért a számítógépek áldozatul esnek**. Jó hír lehet viszont, hogy a hozzáállásunk ingyen és bérmentve változtatható.

A kínai felhasználók **nehezményezik a Microsoft új intézkedését**, amelyet a kalóz Windows példányok elleni harcban vetett be. Ez magyarul annyit tesz, hogy **a lopott, vagy udvariasan fogalmazva "nem legális" operációs rendszereken minden órában megjelenik egy fekete képernyő figyelmeztető szöveggel** a Windows Genuine Advantage új változatának köszönhetően.

Tekintsünk el most attól, hogy technikai tévedés miatt vakriasztásszerűen ez esetleg igazi, fizetős juzereket is zaklathat (ahogy tavaly nyáron ez elő is fordult), és találjuk ki, az intézkedés **milyen reakciót váltott ki? Elemi erejű tiltakozást**. Az egyik blogon a következő vélemény jelent - figyelem, Kretén magazinba illő idézet rulez: "Az én monitorom az én tulajdonom, a Microsoftnak nincsen joga a beleegyezésem nélkül irányítani az én hardveremet!" LOL! Szóval semmi, "Hja igen, lassan gondolkodok már azon, hogy esetleg mégis fizessek a lopott oprendszerért", vagy "Most már nem halogathatom tovább, ideje átállnom az ingyenes Linuxra", vagy ilyesmi. **Én nem vagyok hibás, csak a világ, a mocskos szoftvergyártók folyton zaklatnak engem, szegény ártatlant**. Lassan Kínában is rá kell majd írni a mikrosütőre - mint Amerikában - hogy tilos benne nedves macskát szárítani ;-)

Ennek fényében **el lehet képzelni a biztonsági frissítések ottani naprakészségét**, amely a kivédhetetlen nulladik napi exploitok mellett egy rakat régebbi - akár több éves - sebezhetőséget kínál fel tálcán a támadóknak, és felelős az egyre szaporodó fertőzésekért.

Egy fiataloknak szóló oldalon - talán kissé nyersen, de lehet hogy ide pont ez kell - **próbálják megtörni az "én csak egy hétköznapi ember vagyok, velem nem történhet semmi" téveszmét**. Csak remélhetjük, hogy **a felvázolt forgatókönyvek elgondolkodtatják** a többséget. (Ugyanakkor persze a jólinformált és nagyon is hozzáértő kisebbség egyre tudatosabban piszkálja és deríti fel a határokat, egyre több iskolai rendszer esik áldozatul olyan diákoknak, akik a gyenge ellenőrzést, a csapnivaló biztonsági körülményeket kijátszva manipulálják saját jegyeiket, esetleg jó pénzért másokét is, vagy az eltulajdonított személyes adatokkal történik valamilyen személyes bosszúállás és/vagy pénzkeresés.)

Többször hallottam már, de különböző fórumokon is megy időnként a flamewar, ahol vannak olyan beszólók, akik **azt bizonygatják, ők aztán egyáltalán nem használnak semmiféle vírusirtót, kémirtót meg ilyesmiket. A kártékony kódok "csak a h□lyéket támadják meg"**, őket nem, meg hogy az "csak a gyengék fegyvere". (Persze itt nem *nix és Mac platformról beszélünk, hanem szigorúan Windozerről.)

□alán mégsem olyan jó és kifizetődő dolog, hogy h□lyének lenni állampolgári jogunk. Nem tudom mi lenne a jó megoldás, talán sok CS□t és 24 óra epizódot kellene nézetni az emberekkel, hogy fejlődjön a logikus gondolkodásuk, tudatosságuk és az empátiájuk? Passz.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/733677

Kommentek:

cworm □törölt□ 2008.10.27. 13:□0:37

Én aztán egyáltalán nem használok semmiféle vírusirtót, kémirtót meg ilyesmiket. A kártékony kódok csak a hülyéket támadják meg!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.27. 14:33:39

:-)))

buherator · http://buhera.blog.hu 2008.10.27. 1□:03:20

Idevág:
ha.ckers.org/blog/20081022/security-expert-rehabilitation/

payskin 2008.10.27. 23:24:23

Eh, cworm ellőtte, így csak csatlakozni tudok. Vírusirtót, kémirtót meg ilyesmiket lassan egy éve nem, a kártékony kódok lepattannak a tűzfalról. Ha a jövőben mégis bejönne valami, ami majd megfertőz, csináltatok egy ÉN IS HÜLYE USER VAGYOK feliratú pólót, és emelt fővel fogom hordani.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.28. 08:□7:23

Köszi Buherátor, ez jólesett X-DDD

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.28. 09:08:□1

Szia TRf :-) Köszi, hogy idelátogattál!

Nem téged akart bántani a post, erről szó nincs. Te nem vagy sem felelőtlen, és konyítasz is a dologhoz. Ha pedig valaki elmeköszörülés okán kísérletezik - pláne úgy, hogy tudja is mit csinál pontosan, az az én szememben maximálisan szimpatikus -

én is szeretek olykor járatlan utakon csámborogni.

Mondjuk az igaz, hogy a tapasztalataim mások - volt, hogy emberemnek telepítettem és kérte, az AV legyen az uccsó, hadd gondolkodjon melyik legyen. A vége az lett, hogy minimális netezés után (pl. TCommander download) után egy órán belül már bootolgatott a gépe Blaster miatt a vadiúj Win telepítés.

És végül a statisztikai vetület. Valaki csak tartozik ezekbe a botnetekbe, és biztos, hogy nem azok, akik naprakész KAV, Norton, ESET, stb cuccot hajtanak a gépükön. Kicsit olyan, mint a Havas Henrik könyve a pornóról: "Ha én se nézem, te se nézed, ő se nézi, akkor ki nézi egyáltalán? Mert mégis van" Hasonló a helyzet szerintem itt is, és ha tétre-helyre-befutóra kellene tenni, én akkor is védelem nélküli gépekre tolnám a zsetonjaimat.

gothmog 2008.10.28. 21:26:46

én ugyan nem használok se vírusírtót, se kémprogramok elleni védelmet. csak szép csendben ubuntuzok. :)
Aki meg arra nem képes, hogy kiiktassa a WGA-t, (vagy lopjon egy corporate kulcsot) az valszeg a linuxra való átállást sem fontolgatja.

□idi Rita · http://www.hosnok.hu 2008.11.01. 10:39:42

Úgy látom, megszólalt a felhasználói társadalom 15%-a.
Most akkor jöttem és felszólalnék a maradék 85% nevében: el sem hinnétek, hogy milyen alapvető információik hiányoznak a felhasználóknak.
Ha vannak információik, akkor azokat össze-vissza kutyulják.
Olyan hiányos alapokkal neteznek, hogy kérdezni is képtelenek.

Lehet, hogy Ti sosem voltatok ilyen szinten, max 5 éves korotokban, de a valóság már más. Nem csak a geekek és kockák neteznek.

Akik egy picit már a béka hátsójánál felsőbb szinten mozognak informatikailag, azok fejében már megfordult a Linux használata, de a hónapok alatt összecsipegetett információik kevesek ahhoz, hogy Linuxosak legyenek.

Kész, kör bezárult.
Senki nem akart botnet tagja lenni, ha egyáltalán tud ennek a létezéséről.
Na, visszatérek az enyéim közé:))

□ □ □törölt □2008.11.01. 22: □1: □2

én használok vírusirtókat meg ilyesmiket, de nem vagyok egy nagy expert az informatikában. ha átállok Linuxra, akkor kevésbé vagyok veszélyeztetett?

mennyibe kerül egy nod32?

én inkább úgy próbálom óvni a gépemet, hogy igyekszem tartózkodni a gyanús oldalaktól, gyanús dolgok letöltésétől.. de ez szinte lehetetlen..

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.04. 06:17: □7

Szia WUT!

Igen, jól gondolod, szerintem sokkal jobb helyzetben leszel, ha Linuxozol. Akkor már csak időnként kell körülnézned pl. Rkhunterrel rootkitek után. De ezek száma a Wines kártevőkéhez képest elenyésző. Kérdés persze, hogy a munkád során el tudsz-e szakadni teljesen? Pl. SAP, Adobe Flash Studio, stb. nem léteznek Linux alatt.

NOD32 árakat itt találsz:
www.eset.hu/vasarlas/arak

És igen, egyetértek azzal, amit írsz: "szinte lehetetlen."

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.04. 06:27:42

 Mindenki:

Az állatkertben háromméteres rácsot építenek az új kenguru területe köré, de másnap az állat kint ugrál a kerítés előtt. Erre hatméteres rácsot emelnek, de a kengurut megint csak kint találják. Az igazgató ekkor húszméteres rácsot rendel, de az állat ismét megszökik.

A zsiráf megkérdezi a kengurut:
- Szerinted milyen magas lesz a következő rács?
- Nekem aztán mindegy - feleli a kenguru - csak továbbra is hagyják nyitva az ajtót.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.04. 23:02:10

Emberi hülyeség ügyben egy kis borzongató adalék:
nethackz.com/how-dumb-can-people-be/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.0 07: :06

Nem gondolnám, hogy az újzélandi helyzet sokban különbözne az átlagtól:
www.stuff.co.nz/4778864a28.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.08. 1 : :

Na, egy iggggen tanulságos sztori Buherátortól a sok "nekem nem kö antivirus, és el akarok menni a piramidonokhoz..." típusú embernek:
buhera.blog.hu/2008/12/07/meg_egy_ok_az_av_k_mellett

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.17. 10:21: 3

Ez is egy horrorshow. Most nem csak azt akarom kihozni belőle, hogy na ezért kell naprakész vírusvdélem, hanem hogy az Egyesült Állatokban is mekkora lúzerségek történnek az úgynevezett "igazságszolgáltatás" keretében. Igaza volt apámnak, aki szerint "A bíróságok nem igazságot, hanem jogot szolgáltatnak". Szégyen, amit ezzel a tanárnővel műveltek. És ha 20 gyerek tanúskodott volna, akkor 200 éve lenne? Ezeke idióták :-O
www.kisalfold.hu/kitekinto/szex-tett_pornot_mutatott_a_gyerekeknek_a_tanarno/2091538/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.29. 14:31:47

Ha lenne ilyen versenykategória a Guiness rekordok évkönyvében, Dubai esélyesként indulhatna:
www.itp.net/news/554093-dubai-has-most-botnet-infections-in-middle-east

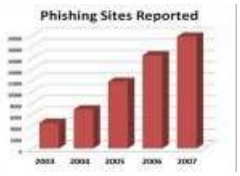
Pénzért mindent

2008.10.29. 16:05 | Csizmazia István [Rambo] | 8 komment

Címkék: pénz atm phishing óvatosság adathalász

Válság ide vagy oda, **könnyű és nehéz időszakban egyaránt kedvelt az adathalász tevékenység**, és remélhetőleg már mindenkinek a könyökén jön ki, hogyan is védekezhetünk ellene. De az sem mellékes körülmény, milyen etikettet követünk a valódi bankkártya használatnál.

A pénzünk, bankszámla adatainkért folyó versenyben **már megtanultuk, hogy a bankok soha (no never) kérnek tőlünk bizalmas személyi adatot e-mailben**, pláne nem jelszavakat vagy pinkódot. Aztán a bank belépőoldalnak látszó tárgyakat is hosszasan ecseteltük: **hasonló, csak éppen eggyel több mezőt kérnek be az űrlapon, és ez a plusz egy, hogy-hogynem éppen a pinkód ;-)**.



Aztán a csalók nem titkosított https oldalon próbálnak minket becsapni, vagy további haladócsoportos trükként hamis, lejárt vagy sajátmaguk által aláírt tanúsítványt használnak. **Nyugodtan emelje fel a kezét, aki a Tanúsítvány - Megtekintés - Részletek - SHA1 és M□5 hasht is rendre ellenőrizni szokta ;-)** Pedig nem butaság, mint ahogy a banki oldal IP címe (ShowIP plugin rulez) félszemmel való csekkolása is építőkockája a tiszta, száraz és biztonságos érzésnek. Ha nagyon szigorúak akarunk lenni, még emellett is van esélyünk arra, hogy ellopják a sütinket (cookie) és egy másik gépen reprodukálják a sessiont, mindenesetre a NoScript használatával kimerül az, amit magunk részéről megtehetünk, innentől már "In God we trust".

Hát ez volt eddig az egyik fele, de marad még **a bankkártyával való intelligens bánásmód**, ami tulajdonképpen pozitív gondolkodású emberi lényből paranoid agymenéses véglényekké degradál minket sokak szemében - de inkább ez, mint az anyagi veszteség az óvatlanság miatt. Murphyvel: "Inkább a borzalmas vég, mint a borzalmak vég nélkül."

A fenti kis videó jól összefoglalja a katonakoromban sokat hallott "Nincs lehetetlenség, csak tehetetlenség" jelmondatát: muszáj, hogy mi is fantázisdúsan találgassuk és alaposan **megismerjük, mit és hogyan tervezhetnek ellenünk, különben a védekezésben fényévekre lemaradunk**. Egy bizonyos Chao nevezetű török cracker már odáig ment, hogy komplett video oktató filmeket készített kezdő rosszfiúknak a tárgykörben. A tanfolyam még arramenően is **részletes tanácsokat adott, hol, milyen napszakban, milyen környéken érdemes telepíteni a trükkös eszközöket**. A csalók a javunkat akarják, ne adjuk nekik ;-)

Kártyás fizetéshez alaptételként néhány egyszerű, de fontos szabály:

- **Sose fizessünk úgy a kártyával, hogy azt a személyzet egy általunk nem látható helyre viszi**. A rosszindulatú tolvaj ilyenkor több mindent tehet: többször is lehúzza a kártyánkat, lemásolja a kártyánkat, illetve ha csak a kártya számát, lejáratát és a hátán szereplő utolsó három, úgynevezett ellenőrző számokat leírja, máris rendelhet a nevünkben az interneten bármit a mi kontónkra.

- **Minden ATM-ezéskor ellenőrizzük, nincs-e valamilyen szokatlan elem felragasztva az automatába**: kandikamera, hangszóró a felső részre, pénzvisszatartó keret a pénkiadó nyílásnál, extra gyűrű a bankkártya fogadó nyílás körül, stb. Ha pénzvisszatartó és/vagy kártya visszatartó keret van, akkor hiába várunk, ilyenkor rendszerint "egy segítőkész idegen" terem ott, és **javasolja, üssük be együtt a PIN kódunkat** vagy elirányít minket, hol tudunk reklamálni. Ő persze marad még, és innen már kitalálható a folytatás: és nem, nem az "álmában csönget egy picit"-tel folytatódik...

- Egyáltalán ne fizessünk kártyával (hehe, jól van na, ez most csak vicc volt;-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/738556

Kommentek:

szilárdan... · http://□ □.flickr.com/photos/haazee 2008.10.29. 18:14:17

Nem árt, ha legalább két számlája van az embernek.
Az egyikhez kártya, rajta épp csak az elköltendő összeggel.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.□1. 19:□5:07

Szia Szilárdan...!
Létezik úgynevezett webkártya, amire a tranzakció előtt 5 perccel utalsz, és bátran megadhatot a számát bárhol, nekem ilyen van és bevált.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.□1. 19:□5:□9

Ez is jópofa, ez ellen aztán végképp nincs orvosság:
www.penzcentrum.hu/cikk/1014313/1/vigyazz_mit_mondasz_egy_banki_call_centeresnek_megutheted_a_bokad

törölt-felhasználó (törölt) 2008.11.05. 01:10:4□

Lenne, de mai profitorientált világunkban a bankok (és ide tartoznak a netszolgáltatók, telefontársaságok és minden hasonló szogáltató is) nem engedhetik meg, hogy olyan sok embert alkalmazzanak, bőven jó a mindenes Micike is. Akár kis OKJ-s képzéssel még technikus, operátor vagy rendszergazda is lehet belőle. :D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.0□.19. 12:47:01

Ha már a gyárban vagy fejlesztőknél le lehet fizetni embereket, akkor nincs mit várni a biztonságtól :-(
www.virushirado.hu/hirek_tart.php?id=1460&ref=hl

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.06. 12:49:19

Lassan az ember nem tudja, merje-e még jószívvek ajánlani a NoScriptet :-O Azért egyelőre maradunk még a fedélzeten, de nagyon nem volt egy szerencsés húzás
www.hwsw.hu/hirek/38763/firefox_mozilla_noscript_adblock_hirdetes_online.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.10. 15:18:24

Éljünk egyszer mi olyan fényesen, hogy csak hónapok után vegyük észre, ha valaki már hónapok óta tőlünk vonatja le Mercedesze törlesztőrészleteit :-) Azért kezeket a paplan fölé, és egyesen a bankkártyánkat szorítsuk vele jól magunkhoz ;-)
www.penzcentrum.hu/cikk/1017753/1/durvan_lehuztak_az_alkoholista_sztart_kocsit_vettek_a_hitelkartyajaval

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.09. 10:02:1□

Éppen vacsorázott, mikor megcsapolták a bankszámláját:
www.mno.hu/portal/648722

Jó estét az EstDomainsnek

2008.10.30. 12:54 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam domain malware estdomains icann registrator

Szakmai körökben már régóta ismerik a hírhedt EstDomains "munkásságát". Nagy számú **spam- és kártevőterjesztő oldal regisztrálásában részes céget** több antivírus vállalat is tudatos felelőtlenséggel vádolja. Nem utolsósorban **rengeteg hamis antivírust terjesztő weboldalt** is náluk jegyeztek be. Most végre lehet, hogy **végleg becsöngetnek nekik**.

Kártékony oldalak ezreit lehetett könnyen bejegyezni az EstDomainsnél. A problémáról többek közt Mikko Hypponen is részletesen beszámolt a blogoldalukon. Úgy tűnik, végre valahára **sikerül végetvetni ennek az ámokfutásnak**. Ha egy cég vezető tisztviselőjét elitélik, akkor az ICANN (Internet Corporation for Assigned Names and Numbers) szabályai szerint felfüggesztheti működésüket. Az EstDomains cég vezetőjének, Vladimir Tsastsint zűrös ügyletei miatt februárban elítélték Észtországban **hitelkártyacsalás, pénzhamisítás és pénzmosás vádjával.**

A mostani döntésen az általuk jegyzett 281 ezer, köztük rengeteg kétes bejegyzés sorsa múlik, **elveszik tőlük ezeket**. Bár a felfüggesztés eredetileg november 12-én megtörtént volna, azonban az EstDomains fellebbezett arra hivatkozva, hogy azóta már Tsasin lemondott a posztjáról, így emiatt most **ez a lépés valamennyi ideig még csúszni fog**.

Lehet, hogy ezúttal KO lesz a vége...

Mindenesetre örömmel látjuk az ilyen irányú lépéseket. A probléma összetett, ezért az ellene hozott lépéseknek is **átgondoltnak, összehangoltnak és mindenre kiterjedőnek kell lennie**. Szurkoljunk ennek együtt!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/740075

Kommentek:

Nincsenek hozzászólások.

Védelmi pénzt fizetünk az interneten

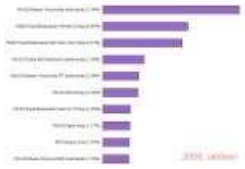
2008.10.31. 09:51 | Csizmazia István [Rambo] | 5 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

A NOD32 antivírus rendszert gyártó ESET **Magyarországra vonatkozó statisztikái szerint októberben lassú átrendeződés** kezdődött a legelterjedtebb károkozók listáján.

A mezőny kiegyenlítődését jelzi, hogy a listavezető Virtumonde elterjedtsége közel 3 százalékkal visszaesett, a top10 fertőzés pedig a szeptemberi 35 százalékkal szemben október során együttesen csak a fertőzések 30 százalékáért volt felelős. Emellett **két új szereplő - az e-mail üzenetek mellékleteiben terjedő Win32/Qhost féreg, valamint a Win32/Adware Antivirus2008** - is felkerült a listára.

A Win32/Adware Antivirus2008 bekerülése egy érdekes fenyegetés terjedésére hívja fel a figyelmet. A károkozó látszólagos támadást szimulálva arra **próbálja rávenni a gyanútlan felhasználókat, hogy egy hamis antivírus programot telepítsenek**. A kitalálók azt ígérik, hogy az álprogram segítségével megtisztíthatják számítógépüket. A programcsalád **fő célja a haszonszerzés**: a felugró figyelmeztetésre kattintva a rémült felhasználó a terméket árusító oldalra jut, ahol azonnal ki is fizettetik vele a szoftvert. A csalók **az elnevezésre is ügyeltek: az XP Antivirus 2008, 2009 és hasonló "terméknevek" kiválóan alkalmasak a megtévesztésre**.



Ha a program egyszer - akár véletlenül, akár tévedésből - felkerült a számítógépre, elindul a véget nem érő ijesztgetés. Az **álvírusirtó esetenként olyan hamis képeket jelenít meg** a képernyőn, mint a lefagyást jelző kék halál (BSOD, Blue Screen Of Death) vagy egy kémprogramfertőzésre figyelmeztető ablak. **A számítógép ellenőrzése is csak színjáték: sok esetben egy animáció, amely mindig talál fertőzést.**

Végül következzen **a magyarországi toplista. Az ESET statisztikai rendszere szerint októberben** az alábbi 10 károkozó terjedt a legnagyobb számban:

1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége az októberi fertőzések között: 7.94%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET kategorizálása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

2. WMA/TrojanDownloader.Wimad.N trójai
Elterjedtsége az októberi fertőzések között: 4.96%

Működés: A Wimad.N egy trójai letöltőprogram, amely a Win32/Adware.PlayMP3Z vírust telepíti a PC-re. A kártevő úgy kerül a számítógépre, hogy a felhasználó figyelmetlenül elfogadja a licencszerződést, amellyel egyúttal jóváhagyja a további tartalmak letöltését. Az Adware programok általában azáltal válnak ingyenessé, hogy cserébe bele kell egyezni, hogy reklámokat jelenítsenek meg a gépünkön.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-wimad-n

3. WMA/TrojanDownloader.GetCodec.Gen trójai
Elterjedtsége az októberi fertőzések között: 4.61%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki .letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files \ VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben, és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja:

.A felhasználó maga telepíti..

Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

4. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége az októberi fertőzések között: 2.39%

Működés: Az Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró-adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/toolbar-mywebsearch

5. Win32/Adware.Virtumonde.FP alkalmazás
Elterjedtsége az októberi fertőzések között: 2.09%

Működés: Ez a kártevő szintén a kéretlen alkalmazások táborába tartozik az ESET kategorizálása szerint. Futása közben különféle felnyíló ablakokat jelenít meg. A trójai megkísérel egy távoli szerverhez csatlakozni, és onnan további komponenseket letölteni.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/adware-virtumonde-fp**

6. Win32/Qhost féreg
Elterjedtsége az októberi fertőzések között: 2.04%

Működés: Ez a fenyegetés fertőzött e-mail üzenetek mellékleteiben terjed. Futása esetén bemásolja magát a számítógép Windows\System32 mappájába, ahonnan a következő rendszerindításkor igyekszik a DNS, vagyis a Domain Name Service működését megzavarni. Mivel a drivers\etc\hosts fájl tartalmát módosítja, képes teljesen elérhetetlenné tenni bizonyos weboldalakat. Ezenkívül a támadók a fertőzött számítógép felett távolról teljes mértékben átvehetik az irányítást.

A számítógépre kerülés módja: e-mail üzenetek mellékletében terjed.
Bővebb információ: **http://www.eset.hu/virus/qhost**

7. Win32/TrojanDownloader.Swizzor.D trójai
Elterjedtsége az októberi fertőzések között: 1.58%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat töltöget le és telepít. A Swizzor.D terjedéséhez a hiszékenységet is kihasználja: olyan programokba szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a „csomagban”. Ha a Documents and Settings\User\Application mappán belül találunk egy „DVDAUDIO” könyvtárat, az is árulkodó jel lehet.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/trojandownloader-swizzor-d**

8. Win32/Agent trójai

Elterjedtsége az októberi fertőzések között: 1.57%

Működés: Ezzel a gyűjtőnévvel azokat rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti
Bővebb információ: **http://www.eset.hu/virus/agent**

9. INF/Autorun vírus
Elterjedtsége az októberi fertőzések között: 1.54%

Működés: INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár .mp3 lejátszókon) terjed.
Bővebb információ: **http://www.eset.hu/virus/autorun**

10. Win32/Adware Antivirus2008 alkalmazás
Elterjedtsége az októberi fertőzések között: 1.50%

Működés: A Win32/Adware Antivirus2008 egy olyan kártevő, amely a gépen felbukkanó hamis riasztási ablakkal próbálja rávenni a felhasználót a kártékony, hamis vírusirtó letöltésére és telepítésére. Egész arzenál létezik már különféle neveken az ilyen programokból. A teljes verzió megvásárlása azonban nem oldja meg a mondvacsinált problémát, csupán a csalókat gazdagítja.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: **http://www.eset.hu/virus/adware-antivirus2008**

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/741830

Kommentek:

FK 2008.10.31. 16:06:52

Azt nem értem, hogy még hátra van 1 nap októberből, akkor honnan tudjátok, hogy egy fertőzés például 1,54%-ot okozott októberben? Ha még a hónapból 3% hátra van, akkor ilyen pontossággal kiírni nincs sok értelme (időgép nélkül)! Miért nem lehet például megvárni a tárgyhó végét egy statisztikával? Így nehéz komolyan venni :D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.31. 17:04:50

Kedves K. Ferenc!

Igyekeztünk, hogy még a halottak napja előtt megjelenhessünk vele.

A gigantikus vírusjárványok kora (pl. Sircam, Blaster, stb.) már lejárt. Igazából nagyszámú mintán alapul a statisztika, ezért szerintem bár a számokat valamennyire igen, de a tizes lista elemeinek az arányát nem igazán változtatja meg ez az egy nap.

FK 2008.10.31. 18:30:39

Halottak napjának mi köze lenne hozzá? Csak kíváncsiság. De köszi az infót!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.10.31. 19:20:23

Ünnepnap nem dolgozunk, és most a hónap vége után pont az jön... Direkt kapcsolat természetes nincs.

Fall 2008.10.31. 19:22:09

Gondolom annyi, hogy a hétvégén nem arról lesz híres kicsiny hazánk internetező közössége, hogy a gép előtt görnyedve blogokat olvasgat és ír. Gondolom a blog tulajának is van szomorú elfoglaltsága a hétvégén.
Másrészt sokan a PCWORLD honlapjáról jutnak ide, ahol pár új bejegyzés után eltűnik ez a bejegyzés is, anélkül, hogy elérné a célját: a figyelmeztetést.
Kissé furcsa vélemény, hogy ha nem várják meg a hónap végét eme statisztikával, akkor komolytalan lenne a dolog. Egy nap ebből a szempontból nem oszt, nem szoroz. Maximum pár századnyi eltérés lehet a fent közöltektől.

Hello Kitty a Design Centerben

2008.11.03. 21:12 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: design rajzfilm figura center antivirus

Ezúttal kicsit könnyedebb vizekre evezünk, rovatunkban **az antivírus piac különleges** érdekességeiből szemezgetünk.

Jóárasítás a hipermarketben
Tesco gazdaságos szoftver: **ez is egyfajta gyűjtő kategória vékony pénztárcájúaknak.** Létezik ebből irodai office csomag, rajzoló program, **és természetesen vírusirtó is**. Ha valaki nem elégszik meg az ingyenes programokkal, de nem is akar vagy tud sok pénzt ráfordítani, annak lehet érdekes az álruhába öltözött Panda program. A kép egy külföldi áruház polcán kapható termékről készült.

Édi-bédi, amely a géped védi
Még hogy nem gondolnak a fiatal lánykák gépeinek védelmére! Ahogy **nálunk a Tibi csokikra költözött a Macskafogó szereplő gárdája**, néha a vírusirtók is készítenek ilyen különleges terméket. Valódi rózsaszín leányszobákba való antivírus – talán így jellemezhetnénk legjobban a **Hello Kitty képével ékesített program** dobozát. Nálunk sajnos nem jelent meg Magillás vagy Mézga Aladáros antivírus ;-)

Én a vizilovakkal vagyok
2006-ban az F-Secure a finn Mommin mesefilm kis fehér viziló figurájával igyekezett **népszerűsíteni Internet Security csomagját a fiatalabb generáció körében**. Magyarországon hétről-hétre a Duna Televízió műsorán lehetett találkozni a Moominokkal. Ezek a mesefigurás termékek talán közelebb hozzák a legfiatalabb generációkhoz a számítógép védelmének az igényét, hiszen ebben a tekintetb ők számítanak az egyik legsebezhetőbb korosztálynak.

Ha valaki esetleg **ismer további hasonló** rajzfilmfigurás AV progit, írja meg nekünk a kommentek közt!

Ajánlott bejegyzések:

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/748166

Kommentek:

Nincsenek hozzászólások.

Fertőző Halloweenes weboldalak

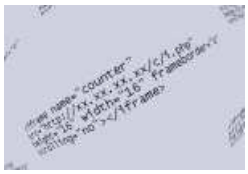
2008.11.04. 23:03 | Csizmazia István [Rambo] | 2 komment

Címkék: halloween malware javascipt

Van, aki nem ijed meg a Halloweenes vigyorgó töklámpásoktól, és alighanem jól teszi. Viszont a legfrissebb felmérésekből az derült, voltak események, amik mégis adhattak okot némi félelelmre.

A Websense Security Labs ThreatSeeker Network figyelt fel rá, hogy az ünnep alatt tömegesen megfertőztek ilyen témájú weboldalakat **JavaScriptes kártevővel**. Nyilvánvalóan belekalkulálták, hogy **kiemelt látogatottság** várható az ilyen helyeken. **Vétlen kereskedők, akik kihasználták az ünnep adta extra reklámlehetőséget**, és átalakították oldalaikat, hogy népszerűsítsék áruikat, boltjaikat.

Sajnos nem vették észre, hogy **a kódba bekerült egy olyan átirányítás**, amely rosszindulatú, gpack exploit készletes oldalakra irányította át a gyanútlan látogatókat. **Több, mint tizenháromezer ilyen, hasonlóan összezavart kóddal operáló weboldalt sikerült beazonosítaniuk**. Emellett azt is tapasztalták, hogy **proxy szerverek használatával** igyekeztek elkerülni a hagyományos URL szűrési megoldásokat.



Úgy tűnik, **a jövő egyik meghatározó veszélye** címért a JavaScriptes kódok keményen ringbe szálltak.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/750227

Kommentek:

törölt-felhasználó (törölt) 2008.11.05. 01:47:42

Usermódban futó böngészőnél a rendszerre ritkán van kihatással. A saját kis "homokozójában" tud csak futni az ártalmas kód. Vagy rosszul tudom?
Adatokat meg csak akkor lophat, ha olyan helyről lépek be, ahol a forrásban már benne van a kód. Ha az URL mezőbe közvetlenül írom a címet, vagy könyvjelzőből lépek oda, akkor nem ékelődhet be, ha csak a böngészőnek nincs erre vonatkozó biztonsági rése.

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.11.05. 21:47:57

Hát veszély szerintem mindenképpen van, gondolj csak arra, hogy scripptel akár el lehet lopni a cookikat, és akkor egy másik gépen belépve folytatható a sessionöd.

Buherátornal vannak mindenféle érdekes esetek, pl. ez is egy ilyen:
buhera.blog.hu/2008/09/11/sutiszorny_1

Klassz a Chrome blogot, szépen megcsináltad, gratula :-)

Vadászidény botnetekre

2008.11.05. 21:19 | Csizmazia István [Rambo] | Szólj hozzá!

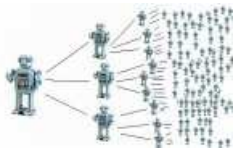
Címkék: botnet honeypot mézesbödön bothunter

A BotHunter nem kevesebb ígér, mint **hatékony botnet felderítést a hálózati forgalom elemzése alapján**, mindezt Window, Linux és MacIntosh platformon.

A mostani 1.0.1-es verzió **gyorsabb és még megbízhatóbb** botnet felderítést biztosít a fejlesztők szerint. A **dinamikus frissítés** gondoskodik az új szabályok felvételéről és a feketelista egyszerű bővítéséről, valamint a program továbbfejlesztett **grafikus felületen mutatja meg a fertőzött számítógépeket**.

A BotHunter a hálózati forgalom lehallgatása és ezen adatok értékelése alapján dolgozik, **számos technikát és jellemzőt képes azonosítani**, mint a DNS machinációk vagy például a Russian Business Networkre jellemző IP adatok alapján. Közben igyekszik megtalálni a vezérlés forrását, magát a botnet pásztort.

Számos mézesbödön (honeypot) szolgáltat érdemi információt a frissítésekhez, melyek közül sokat a program készítői, az SRI International tart fent. A projekt támogatói között olyan neveket találunk, mint például az US Army Research Office (ARO).



Az eszköz egyébként nemcsak több platformon futtatható változatban, hanem **telepítés nélkül használható bootolható Live CD formátumban is** letölthető a készítők weboldaláról.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/752776

Kommentek:

Nincsenek hozzászólások.

32 millió forint bevétel hetente

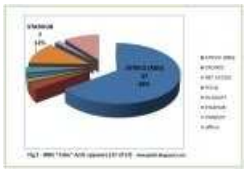
2008.11.06. 21:25 | Csizmazia István [Rambo] | 12 komment

Címkék: russian business hamis botnet antivírus network rouge

Nem mindenkinek kell **aggódó pillantásokat vetni a hónap végén a postaládába érkező sárga csekkek** miatt. Egy **heti 158 ezer dolláros kereset** már igazán nem számít rossznak. Találgassunk együtt, **mi lehet ez a remekül jövedelmező szakma**: agysebész, politikus, rocksztár, sportoló?

A helyes válasz egyik sem. A **megoldást a hamis antivírus programokat terjesztő orosz bűnözőknél kell keresni.** A hamis fertőzésekkel riogató Antivirus XP 2008, 2009 és hasonló nevű társaik felbukkanó popup ablakokkal, visszatérő vásárlásra buzdító figyelmeztetésekkel operálnak, és minden megvásárolt teljes program verzió 49.95 amerikai dollárt hoz a konyhára. Vicces módon már az Antivirus 2010 is megjelent már.

Az orosz botnetek segítségével igen hatékonyan tudják terjeszteni a fertőzést és növelik a saját profitjukat. Egy ilyen támadásokban résztvevő Bakasoftware nevű cégnél dolgozó egyik **bűnöző 158 ezer dollárt kasszíroz egyetlen hét alatt**.



A **PC World novemberi számában egy részletesebb cikkben is bemutatjuk** a hamis antivírus programok működését a Virusok Varázslatos Világa sorozatban.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/754646

Kommentek:

keeroy · http://music.blog.hu 2008.11.06. 22:37:03

Itt bizonyosodik be századszorra is, hogy megfelelően marketing mellett teljesen mindegy, hogy milyen maga a termék. Már az sem szükséges, hogy egyáltalán létezzen. :)

Parasite 2008.11.06. 22:44:16

azok a legviccesebbek, amik megfertőzik a gépet, felugrik a reklám és már ajánlja is a programot amivel leszedheted. és gyakorlatilag semmi más nem tudja leszedni :D persze pénzért

AnyádnakPalánkot (törölt) 2008.11.06. 22:54:33

Azé' a számok sántítanak. Hetente találnak ~3000 embert, aki mind "megveszi" 50 dollárért az antivírusprogramot? Rossz pályát választottam..

Repülő Majom · http://www.kutyushop.hu 2008.11.07. 00:33:10

Akkor már inkább letöltöm torrentről ingyen a tört változatot :)))

lifelike 2008.11.07. 02:23:51

a tobbi antivirus fejleszto is neha csinal egy virust amit csak a sajat programja ismer fel

ez az uzlet benne

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.07. 07:03:07

Hello Parasite!
Van ám még ennél is viccesebb, amikor megveszed, de mégsem szedi le, és minden marad a régiben. Erre mondják a klasszikusok: "Ügyes" :-)

Pikk 2008.11.07. 07:06:55

Ez már a látszat valósága..

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.07. 07:08:43

@AnyádnakPalánkot:
Ha megnézed, akkor ez akár hasonló lehet a spamekhez, ahol az átlagemberek 1%-a nemcsak hogy elolvassa a Viagra, Rolex, egyéb shit levelet, hanem még rendel is belőle :-O

Rossz pálya: csak nem azt akarod ezzel mondani, hogy heti 32 gurigánál kevesebbet keresel? ;-)

különvélemény 2008.11.07. 07:10:50

AnyádnakPalánkot 2008.11.06. 22:54:33
"Azé' a számok sántítanak. Hetente találnak ~3000 embert, aki mind "megveszi" 50 dollárért az antivírusprogramot?"

Így van, ez kb. az internetezők 0.001%-a.
Hihetetlen lenne, hogy van ennyi hülye ember?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.07. 07:16:38

Hello Lifelike!

Ez a vád időről időre elhangzik, de - személyes véleményem szerint - nincs semmilyen valóságalapja.

Sok évet dolgoztam együtt KAV, FSAV emberkékkel, láttam nennyi minta érkezik naponta csak a VirusBuster és most a ESET víruslaborjába, hidd el, ezek az emberek megszállottan és elkötelezetten küzdenek ellene, és még így is szinte belefulladnak a napi többezer minta feldolgozásába...

bolczayhenrik (szervízút) (törölt) 2008.11.07. 08:38:27

Az egész vírustejesztéses biznisz a számítógépfelhasználók kiszolgáltatottságán alapul persze, ettől válnak ezek a mocsokszemetek olyan végtelenül hatékonnyá. Én pl. semmilyen szoftveres védelmet nem használok, csak hardveres tűzfalat, mert nálam mindig minden állandóan le van mentve, imázsból negyedóra alatt visszarakom pl. az installált XP-t, csontszáraz vinyóra is felrakom a működő rendszert mindenestül egy óra alatt, három gépet tudok indítani egyszerre itthon, és mégis... Ha néha bekapok egy ilyen szart, még én is belesápadok....

Azon szoktam tűnődni ilyenkor, mit érezhet az, akinek ilyen szintű védelme, ahogy a felhasználók nagy többségének, egyáltalán nincs...

Micsoda rohadékok között élünk...

nuart · http://nudeart.blog.hu/ 2008.11.07. 13:46:11

de szeretnék orosz fake vírus gazda lenni

egy hónap elég is lenne belőle

Dr. Antivirus benézi a Mac-et és a Linuxot

2008.11.07. 21:06 | Csizmazia István [Rambo] | 9 komment

Címkék: mac linux osx ubuntu hamis antivírus

Vicces látni, amikor **egy fehérköpenyes hamis antivírus program az alternatív operációs rendszereken küzd,** mint disznó a jégen. Ja igen, és fertőzött DLL-eket bír felfedezni, na és hogy Win32-es vírusokat is lel OS X és Linux alatt legott :-)

Kedvencünk az olyan hamis antivírus, **amelyik lejátssza azt az animációt, aminek eredetileg keresésnek kellene lennie**. Az eredmény? **Mindig ugyanazt látjuk**, és ennek aztán lehetnek tréfás mellékhatásai.

Indítsuk el **a fertőzött weboldalt Ubuntu Linux alatt**. A JavaScriptes ablakok persze jönnek, ezzel nincs is semmi hiba, de **a "szkennelés" eredménye azért itt elég érdekes :-O**

Csak a vicc kedvéért **egy Leopard OS X-es MacBookon is kísérletezünk egyet**, bár az eredmény már nem is kétséges.

Hurrá, **Windows kártevők fertőzték meg a MacIntosh gépet** - a Rapid Antivirus szerint. És persze ezt mi el is hisszük.

A tréfát félretéve az azért viszont **mindenképpen riasztó, amilyen agresszívan ezek a pop-up ablakok nyílnak**, nagy számban, sűrűn és rendkívül idegesítően. Fehérköpenyes doktorunk mindkét platformon bőszen lengeti szokásos idióta hamis riasztásait. **Talán kellene neki egy másik fehérköpeny, amely hátulgombolós** és igen hosszú ujja van, kacifántos madzagokkal ;-)

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/756233

Kommentek:

gothmog 2008.11.07. 21:48:03

Mindig sejtettem, hogy az ubuntu csak egy vindóz téma.
:O :) :D (LOL)
Klassz ez a háttérkép a León!

cworm (törölt) 2008.11.10. 09:56:57

Isten ments, hogy védeni akarnám ezeket a bűnözőket, de egyik ablakban sem az van, hogy íme ezeket a kártevőket találtuk a gépeden, hanem hogy TOP 10 threats for last week. Alatta a win-es cuccok felsorolva. Alatta pedig, hogy hány gyanús fájlt talált. Persze ez az egységsugarú júzert simán megtéveszti.:)

gothmog 2008.11.10. 17:49:04

hát, nem tudom, én egy animáció képeit látom, ami szerint szkenneli a "computert" és biztonsági hézagokat "talál", pl. 26 vírust, amiből 0-t sikerült "leírtani".
Na persze, a fejlécben csak annyit ír "may be infected", ami ugye feltételes mód.
A trükkös rész az, hogy ha a júzer csupasz seggel netez, akkor itt már meg is kapta a fertőzést. A biztonság kedvéért mindjárt többet is.
És amilyen viccesek ezek, azzal kezdik a ténykedést, hogy tiltják az összes igazi vírus/kémírtó cég oldalát/ip-címét. Igazán mókás, mikor beírod, hogy eset.hu, bejön az oldal, aztán egy másodperc mulva eltűnik, és kiírja, hogy "nem található". Persze én is csak azért vigyorogtam, mert más gépén láttam.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:37:21

Szia □othmog□

Igazságod vagyon, bár a piros Top10 ablakban az is ott van, hogy "Suspicious files found: 45" ami azért arra utal, azt sugallja, hogy nálam talált valami brejzlit :-O

Az a szomorú, hogy állítólag egy komplett programozói csapat fejleszti ezeket napi nyolc órában, és félő, hogy lesz még jó pár "remek" ötletük...

gothmog 2008.11.10. 20:22:57

Szia Rambo!
Hát, azellen nem tehetünk semmit. Amit tehetünk, hogy segítünk a népeknek a biztonságos nethasználatban -ha kérik-, meg terjesztjük az igét.
Nekem pl. 75%-al csökkentek a ráncaim, mióta Ubuntut használok. ;D
Bár lehet, nekem is kellene egy ilyen Rambós háttérkép, mielőtt túl nagy biztonságban érezném magam.;)

Konegafi (törölt) 2008.11.19. 22:22:30

az a rambós háttérkép nagyon ott figyel :D
léccilécci, linkelje már be valaki, ha lehet esetleg 1920x1200-as paraméretek mellett

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.20. 21:52:58

Szia Konegafi és Gothmog!

Közkívánatra az "Önök kérték, mi teljesítjük" rovatban ;-) következzen hát a nagyfelbontású Rambo 4 pix lelőhelye :-D
www.collider.com/uploads/imageGallery/Rambo_To_Hell_and_Back/rambo_writer-director_sylvester_stallone_at_work_on_the_set_of_rambo__filmed_in_thailand_l.jpg

gothmog 2008.11.20. 22:14:03

danke sőn - mondták a partizánok

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.06. 12:50:31

Ez is "jópofa"story :
index.hu/tech/biztonsag/pavir090205/

Spammelés Abszurdisztánban

2008.11.10. 10:09 | Csizmazia István [Rambo] | 25 komment

Címkék: spam reklám kéretlen herminabau

Következmenyék nélküli országunkban hiába vannak szabályok, törvények, bátran át lehet hágni azokat, úgysem történik semmi. A Herminabau (vagy Nemecsekesen herminabau) is így gondolja, és **okádja postaládáinkba a viccesnek gondolt** kéretlen reklámleveleket rendületlenül.

Biztos akad majd, aki azt mondja, hogy ez jópofa, meg "jaj de cuki ez az ungyuri-bungyuri kutyuska", őket biztosíthatjuk, nem az állatok szeretete hiányzik belőlünk, sőt. De hogy megrendelés (opt-in) nélkül **miért kell kéretlenül spameket küldözgetni**, mikor ezt ugye nem lehetne, és hogy ennek **a sokadik NHH-es bejelentés után se legyen foganatja, az már rejtély**.

Épp csak az hiányzik a végéről, ha én is nem küldöm tovább x darab ismerősömnek, elüt a villamos :-O Ez már perverzió: nem csak ők küldözgetik kéretlenül, még a címzett is tegye ugyanezt, és akkor "nagy-nagy szerencse" fogja érni!

A céges kreatív csapat persze minden tőle telhetőt megtesz, hogy érdekességet hozzon össze: egyszer egy vitorlás üti el a levélíró apját (véleményünk szerint ezt már annak gyerekkorában kellett volna;-), **most egy kutyától kapunk levelet, aki beszél, de mégsem Foxi Maxi a neve**; legközelebb már azon sem fogunk csodálkozni, ha egy ágytakaró vagy egy cipőkrémes doboz lesz a feladó - három sör után már Attila sírját is megtaláltatták velünk.

Sokféle üzleti modell létezik, és úgy látszik, **van aki arra gerjed, ha a Google-ba beírják a cége nevét, akkor minden találatban a spam szerepeljen**. Jó ez nekik?! **Kéne már valami elrettentő dolog, amitől legalább azok nem folytatnák a spammelést, akik névvel, címmel szerepelve élnek vissza a türelmünkkel**. Talán szegény Hobó kétségbeesett módszere beválna, ha már a jó szó falrahányt borsónak bizonyul.

Igaz, ettől még a kinyomozhatatlan Charlie Palmer, Milton Gardner, Hillario Mooney még ugyanígy idehányja nekünk a szemetét, de hát élet nem habostorta.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/759900

Kommentek:

OkoskaTo:rp 2008.11.10. 13:49:11

Mivel az NHH sajátos jogértelmezése folytán tojik komolyan rálépni a HermniaBau tökére, én már csak azt tartom célravezető próbálkozásnak, hogy a cég internetszolgáltatójánál köttetni le a teljes céget, weblapostul.

ex-dr. vuk • http://www.aisha.hu/ 2008.11.10. 14:01:54

Az NHH is altalaban csak 'figyelmeztet es felker a tovabbi jogsertes mellozesere', ahogy en tapasztaltam.
Sokra megyunk vele, eddig is tudtak h tilos.

Alf (törölt) 2008.11.10. 14:10:19

a szorongok pont hu meg az iwiwen spammel, de mint az őrült. minden nap kapok valami "cuki videó" - vagy "a barátom videója, szavazz rá plíz" linket valahova, amely az ő oldalukra vezet.

0xFFFF 2008.11.10. 14:10:37

Én visszairányítok minden spamet a postmaster@küldődomain.tld címre. postmaster címe mindenkinek van kötelezően :) ...a .hu zónában legalábbis.

0xFFFF 2008.11.10. 14:11:28

Ja, mindegyikhez teszek attachment-et is, hogy ne legyen olyan karcsú a levél :) ...és ez bizony automata módon megy, csak egyszer kell a domain-t felvennem a spammer listámra.

gitáros 2008.11.10. 14:32:55

0xFFFF:
és hányszor kapsz a mélerdémontól levelet a nemlétező cím miatt? :)

DjZoNe • http://djz.hu/blog/ 2008.11.10. 14:42:52

0xFFFF,
postmaster már nem kötelező. Csak akkor ha az adott domainnek van MX rekordja.

bicski 2008.11.10. 14:59:44

a probléma csupán annyi, hogy 500e Ft-ot szabhat ki az NHH.

egyébként teljesen egyszerűen tisztességtelen kereskedelmi gyakorlat miatt ajánlom felnyomni a céget a fogyasztóvédelemnél / GVH-nál is

konkrét pont: :
2008. évi XLVII. törvény
a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról

törvényi feketelista:
22. Annak valótlan állítása vagy olyan hamis benyomás keltése, hogy a vállalkozás nem a saját vállalkozásával, gazdasági tevékenységével vagy szakmájával összefüggő célból jár el, vagy egyébként hamisan fogyasztóként való fellépés.

továbbá agresszív kereskedelmi gyakorlatra és generálklauzulára kell hivatkozni.

Ha valakiben van egy kis kurázsi (pl a blog írója), nyomja már föl Őket

thx

dark future · http://□ □.□andocsek.hu 2008.11.10. 15:05:3□

Ezzel a posttal is csak reklámot csinálsz nekik!
A legjobb, amit tehet az ember, hogy olvasás nélkül nyomja az ilyen leveleket a kukába. Jogi fellépés... ugyan már.

□1A6H 2008.11.10. 15:13:45

0xFFFF
Az email From: mezőjének értékére visszairányítani nem túl bölcs dolog, ugyanis az esetek 100%-ában nem ő az igazi feladó, és így te is ugyanolyan spammer leszel, mint az, aki elküldte neked az eredetit.
Én már sokszor jártam úgy, hogy az én mail címemet hamisították feladónak, volt olyan eset, amikor 620MB visszapattant levelem érkezett rá.
Amúgy a témához szólva: ha a post szerzője bevágna ide egy mail headert, kiderülne, honnan küldték a levelet. Ha esetleg saját szervert használnak, azt feketelistára lehetne tenni.

31A6H 2008.11.10. 15:14:57

Még az előzőhöz, ha nem a From: mezőre irányítod vissza a levelet, hanem a postmaster címre, akkor meg egy ártatlan email cím tulajdonos még ártatlanabb szolgáltatóját szívatod vele.

OkoskaTo:rp 2008.11.10. 15:15:24

bicski: Az értelmezési kérdés ott van, hogy az 500e spamkampányonként, vagy bejelentésenként érvényes-e. Ha ugyanazon kampány kapcsánt tett több külön bejelentést nem egyetlen jogsértésként kezelne az NHH (hiszen több, különálló személy sérelmére történt), hanem egyenként, a bírság összege elég hamar megugrana pár nagyságrendet.

ehhh 2008.11.10. 15:31:38

www.domain.hu/domain/domainsearch/whois.html?
domain=2x.hu&ekes=2x.hu&crypt=mnpa3p0c3ns4ucbzly4jf7pdc7ekdbo0&code=jx3nc6k

movhu 2008.11.10. 15:33:21

Ugye az sms warez ugyanígy reklámozott:

mover.blog.hu/2008/09/25/spamiszony

Most mit vár az ember, amikor hirdetésben illegális letöltést lehet eladni?
A megoldás egyértelmű. A spamelő cégek éves árbevételéhez mért büntetés, ami 1%-nál nem lehet kevesebb, de akár elmehet 10%-kig.
SMS warez esetében pedig vagyonelkobzás.

bicski 2008.11.10. 15:40:37

szerintem egy államigazgatási ügynek minősül ha ugyanaz a tényállás (ugyanaz a hirdetés és egyszerre többen jelzik a problémát) és egyszer szabható ki az 500.000 Ft bírság. Ezt a törvény "közzététel" fogalmából vezetem le, ugyanis közzététel mind az egyedi címzettnek, mind pedig a nagyobb nyilvánosság számára történő közzététel, tehát nem egyénenként kell elbírálni, ha több személynek küldik is ki. Egyébként ez racionális, ugyanis magas a látencia.

egyébként nem értem, hogy miért ne lehetne elkapni a hermina bau-t. Szerintem kötelezést nekik, aztán utóvizsgálat és eljárási bírság, napi 1 misi

Hurrá Torpedó · http://□ □.youtube.com/□atch□v□br-D7□neS0□ 2008.11.10. 15:□5:□8

én a spameket, a spam mappába irányítom, a spam mappa naponta többször olvasás nélkül magam által törlődik. ha olyan kedvem van néha átfutom a feladókat.

volt már olyan hogy spamként érzékelte valakinek a levelét, pedig ismertem, mert hogy úgy írja a nevét hogy "bél@" persze nem béla, csak egy példa volt.

Avraham NetJézus (törölt) · http://tinyurl.com/a-zsido-valosag 2008.11.10. 15:50:19

31A6H :

Csak azt hagyod figyelmen kívül, hogy ez a 0xFFFF itt a mindentudó netszerte miközben csak egy word.

31A6H 2008.11.10. 15:53:55

Avraham, nem tudtam, új vagyok még.
16 biten viszont tuti a legnagyobb :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:09:18

@ OkoskaTo:rp:
Az ötlet tetszik, internet off, aztán majd csak észbekapna a kecsege :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:11:50

@Alf:
Csupa ismeretlen ír nekem is valami homályos szavazási púderral. Nekem a jó kis Erurópa Kiadó: Szavazz rám című nótája jut eszembe ilyenkor ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:15:04

@ 0xFFFF:
"Ja, mindegyikhez teszek attachment-et is, hogy ne legyen olyan karcsú..."
Csak nem extraméretű genitálékat ábrázoló, nevelő célzatú fotókkal ;-)? Az a baj, hogy egyáltalán nem lehetsz biztos benne, hogy valóban azt bünteted így, aki eredetileg küldte :-O

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:18:00

@Bicski:
Megpróbálok utánanézni, mit tehetek, rajtam ne múljon.
És a bejelentésenként 500 kHUF lenne valóban az elrettentő, a kampányonként számolt ugyanilyen összeg csak aprópénz, amit talán alapból bele is kalkulálnak az üzletmenetbe :-(

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:20:20

□ Dark □uture:
Nem egyszerű dilemma, mivel használsz többet, ha befelé sírsz vagy ha teszel valamit ellene :-O

Idevágó nóta a Ricetől: "Kiszívott nyakkal jött haza az én szerelmesem. Most megüssem vagy ne üssem, azon tűnődtem. Mert jól tudom, két pofon nem old meg semmit sem..."

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:2□:□2

@31A6H:
Ezen nem múlik, itt az emailcímemtől megszabadított fejléc:

From - Sun Nov 9 08:22:34 2008
X-Account-Key: account2
X-UIDL: GmailId11d72eae484fa18a
X-Mozilla-Status: 0001
X-Mozilla-Status2: 10000000
X-Mozilla-Keys:
Delivered-To: xxxxxxxxxxxx@gmail.com
Received: by 10.187.178.4 with SMTP id f4cs131389fap;
Thu, 6 Nov 2008 10:46:50 -0800 (PST)
Received: by 10.210.71.11 with SMTP id t11mr2815897eba.57.1225997209570;
Thu, 06 Nov 2008 10:46:49 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning pottom@2x.hu does not designate 195.56.151.67 as permitted sender) client-ip=195.56.151.67;
Received: by 10.68.53.32 with POP3 id b32mf775334ika.1;
Thu, 06 Nov 2008 10:46:49 -0800 (PST)
X-Gmail-Fetch-Info: xxxxxxxxxxxx@vipmail.hu 4 pop3.vipmail.hu 110 xxxxxxxxxxxx@vipmail.hu
Return-Path:
Delivered-To: xxxxxxxxxxxx@vipmail.hu
Received: (qmail 6662 invoked by uid 89); 6 Nov 2008 17:47:50 -0000
Received: from unknown (195.56.151.67)
by mail08.indamail.hu with QMTP; 6 Nov 2008 17:47:50 -0000
Received: (qmail 16744 invoked by uid 0); 6 Nov 2008 17:47:50 -0000
X-MessageCheck: 1801289383
X-Envelope-From: pottom@2x.hu
Received: from unknown (HELO firefly.hu) (193.202.63.221)
by mail04.indamail.hu with SMTP; 6 Nov 2008 17:47:50 -0000
Received: from localhost.localdomain (localhost [127.0.0.1])
by firefly.hu (Postfix) with ESMTP id A634A12E9E0
for ; Thu, 6 Nov 2008 18:47:56 +0100 (CET)
Date: Thu, 6 Nov 2008 18:47:56 +0100
To: xxxxxxxxxxxx@vipmail.hu
From: =?iso-8859-1?Q?P=F6tt=F6mke?=
Subject: Gazdit keresek!
Message-ID:
X-Priority: 3
X-Mailer: PHPMailer (phpmailer.sourceforge.net) [version 2.0.0 rc3]
MIME-Version: 1.0
Content-Type: multipart/related;
type="text/html";
boundary="b1_99e0c884a330a23902d437dd898f414f"
X-Scanned-By: MPP/Nod32 www.messagepartners.com
X-Scanned-By: This message was scanned by Indamail.hu
X-Scanned-By: MPP/Cloudmark www.messagepartners.com

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.10. 18:27:19

@Movhu!

Sajnos amikor nincs következménye a dolgoknak, akkor azok elfajulnak. Pedig tényleg kellene a szigorúság.

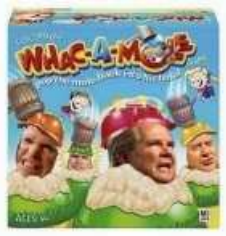
Nem tudhatod, másnak e szoftver mit jelent

2008.11.11. 15:33 | Csizmazia István [Rambo] | 1 komment

Címkék: download hamis ellenőrzés felelőtlenség shareware virusirtó

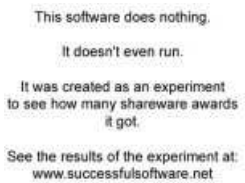
Régebben, ha le akartunk tölteni **az internetről egy programot, még talán számított** az "X weboldal szerkesztőinek ajánlata", vagy a "Best Choice", netán a "Tested Spyware Free" plecsni. **Manapság már nem ajánlatos** az ilyenekben vakon megbízni. Totális kaotika és **zűrzavar a letöltési oldalakon**.

A hamis antivírus üzletág virágzása és a letöltő oldalak nemtörődömsége együtt már átlépte azt a kritikus határt, ami **jobbára az egyszerű, tapasztalatlanabb felhasználókat veszélyezteti**. Még Randy Abrams is azon elmélkedik, hogy fordulhat elő a **download.com esetén, hogy olyan nyilvánvaló fertőző csomagok megjelenhessenek, mint az "Antispyware 2008"** vagy az "Antivirus Defender". Hát Google hirdetés formájában simán megjelenhet :-O De még ha pontosan tudjuk is, mit szeretnénk letölteni egy letöltő oldalról, **nem zárható ki**, hogy azok között olyan csomagba botlunk, ahol wrapperekkel beleforgattak a telepítőbe egy plusz kémprogramot vagy trójait, vagy pedig az általunk ismert néven egy ugyanolyan nevű, de hamis kémirtót kapunk a nyakunk közé.



Persze a gyártók és fejlesztők weboldala is áldozatul eshet elvileg valamilyen javascriptes "huncutságnak", de ennek az esélye azért jóval kisebb, mint **az elhanyagolt és napi 10-20-100 tételt mozgató ipari letöltő oldalaknak**. Mindenesetre emiatt is érdemesebb közvetlenül a fejlesztők weboldalát választani, ha tehetjük.

Sikerült végre megtalálnom az autentikus forrást, melyben főhősünk jó egy éve gondolt egyet, és a nagy semmit becsomagolva elküldte a letöltési oldalakra. A nagy semmi esetünkben egyetlen szövegfájlt jelentett - EXE-re átnevezve -, melyben a szerző nagyjából ezt írta:



"Ez a program egyáltalán nem csinál semmit. Sőt, még csak nem is fut. Azért készítettem, hogy kísérletezzek, vajon hány díjat nyer majd a shareware oldalakon. Az eredményt a www.successfulsoftware.com weboldalon teszem közzé."

De akár írhatta volna azt is, hogy **"aki ezt elolvassa, kap egy korsó sört" ;-)** És amint látjuk, **igenis lehet canis merga-ból várat építeni**, íme a **Brezsnyev mellkasát megszégyenítő díjtáblázat**, amiket a különböző letöltő oldalak szerkesztői adományoztak neki. Volt, amelyik még e-mailben is gratulált, hogy "Great job!" :-D

Persze **egy nagy semmit még mindig jobb letölteni**, mint egy nyilvánvaló kártevőt. Hát szomorú vagyok, mindenesetre az itt közölt felhívás - melyben e sztori forrása után kutattam - ezennel érvényét veszti, és mivel én találtam meg végül, ezért magamnak utalom ki a jutalom korsó sört ;-)

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/763254

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.12.08. 16:04:36

A semmi témakörében egy kis szilánk ugrott be még a középiskolából, adaléknak jó lesz :-)

"I have nothing to say,
and I'm saying it,
that is the Poetry..."

Online scan teszt

2008.11.12. 12:19 | Csizmazia István [Rambo] | 5 komment

Címkék: online virustotal scan jotti novirusthanks

Ha valamilyen gyanús fájl kerül a látókörünkbe, **sokszor élünk a több víruskeresővel dolgozó online ellenőrző oldalak segítségével, mint amilyen a VirusTotal** is. Ahogy víruskeresőkből sem mindegyik egyforma, itt is a régóta ismert, neves nagyobb oldalak nyújtják a megbízhatóbb teljesítményt.

A véletlen sodorta az utamba a NoVirusThanks.org weboldalt. Férfiasan bevallom, korábban nem ismertem, ezért el is kezdtem belehajigálni ezt-azt-amazt, amikor is legendás emlékezőtehetségem arra figyelmeztetett ;-), mintha **más korábbi vizsgálatoknál nem pont ugyanezeket az eredményeket** kaptam volna :-O

Nosza, néhány állománnyal párhuzamosan eljátszadozva világossá vált, hogy "a győztes csapaton ne változtass" elv alapján **aligha fogok elpártolni a jól bevált VirusTotal oldalról**. Igaz, hogy itt még a 2.7-es NOD32 programot futtatják a parancssori keresők között, de amúgy is meg szoktam nézni az új változattal élőben is, és ezt itt a blogban is meg szoktam említeni.

Most a bemutató kedvéért **a PC-Antispyware csomaggal végeztem az ellenőrzést**, és lőtéri zsargonnal szólva az "szórt, mint kecske a hegyoldalban".

Íme a véleményem szerint legkiforrottabb és legautentikusabb eredménylista a VirusTotal csapatától: **nincs benne egyetlen olyan értékelés sem, ami más oldalakon ennek ellentmondana**. Eltárolja a korábbi keresést a vizsgált fájl MD5 hashértéke alapján, ezért ugyanazt a fájlt nem kell újra megvizsgáltatni legközelebb, hanem azonnal megnézhetjük a legutóbbi eredményt.

A Jotti is régi ismerős, korábban még többet használtam, ez az oldal Debianon elérhető motorokat használ. Ezt a listát kapjuk a Jottis fiúktól: **Például szerinte a Panda és a VirusBuster nem észleli, míg a VT-nél és a NVT-nél egyértműen látszik** ennek ellenkezője. Ennyire különbözne a Windows és a Linux ellenőrzés eredménye? A korábbi vizsgálatok eredményei a VT-vel ellentétben itt látszólag nem őrződnek meg a nagyközönség számára.

És végül, de nem utolsósorban a NoVirusThanks teljesítménye: **Például a VT szerint az AVAST látja a kártevőt, a Jotti is ezt mutatja, itt pedig "Nothing Found!" üzenet** fogad bennünket.

Egy ősi közmondás szerint: "**Ha egyetlen órád van, mindig tudhatod, mennyi a pontos idő. De ha már kettő van, akkor sosem**

lehetsz biztos benne." ;-)

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/764978

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.02. 21:44:01

Érdekes, hogy van egy újabb hasonló oldal, de úgy tűnik, itt is egész más eredmény születik a VT-hez képest, például a Panda és a TrendMicro adataiban :-O
www.virscan.org/report/8cd8553d6c00524c40caec86e6126e97.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.02. 21:56:58

Revidálom a nézeteimet, itt most a különbség oka az időmúlás: azóta a kártevőt már felvették az adatbázisukba.

Akit érdekel, itt egy rakat, 60 különféle online scan gyűjtemény. A linkek tartalma egy sima ingyenes regisztráció után válik láthatóvá.
www.feloos.com/?p=1774

Algernon 2008.12.20. 23:34:24

Szia István!

Egy torrentről töltött "karaoke" file installja (magyarítása).
Érdekes:
www.virustotal.com/hu/analisis/0beaa46efd2ca8f135c7730576b4f239

www.virscan.org/report/e2a725ec16a6927de16eaaec4380c919.html

Hm...Ötlet?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.21. 20:18:18

Szia!

Itt a virscan.org-on valamit nagyon nem jól csinálhatnak :-O

Amit a VT-n simán detektál például az Avast, Kaspersky, Symantec, stb, az a VS-en meg látszólag hiányzik. Én VT hívő vagyok inkább, amúgy meg torrentről is be lehet szerezni a napi "betevő" malwaret ;-)

Arra gondolsz esetleg, hogy a "magyarítás" tiszta, és csak false positive lenne?

Algernon 2008.12.22. 22:48:32

Nem, csak csodálkoztam, hogy lehet ekkora különbség a VT és a VS között, mikor mindkét oldalon up-to-date-ek a keresők...

A Virscannál van egy olyan lehetőség is, hogy a legutóbb feltöltött kb. 30-40-50 (még nem számoltam meg) file keresési eredményét megnézheted. Nem lehetséges, hogy valamiféle "marketing-manipuláció" áll a háttérben? Bizonyos termékek naprakészen vannak tartva (mások nem), s így az egyszeri fogyasztót empirikusan meggyőzik egy-egy AV magas hatékonyságáról?
Vagy lehet, egyszerűen csak nagyon elbénáztak valamit...:)

Bacimentes ünnepeket!

Paypal phishing

2008.11.17. 14:47 | Csizmazia István [Rambo] | 4 komment

Címkék: kína paypal phishing

Talán a **nehéz gazdasági helyzet is hozzájárul**, hogy ismét felszállóágban van az adathalászat.

A PayPal rendszer **mindig is kedvelt célpontja volt** az efféle támadásoknak, mondhatni benne volt a Top10-ben. Nincs is ezzel a dologgal semmi baj, sokszor és sokat is beszéltünk már magáról a módszerről, és hogy e-mailben sosem érkezik ilyen kérés, stb.

Most inkább csak azt foglalnám így össze, hogy a gondos nezető ha jól választja meg a környezetét, és Outlook Express helyett Mozilla Thunderbirdet használ, hálából máris kaphat egy figyelmeztetést, miszerint ez egy gyanús üzenet.

Aztán ha ráadásként Mozilla Firefox ketyeg Internet Explorer helyett néhány egyszerű pluginnel, akkor béke van. Mert azért valljuk be férfiasan, **a hétköznapi ember az ilyen NoScript megoldásoktól sajnos viszolyog** és talán jogosan. Használatát nem segítségnek, hanem megpróbáltatásnak éli meg, **és csak a fejét forgatja a felugró ablakok vekzatúrája közben, kandikamerát gyanítva a közelben**. Az emberbarát NetCraft Toolbar viszont hatékonyan és csak a szükséges alkalmakkor adja kezünkbe az irányítást: bluepill or redpill. Igaz, ez a bejelentések alapján, tehát valamekkora késéssel teheti csak meg.

Azt már meg sem említem, hogy **az oldal meg sem próbál valamiféle betűcserével, vagy hasonló webcímmel operáni, ő egyszerűen a status-updates.com**, valószínűleg ezzel **jól cselezi ki az új domain regisztrációkat ellenőrző** fürkész szemeket.

Bár **a csalók az eredeti www.paypal.com oldal elemeit linkelték be**, az mindenesetre bizonyos, hogy a hivatalos PayPal center nem xianggangtebiexingzhengqu ország xianggangtebiexingzhengqu megyéjében fekvő xianggangtebiexingzhengqu városban fekszik és valószínűleg nem 2008.11.15.én foglalnak le Kínában egy külön adategyeztető weboldalt a 423@126.com e-mail címről ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/773667

Kommentek:

Sorkapocs (törölt) 2008.11.17. 15:42:08

Nálam az IE (legalábbis az IE7 és IE8b2) Netcraft Toolbar nélkül is jelzi, hogy nem biztonságos a cikkben szereplő cím. Az Opera 9.62 is jelez, viszont érdekes módon a Firefoxnak se a 3.0.4-es, se a 3.1b1-es verziója sem szól egy szót sem. Időközben eltávolították volna a listájukról az oldalt?

cworm (törölt) 2008.11.17. 16:07:31

"Aztán ha ráadásként Mozilla Firefox ketyeg Internet Explorer helyett néhány egyszerű pluginnel - mert azért valljuk be a hétköznapi ember az ilyen NoScript megoldásoktól sajnos viszolyog és megpróbáltatásnak éli meg, vagy csak a fejét forgatja a vekzatúra közben kandikamerát gyanítva a közelben."

Asszem valami nagy gáz van ezzel a mondattal, mert sehogy sem értelmes... És minimum egy vessző meg még egy gondolatjel hiányzik...:P

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.18. 10:44:58

@Sorkapocs:
Igen, jogos az észrevétel, az új IE már valóban tartalmaz ilyet, és persze nagyon sokan tartják a "legbiztonságosabb" böngészőnek az Operát, ami van Win és Linux alá egyaránt.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.18. 10:48:19

Szia Cworm!
Megműtöttem a mondatot, és remélhetőleg most már értelmes lett. Köszi a segítséget :-)

Elmebajnokság

2008.11.18. 12:36 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság jelszó lopás gondosság

Talán van aki még emlékszik az Egri János jéghokis/műsorvezető által jegyzett televíziós játékra, ahol az nyert, aki minél jobb memóriával rendelkezett. Sajnos manapság sokan vannak, akik **a jelszóválasztásuk egysíkúságával (mindenhol ugyanazt használják) és sekélyességével (abc123 szintű szavak, melyek szótárral percek alatt törhetőek)** igyekeznek memóriájukat egyáltalán nem használni.

Tegyük fel, hogy van egy felhasználónk, valamennyire érdekli is a számítástechnika, hébe-hóba olvas ilyen témájú portálokat, munkahelyén átfutja a Chip/PC World újságokat, hallott már adathalászatról, és a vírusirtó, kémirtó, személyi tűzfal szentháromságot is szépen használja a gépén. Ez eddig nagyszerű - bár itt tartana már mindenki - és ezzel **sikeresen meg is védi a _SAJÁT_ számítógépét**. De vajon az adataiért is megtett mindent? Ez már azon múlik, mennyire erős jelszavakat választott a különböző belépési helyein, és hogy **minden helyen másikat használ-e.**

Vannak olyan hasznos biztonsági szokások, amelyek mellőzését egyetlen vírusirtó vagy tűzfal sem kompenzálhatja, ez pedig **a használt jelszavak minősége, mennyisége és változtatási gyakorisága**, továbbá ezek gondosan és bizalmasan való kezelése. Ez egyrészt a vásárolt hardverelemek (pl. wifi router) alapértelmezett gyári jelszavainak azonnali lecseréréséből áll, de természetesen ide tartozik **a látogatott webhelyek, közösségi portálok, levelezések** belépési adatainak jól végiggondolt és biztonságos kezelése is.

Sokan gondolkodnak még úgy, hogy őket ez pont nem érinti, **az ilyesmi csak mindig mással történik** - ahogy a betörés vagy autólopás előtt is mindenki sajnálja a pénzt a drága többpontonzáródó bejárati ajtóra, riasztóra, aztán a baj megtörténte után minden átértékelődik, és hipp-hopp lesz pénz hevederzárra, rácsra, ajtócserére, riasztórendszerre. A mostani esetnél a **TYPO3.org webhelyén történt biztonsági incidens** - ellopták a userek adatait - után arra figyelmeztetnek az üzemeltetők, hogy kikerülhettek név-jelszó adatok, ezért ha valaki esetleg netalántán azonos accountot használ máshol is, azonnal változtasson. Az ilyen malőrök - például az SQL injection elterjedtsége miatt - az kell, hogy figyelmeztessenek minket, hogy tanuljunk a más kárán, és ne kövessünk el ilyen gyerekes hibákat.

Összefoglalva a jelszóval való törődés **nem azért van, hogy bosszantson minket**, hanem hogy sikerrel szolgáljon bennünket, amit meg is tesz, ha mi is gondosan állunk hozzá. **Ha rendszeresen cseréljük, kellően erőset választunk és nem ugyanazt használjuk mindenhol**, máris sokat tettünk - sajátmagunkért.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/775167

Kommentek:

Nincsenek hozzászólások.

Ingyen ebéd

2008.11.19. 15:03 | Csizmazia István [Rambo] | 6 komment

Címkék: microsoft ingyenes defender onecare

A Microsoft feladta azt az elképzelését, hogy a Live OneCare fizetős biztonsági szoftverével versenyezzen a többi vírusirtó program mezőnyében. Helyette **Morro kódnéven ingyenes alkalmazással** rukkolnak elő jövőre.

Két évvekkel ezelőtt is **lehetett sokakban egy ellenérzés, hogy ugyannarra a cégre bizza** az ember a számítógépe biztonságát, aki a "vírustanya" Outlook Expresst vagy a biztonsági lyukaktól hemzsegő Internet Explorer 6.0-t tette le korábban az asztalra. Akkor már **inkább egy számítógépes biztonságban profi thirdparty gyártó** alkalmazása felügyelje az életet, mint sem az MS úgynevezett biztonsági programja.

Ha megnézzük a korábbi elől, a Windows Defender és a OneCare hatékonyságát és szerepléseit a különféle teszteken, azt láthattuk, nem veszélyeztette komolyan az élboly életét, egyetlen McAfee, ESET vagy Nortonos vezér sem követett el ijedtében harakirit, hogy ettől kezdve munka nélkül fog maradni. És bár a Live OneCare igyekezett elmozdulni az átfogó kártevő védelem irányába, valószínűleg **mostanra belátták, nem képesek versenyezni az e területen** több évtizedes tapasztalatokkal rendelkező neves gyártókkal, fejlesztőkkel; **sem technikailag, sem pedig a piac frontján**.

A legfrissebb hírek szerint most az MS Morro szoftvere 2009-es esztendő második felétől lesz elérhető, és hanyagolni fogja az olyan komplett biztonsági csomagokra jellemző extra szolgáltatásokat, mint az adatmentés vagy a PC tunning, pusztán **a kártevő felismerésre és eltávolításra** fogja helyezni a hangsúlyt - és ezt ingyenesen fogja majd megtenni. Mindesetre majd **meglátjuk, milyen pluszokat tartalmaz a jó háromnegyedéves programfejlesztési munka a Live OneCare-hez képest** - hiszen ha a Morro ugyanaz lenne, elég lenne átnevezni és most azonnal piacra dobni. Kíváncsian várjuk a további fejleményeket.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/777747

Kommentek:

gothmog 2008.11.19. 18:22:01

Tényleg nekiálltak maguk biztonsági szoftvert fejleszteni? Ez furcsa. Náluk inkább az szokott lenni, hogy keresnek egy olyan céget, amelyik jártas a témában, és megveszik...

Algernon 2008.11.19. 22:37:46

Egy keveset azért fejlődtek tavaly óta:
www.av-comparatives.org/seiten/ergebnisse_2008_08.php

Egyébként pedig nem értem a fizetős vírusirtók felzúdulását. Ha valaki ingyenes irtót szeretne, nyugodtan választhatja az Avast!-ot, a fizetős mezőny nagy részét veri.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.20. 22:09:08

@Gothmog:
Biztos sántít egy kicsit a hasonlat, de ha mondjuk pl. a Suzuki most elkezdene a nulláról gumiabroncsot fejleszteni, sokan maradnának inkább továbbra is a Good Yearnél vagy a Michelinnél. Aztán ha a Suzukinak nem jönne be a bolt, és rendre lemaradna a teszteken, nem jönne az elvárt profit, ezért elkezdené ingyen adni utána a termékét, egy időre biztosan összetudná zavarni ezzel a "bedobom a gyeplőt a lovak közé, dögöljön meg a szomszéd tehene is, stb..." mentalitással. Igaz, hogy hosszútávon ezzel sem érne el semmit. De mint mondtam, várjuk ki a végét, mi lesz a programból, legyünk alapból bizakodóak :-)

@Algernon:
Az ingyenes progik közül valóban van néhány, amit én is jó szívvel ajánlok azoknak, akik nulla forintot szánnak erre a célra (pl. AVG), ez valóban jobb megoldás a semminél. Nyilván azt is bele kell kalkulálni, hogy egy fizetős terméknél a technikai support is egy olyan hozzáadott érték, ami miatt sokan például ez alapján vásárolnak.

amitlatok (törölt) · http://amitlatok.blog.hu/ 2008.11.21. 06:18:59

Majd meglátjuk, én maradok egyelőre az avastnál.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.24. 09:09:27

Közben az AVG az üzleti modelljének másolásával vádolja az M$-t ;-)
www.itnews.com.au/News/89706,microsoft-copied-us-avg.aspx

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.19. 21:51:03

Idézet ON:

"Magyar nyelvű verzió nem lesz a véglegesből sem, de az még kérdéses, hogy az angol verzió és a mögötte álló támogatás elérhető lesz-e itthon, és ha igen, milyen módon” – ismerte el Budai"

Idézet OFF

index.hu/tech/biztonsag/2009/06/19/a_magyaroknak_nem_jar_a_microsoft_virusirtoja/

Újabb tördöfés a Vistának

2008.11.21. 12:13 | Csizmazia István [Rambo] | 7 komment

Címkék: vista exploit sebezhetőség

Osztrák biztonsági kutatók olyan sebezhetőséget találtak a Microsoft Windows Vistában, amely a támadóknak **lehetővé teszi tetszőleges kód lefuttatását**.

A problémák a belső eszközmeghajtók kezelésénél vannak, és a Phion kutatói két különféle módszert is bemutattak a sérülékenység puffertúlcsordulásos kihasználására, amely képest volt az operációs rendszer kernelét megzavarni. Igaz, ehhez az egyiknél admin jogokra is szükség volt, de a szakértők szerint ez nem igazi akadály, hiszen a támadók rendszerint képesek ezt megszerezni.

De **lehetséget root jogok nélkül is végrehajtani** a támadást, amelynél tetszőleges kártékony kódot - például rootkitet - csepészhetnek be Tomas Unterleitner, végpont biztonságért felelős igazgató szerint. Cégük október 22-én értesítette a Microsoftot az észlelt problémáról, amire azt a választ kapták, hogy majd a Vista Service Pack 2-be fogják beépíteni a javítást. Ez **magyarul azt jelentené, hogy annyira lebecsülik a veszélyt, hogy 2009 nyaráig** - az SP2 megjelenéséig - nyitva maradna ez a sérülékenység a korábban "minden idők legbiztonságosabb operációs rendszerének" kikiáltott platformban. A kutatók szerint **máris nagy az érdeklődés az új sebezhetőség technikai részletei iránt**, hogyan is lehet pontosan kihasználni a nemrég felfedezett rést. A Microsoft eközben hivatalosan nem kommentálta az esetet.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/780721

Kommentek:

buherator · http://buhera.blog.hu 2008.11.21. 13:47:36

Kérdés: Távoli vagy helyi sebezhetőség?
Kötözködés: Ha van admin jogunk, akkor minek a csordítgatás?

buherator · http://buhera.blog.hu 2008.11.21. 13:51:46

Akkor válaszolok is: helyben kihasználható a probléma.

A reportban egyébként elég jó támpontokat lehet találni a kihasználáshoz, szerintem egy héten belül lesz nyilvános exploit:

securityvulns.com/Udocument888.html

buherator · http://buhera.blog.hu 2008.11.21. 13:54:11

Jólvan, csak lejjebb kellett görgetni: ott a PoC :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.21. 16:37:05

Hali!

Kötözködés jogos ;-)

Nem csak hogy egy héten belül ITW, hanem jövő nyárig szüret - hacsak az M$ nem korrigál...

Kazi (törölt) · http://redmond.blog.hu/ 2008.11.22. 00:44:53

A helyzet az, hogy ez úgy faszság, ahogy van, ugyanis a CreateIpForwardEntry2 függvény hívásához admin jog kell.

Idézet az eredeti leírásból:

www.securityfocus.com/archive/1/498471

"When adding a route entry to the IPv4 routing table using the method CreateIpForwardEntry2 and passing an illegal value greater than 32 [2] for the destination PrefixLength member in the DestinationPrefix structure contained in the MIB_IPFORWARD_ROW2 structure [3], kernel space memory is being corrupted resulting in random blue screen crashes."

A CreateIpForwardEntry2 függvény leírása az MSDN oldalon:

msdn.microsoft.com/en-us/library/aa814399(VS.85).aspx

"The CreateIpForwardEntry2 function can only be called by a user logged on as a member of the Administrators group. If CreateIpForwardEntry2 is called by a user that is not a member of the Administrators group, the function call will fail and ERROR_ACCESS_DENIED is returned. This function can also fail because of user account control (UAC) on Windows Vista and Windows Server 2008."

Itt a mese vége. Pont.

u.i.: egyébként a leguccsó linkelt cikk címe "A Vista minden idők legbiztonságosabb Windows operációs rendszere lesz", nem pedig minden idők legbiztonságosabb oprendszere. Nem ugyanaz.

charlie · http://blogocska.org 2008.11.22. 21:50:16

Kik azok az "Oszták biztonsági kutatók"?

Használj elgépelés ellenőrzőt legalább...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.23. 06:06:35

Köszi Charlie!

Gmail eltérítés

2008.11.24. 11:09 | Csizmazia István [Rambo] | 6 komment

Címkék: gmail hack exploit hijack noscipt godaddy.com

Van új a nap alatt, mindig sikerül rácsodálkozni az egyre újabb és furmányosabb trükökkre. Ezúttal emberünk bemutatja, **hogyan továbbít magának leveleket idegen postafiókból, és töröl ki az illető G-Mail-es Inboxából annak tudta nélkül**.

Ha valaki **képes megszerezni azokat a változókat, amelyek a levelezéskor a felhasználó nevünket reprezentálja** a Gmail szerverrel való kommunikációnál, akkor fel tudja használni. A böngésző ezeket elrejti az átlag felhasználó szemei elől, de ha valaki kíváncsi, az ilyen turkáláshoz kiváló eszköz lehet a LiveHTTPHeaders plugin a Firefoxhoz, amely **a HTTP kérések fejlécadatait tudja teljes részletességgel** megmutatni.

Ezt a változót **sikerülhet kinyerni az áldozat gépéből, ha rávesszük, látogasson meg egy kártékony kódot tartalmazó weboldalt**. Igen **kevesen lépnek ki azonnal és törlik az oldalhoz tartozó cookiejaikat**, amikor már nem használják az adott szolgáltatást, ezért működhet a dolog. A Geekcondition oldalon részletesebben bemutatják a módszert, ami **egy szűrő segítségével az üzeneteket arra kényszeríti, ne érkezzenek meg a bejövő postafiókba, továbbítódjanak a támadó címére, végül pedig törlődjenek ki** nyomtalanul a megtámadott postafiókból. A dolog veszélye, hogy **a manipuláció igen nehezen észlelhető**. A sebezhetőséget alapvetően az okozta, hogy néhány ember elvesztette a domain nevét, amelyet korábban a GoDaddy.com-nál regisztrált.

Addig is mindenki **ellenőrizze rendszeresen a G-mailes levelezésében működő szűrőket**. És biztos unalmasan hangzik - kicsit olyan mint a gyógyszerreklámoknál a TV-ben elhadart: "Ésamellékhatásoktekintetébenkérdezzemegorvosátgyógyszerészét" - de **mi is csak ismételni tudjuk** magunkat: **a NoScript pluginnel mindez nem történt volna meg.**

· 1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/785506

Trackbackek, pingbackek:

Trackback: BuheraBlog **2008.11.25. 10:22:58**

Filterezés a GmaillelRambo már írt egy kis összefoglalót a külföldi blogszférát lázban tartó "problémáról", melynek segítségével több GoDaddy-s domian név fölött is sikerült átvenni az irányítást az illetékteleneknek. Én kezdetben úgy állta…

Kommentek:

penge™ · http://www.thevenusproject.com/ 2008.11.24. 12:16:31

Ez HTTPS esetén is működik? Illetve minden böngészőnél?
A nehéz észrevenni alatt azt érted, hogy látható nyomot hagy a beállításokban egy szabály formájában, tehát csak az nem veszi észre, aki nem nézi meg a szűrőit?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.24. 16:09:12

Szia!

A HTTPS arra jó, hogy ne clear textben utazzon a jelszó. Ám ettől függetlenül a session cookie még ellopható.

És igen, egy átlag juzer valószínűleg azt sem tudja, mi az a Gmail szűrő, nem hogy rendszeresen ellenőrizné azokat...

4th05 (törölt) 2008.11.24. 20:52:19

Megint feltalálták a CSRF-et (XSRF)? Tavaly ősszel olvastam legutóbb, hogy egy kártékony oldal szűrőt tud létrehozni egy aktív Google session-nel rendelkező látogató postafiókjában, és már rég kijavították. Esetleg egy működő exploitot láthatnánk?

A hír tavalyról: pcforum.hu/hirek/10727/Barki+beleolvashat+Gmail+leveleinkbe.html (fenn volt HUP-on is).

A leírt módszer (rejtett iframe-be betölteni egy preparált request-et) pontosan a CSRF legegyszerűbb változata.

Vidi Rita · http://www.hosnok.hu 2008.11.25. 14:55:42

hát nemtom.. egyedül vagyok a google cuccok használatával kapcsolatos fenntartásaimmal?
na mindegy, ezen nem elmélkedem, az viszont tény, hogy a noscript egy isten áldása ezekben az exploit-zivataros időkben:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.25. 21:08:08

Szia 4th05!
Lényegében igen, Buherátor közben szépen összefoglalta a dolgokat.
A tavalyi esetnél én ezt ismertem:
www.gnucitizen.org/blog/google-gmail-e-mail-hijack-technique/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.25. 21:20:47

Szia Rita!

Fenntartásai mindenkinek vannak, de az élet tele van kompromisszumokkal. Hogy egy konkrét példával éljek: ismerősnek saját domainje van, de csak 300 MB tárhely jár hozzá külön a levelekhez. Amióta a főníciaiak ;-) feltalálták a spamet, azóta ez

ugyebár smafu. Emiatt kétszer is leállt már a levelezése, utóbb kiderült, elfogyott a kvóta, tombolt dühében, mert épp fontos külföldi levelet várt. Később felemelték neki 500 MB-ra, de néhány hónap után az is beállt mégegyszer hasonló okok miatt. Ehhez ugyebár elég néhány idióta is, aki elég gyakran megszór vicces videókkal, világmegváltó PPT-kkel.

Utána fogta magát, befűzte a levelezését a Gmail alá, és ettől kezdve a spamszűrési gond megszűnt, és 7 GB az meg 7 GB. Az hogy a Google nagy tesó esetleg belenézhet, meg hogy vannak ennek veszélyei - még ha nem is rengeteg - ez nem érdekli, és én egy cseppet sem csodálkozom rajta: most elégedett, öröm és bódottá van nála.

Ezzel csak azt akartam mondani, hogy mindig van oka annak, hogy emberek milyen motivációk miatt döntenek úgy, ahogy döntenek: Herbert Spencer is ezt írta az Alapvető elvekben :-)

Karácsonyi exploit készletet tessék!

2008.11.25. 20:50 | Csizmazia István [Rambo] | 2 komment

Címkék: ünnep xmas fertőzés kártevők

Nem kell különösebb jóstehetség vagy üveggömb hozzá, hogy elképzeljük, az idei karácsonyi időszak sem lesz kivétel és **az ünnepeket kihasználó kártevő terjesztők akciói már nagyban futnak**. A repertoár széles: fertőzött weblapok, manipulált webáruházak, ünnepi üdvözlőlapok, stb.

Dancho Danchev egy olyan hirdetést fedezett fel, ahol **a rosszfiúk komplett, azonnal használatbavehető kártevőterjesztő készleteket kínálnak**, melyek segítségével "biztosan meg lehet keresni a karácsonyi ajándékra valót".

Az interneten **orosz weboldalakon hirdetett eszköz** Basic, Standard és Professional változatban kapható, és természetesen a legdrágább profi verzió képes a legtöbb sebezhetőséget kihasználni. A sérülékenységek között **IE6, Opera, Firefox, PDF, XLS és SWF állományok elleni támadás szerepel**, és a készítő még azzal is dicsekszik, hogy 37 antivírus programból mindössze 6 látja a kártevőt, amely TDSSserv.sys néven **egy rootkit komponenst is megkísérel** a rendszerbe juttatni.

Lényeg a lényeg, a karácsony a szeretet ünnepe, és ugyan szép dolog a bizalom, de azért ennek ellenére legyünk résen a közelgő ünnepi forgatagban is.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/787483

Kommentek:

Algernon 2008.11.26. 10:28:05

Szia István!

Lenne egy nem teljesen a témához kapcsolódó kérdésem. A netes vásárlásoknál sok esetben ugye keylogger progikkal lopják el a szükséges bankkártya adatokat. Ha jól emlékszem, a KIS legújabb verzióját reklámozták egy virtuális billentyűzettel, ami ezt a problémát kiküszöböli. Engem az érdekelne, hogy a Windows beépített Képernyő-billentyűzetét tudják-e ezek a keyloggerek naplózni vagy ha ezt használja valaki a fontosabb adatai megadásánál, biztonságban van.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.26. 12:38:15

Szia Algernon!

Biztos előfordul ilyen is helyi gépen, de szerintem sokkal gyakoribb a hamis űrlap, hidden mező, javascriptes okosság, etc.

A válaszom röviden: sosem vagy biztonságban :-)

Kicsit hosszabban: ha a kérdésed arra vonatkozik, hogy a keylogger ellen a virtuális billentyűk adják-e a 100%-os védelmet, akkor nem. Szinte mindegyik rendelkezik screenshot funkcióval is, és az ellen így hiába trükközöl.

És most ugye csak a keylogger szempontjából nézgelődtünk, a forgalmad figyelésével, csomagelemzésével, eltérítésével gyakorlatilag bármi megszerezhető. Amit te tehetsz, az a tőled telhető legnagyobb gondosság. Pl. fontos és bizalmas anyagot, jelszavakat, stb. mindig titkosított formában tárolsz, pl, TrueCrypt; naprakész AV és kémirtó full módban és frissítve fusson, logolós kétirányú tűzfal használata, egészséges gyanakvás. Wiifinél WPA2 vagy Radius szerveres autentikáció alkalmazása. Kb. ennyi.

Vége az ideiglenes spam szünetnek

2008.11.26. 11:55 | Csizmazia István [Rambo] | 1 komment

Címkék: spam fbi szünet rustock

Felnőtt emeberek vagyunk és csak egy icipicit hiszünk a mesékben, de azért a McColo szervereinek lekapcsolása utáni spam csökkenés időszakát valamivel **hosszabbnak reméltük**. Hát tévedtünk. **A csilliónyi szemétlevél ismét** robog a bitek országútján.

Nyilván senki nem végleges megoldásnak képzelte **az FBI egyszeri rajtaütését**, de a rövidke, mindössze néhány napos visszaesés után **a Rustock megrázta magát, és ismét emelkedést regisztráltak** a spamek frontján a Sophosnál.

Rendszerük újrakonfigurálása után a rosszfiúk kb. 12 nap elteltével ismét **a "szokásos" közeli szintre emelték** kéretlen leveleik számát. A Rustock egyik fő profilja a kanadai gyógyszerek típusú reklámlevelek szétküldése, talán nincs is olyan felhasználó, aki ebből ne kapott volna már.

Ezt ki veszi be, hogy egy MS szolgáltatásról Kínából kell leiratkozni?!

A visszaesést **Magyarországon is jól meg lehetett figyelni**, ismerőseim között - akik céges postaládájukba korábban napi 60-100 ilyet kaptak, most "mindössze" 10-20 érkezett naponta. Igaz, ebből egy is sok, de legyünk realisták, kicsit a normális és **kezelhető retro szint ereszkedhettük vissza egy szusszanásnyi időre**. Hosszú távon talán egy külön spamszerver rajtaütő egységet kellene szervezni az FBI-nál, akik **a napi eredményes akciók számával arányos prémiumot kapnának** - ez talán segítene ;-)

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/789250

Kommentek:

dark future · http://www.andocsek.hu 2008.11.26. 15:03:58

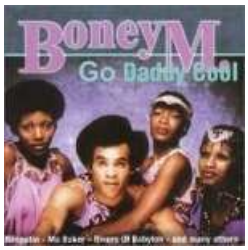
Elkelne egy ilyen akciócsoport Kínában és Oroszországban is...

Hamis antivírus után hamisított antivírus

2008.11.27. 22:42 | Csizmazia István [Rambo] | 5 komment

Címkék: letöltés csalás hamis avg webhely

Egy friss hír szerint már nem csak az Antivirus XP 2009, 2010, és hasonló trükkök dívnak, hanem a **létező AV cégek imázsának lejáratása, nevükkel való visszaélés lehet a kártevőterjesztők új módszere**. Lehet aggódni.



Ugyan a hamis antivírus trükk már ismert a hozzáértők előtt, de **még mindig sikeresen lehet vele embereket átverni**. A PC Worldben a Vírusok Varázslatos Világa sorozatban a 15. novemberi számában már részletesen írtunk erről a témáról. Ott **a lényeg az, hogy kitalálnak egy új nevet - pl. CsilliVilli Antivírus 2099 - aztán hirdetik, spammelik, ablakot nyitnak a böngészőben, és igyekeznek terjeszteni, hogy a gyanútlan vásárolók fizessenek a semmiért**. Mit mondunk mi erre? Muszáj figyelni és tájékozódni, és **részesítsük előnyben a neves gyártók termékeit**, mint ESET, Kaspersky, McAfee vagy Norton.

De mi lenne - sőt most már mi van - akkor, ha a gazfickók **nem pusztán fantázianevekkel, kitalált programnevekkel játszanának, hanem vérfagyasztó módon valódi antivírus programok nevében**, azok letöltési oldalát hamisítva, a vásárolni szándékozók személyes és banki adatainak ellopásával szereznének pénzt? Nos, ez már nem a jövő, nem Sziriusz Kapitány és a Csillaglány a főszereplő, sem Mikrobi, hanem **ez már itt és most van**.

Van itt minden - VB100, díjhegyek - mint karácsonykor

Ezúttal az AVG került célkeresztbe, és az ő oldalukat hamisították meg egy GoDaddys weboldalról. A cikk ugyan hibásan hivatkozik a webhelyre (http://0fficial-page-com/AVG1), de "szerencsére" rövid próbálkozás után sikerült megtalálni az igazi csaló oldalt is (http://0fficial-page.com/AVG1). A hivatkozott szakértő szerint a támadásnak az AVG online scanner funkciója is potenciális célpontja lehet, ennél a lépésnél ugyanis egy komponens töltődik le a delikvens gépére, ami az online vizsgálatot végző programocska helyett akár kártevő is lehet.

Itt látszólag (még) nem a fertőzésre, kártevő terjesztésre megy ki a játék, egyelőre ?! megelégszenek a pénzünkkel is ;-) Ha **valaki az eredeti weboldal helyett itt rendel, az futhat a pénze után**. Sőt, nem csak, hogy a kívánt vírusirtót nem kapja meg, de a megadott bankkártyájával és annak 3 jegyű biztonsági kódjával **a bűnözők villámgyorsan leüríthetik a számláját is**. Végülis annyi megmaradt, hogy **most is a semmiért fizetünk**.

Még belegondolni is félelmetes, **mi lesz, ha több más vagy akár az összes komoly antivirus cég nevében elkezdenek majd**

machinálni□□ó, a geekek úgyis tudják fejből kedvenc vírusvédelmi oldaluk IP címét ;-) de mi lesz a többiekkel?

Az új szabály talán az lehet, hogy levélben érkező linkről vagy nem a gyártó domainnevéről nyíló oldalról sose rendeljünk szoftvert, és semmiképpen ne adjuk meg személyes adatainkat. Már a jövő sem a régi...

□1 trackback

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/792161

□rackbackek, pingbackek:

□rackback: klikk.usite.hu 2008.11.28. 10:44:09

Hamis AVG letölthető, megvehetőMi lenne - sőt most már mi van - akkor, ha a gazfickók nem pusztán fantázianevekkel, kitalált programnevekkel játszanának, hanem vérfagyasztó módon valódi antivírus programok nevében, azok letöltési oldalát hamisítva, a vásá…

Kommentek:

VistaMan 2008.11.28. 09:53:45

Ezt a GoDaddy ügyet nem értem.
GoDaddy egy regisztrátor (akiről még nem sok rosszat olvastam). Igaz, hogy nála regisztrálták a fenti domaint, de nem az ő tulajdona. (Vagy valamit félreértek?)

waces · http://photos.waces.hu 2008.11.28. 10:02:10

namost aki egy akarmilyen oldalon kepes venni barmit is ott azert a hulyesegfaktor is bejatszik. ilyenolyanoldal/avg eleggen "un-officialnak" tunik.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.28. 10:03:03

Hmm, igazad van ebben, elkevertem, rögtön javítok is. A sok EstDomainses ügy elterelte a figyelmemet, sajnálom...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.28. 10:08:36

@VistaMan: köszi az észrevételt

 Waces: Szentigaz, de hát nem is arról szól ez, hogy te vagy én benézem ezt, hanem az átlagember. Neki pedig van rá sansza erősen. Például ha hall olyat, hogy az AVG az elég jó, aztán látja a fenti weboldalt, mit fog tenni?

Az ilyen cégnevek elleni manipuláció szinte már szokásosnak mondható, sokan rá is játszanak, egy "átlagszülő" meg vesz egy gagyit a gyerekének "ócsóért" :-(
homar.blog.hu/2008/11/27/kamu_wii_t_arul_az_auchan

gothmog 2008.11.28. 1□:2□:18

amíg a gúgli az "avg" kifejezésre az első ötven (legyünk optimisták) találat között nem hozza fel ezt a szemétdombot, addig viszonylag nyugodt vagyok.
Az ilyen "hallomás" nálam úgy szokott történni, hogy:
...
én: -van ingyenes az avg-ből, az avast-ból, meg az avira-ból is. például.
kezdő júzer: -fú, és honnan lehet letölteni?
é: -beírod a gúgliba, és első találat.
kj: -nem írnád le nekem mégis egy darab papírra?
é: -dehogynem... tessék. illetve nincs nálad egy pendrájv? akkor mindjárt feltolom rá az installert, és neked csak telepíteni kell.
kj: -köszi!
ennyi. kb kettő perc.
És ilyenkor azzal a kellemes tudattal dőlök hátra, hogy talán egyel csökkentettem a potenciális zombik számát.
A másik lehetőség, amikor a "kezdő júzer" megkér, hogy "állítsam be az internetet", akkor az nem akkor van kész, amikor beírjuk a felhasználónév/jelszót, hanem akkor mikor fent van a tűzfal, egy friss böngésző, egy antivírus, meg egy antispyware. Bár ez inkább utólag szokott történni, komplett újratelepítéssel egybekötve. Miután az egyszeri felhasználónak már egy másodperc gépidő se jut a sok virtumonde és társai típusú "alkalmazástól".
És ilyenkor konkrétan _tudom_ hogy csökkentettem egyel a zombik számát. És kajánul vigyorgok közben. ;)

NOD32 okostelefonokra

2008.11.27. 16:55 | Csizmazia István [Rambo] | 2 komment

Címkék: windows mobile okostelefon smartphone nod32 antivírus eset

Az okostelefonok terjedésével fokozódnak **a mobileszközökhöz kapcsolódó biztonsági kockázatok** is. A vírustámadások kivédésére **az ESET piacra dobta új szoftverét, a Mobile Antivirust**. Az itthon december első napján megjelenő vírusirtó a cég vállalati ügyfelei számára ingyenesen vagy jelentős kedvezménnyel lesz elérhető.

Az okostelefonokat támadó kártevők **nem csak az eszközökön tárolt adatokat rongálhatják meg, de akár továbbíthatják a felhasználók személyes adatait** a vírusok készítői számára. A NOD32 fejlesztése során megszerzett tapasztalatokat felhasználó ESET Mobile Antivirus **proaktív védelmet nyújt a kártevők ellen, és képes a kéretlen SMS üzenetek blokkolására is**.

A program a Windows Mobile 5.0, 6.0 és 6.1 platformokon használható.

A **Windows Mobile platformon működő szoftver** a többfajta ellenőrzési funkcióval és az automatikus frissítés lehetőségével kiegészítve megbízható védelmet biztosít az okostelefonoknak.

A szokásos részletes beállítási lehetőségek állnak rendelkezésre

A Mobile Antivirus fejlesztése során az ESET szakembereinek **számos olyan nehézséget kellett leküzdeniük**, amelyek szinte ismeretlenek az asztali számítógépeken és laptopokon használt vírusirtóknál. Korlátot jelentett az okostelefonok limitált memóriája, az eltérő akkumulátorfajták kapacitása és a különböző sávszélességek létezése. "A számos kihívás ellenére sikerült egy olyan szoftvert létrehozni, amely a telefon teljesítményének befolyásolása nélkül képes teljes körű védelmet biztosítani" - mondta Csiszér Béla, az ESET NOD32 magyarországi forgalmazásáért felelős Sicontact Kft. ügyvezetője.

Próbaképpen ráeresztettük az EICAR tesztfájlra

A mobiltelefonokra készített védelemhez az ESET Smart Security Business Edition licenctulajdonosok ingyenesen, az ESET NOD32 Antivirus Business Edition licenctulajdonosok pedig 50% **kedvezménnyel juthatnak hozzá**.

Bannoljuk ki a nem kívánatos SMS-ek küldőit blacklistával

Az ESET Mobile Antivirus tulajdonságai:
- **eurisztikus vírusvédelem**: Mesterséges intelligencián alapuló, valós idejű vírusvédelem a már létező és a még nem ismert károkozók ellen.
- **Kisméretű frissítési fájlok**: A kompakt, optimalizált frissítéseknek köszönhetően az ESET Mobile Antivirus naprakészen tartása nem igényel nagy adatforgalmat a mobilhálózatokon.
- **Automata vagy kézi indítású frissítés**: Manuális vírusadatbázis-frissítés, vagy napi, heti és havi gyakoriságú automatikus frissítés.
- **Kézi indítású ellenőrzés**: A belső és külső adathordozók ellenőrzésére egyaránt alkalmas eszköz.
- **Cabinet fájlok ellenőrzése**: A tömörített cabinet fájlokban megbújó vírusok felderítésére használható alkalmazás.
- **Naplófájlok**: Az elvégzett ellenőrzések statisztikái felhasználóbarát formátumban.
- **SMS szűrő**: A kéretlen szöveges üzenetek ellen nyújt védelmet, azáltal, hogy a gyanús üzeneteket a levélszemétmappába helyezi.

A programnak mind a telefonnal internetezők, mind pedig a telefon memóriáját/memória kártyáját USB kulcsként használó okostelefonok tulajdonosok nagy hasznát vehetik.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/791639

Kommentek:

penge™ · http://www.thevenusproject.com/ 2008.11.27. 18:58:13

Symbianra lesz valamikor a jövőben?

Csizmazia István [Rambo] http://antivirus.blog.hu 2008.11.27. 20:22:23

Szia Penge

Konkrétumról nem tudok, csak annyit, hogy a jövőben tervezik a többi platformon való megjelenést is.
www.eset.com/emabeta/faq.php

Megérkezett a 4.0-ás NOD32 béta verziója

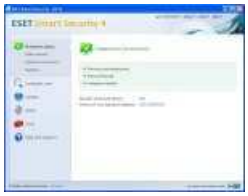
2008.12.01. 17:28 | Csizmazia István [Rambo] | 2 komment

Címkék: béta security új smart nod32 eset ess

Az ESET NOD32 vírusirtójának és az ESET Smart Security integrált biztonsági csomagjának **új változatai** önmagukat is megvédik a kártevőktől, fejlett rendszerfelügyeleti funkciókat tartalmaznak, emellett **a fertőzött rendszerek külső forrásból történő ellenőrzését is lehetővé teszik.**

A NOD32 antivírus és a tűzfalat és levélszemétszűrőt is tartalmazó Smart Security új változata **támogatja egy Rendszerellenőrző CD létrehozását**, így lehetővé vált a fertőzött rendszerek külső forrásból történő ellenőrzése. Ily módon olyan esetben is megtisztíthatók a számítógépek, amikor egyébként a merevlemez kiszerelésére lenne szükség. **Mindkét szoftverbe bekerült az ESET SysInspector rendszerfelügyeleti eszköz is**, mely eddig önálló alkalmazásként volt elérhető. Ez részletes adatokat szolgáltat a felügyelt számítógépeken futó folyamatokról, **megkönnyítve a rejtett fertőzések, például rootkitek felderítését**. (Az eszköz funkcióinak bemutatásáról készült videó az ESET honlapján megtekinthető.)

Az ESET folyamatosan fejleszti termékeit, az újítások pedig **minden esetben jelentős előrelépést hoznak** a kártevők elleni védekezésben. „A végleges változatban néhány hónap múlva megjelenő szoftverek a rendszermag szintjén kódolt önvédelmi funkciókat tartalmaznak, így **még biztosabban észlelik majd, ha egy kártevő megpróbálja kiiktatni a védelmet**” – emelte ki Csiszér Béla, az ESET magyarországi képviseletét ellátó Sicontact Kft. ügyvezetője.



A most bemutatott, ingyenesen letölthető béta változatok után a végleges 4.0-ás verziók várhatóan 2009. februárban lesznek elérhetőek angol nyelven, magyarul pedig egy-két hónap késéssel jutnak el hozzánk.

Az ESET NOD32 Antivirus és az ESET Smart Security 4.0-ás változata részletesen az alábbi újdonságokat tartalmazza:

Általános funkciók (NOD32 és Smart Security)
Megújult és kibővült Védelem állapota ablak: Az új ablakban grafikusan és statisztikákon keresztül követhetjük nyomon a rendszer és a hálózat működését. Statisztikák kérhetők le többek között a valós idejű fájlrendszervédelem, a webhozzáférés-védelem és az e-mail-védelem működéséről. Szintén fontos adat az Utoljára ellenőrzött objektum, amely a NOD32 2.7-es verziójában megszokottakhoz hasonlóan jelenik meg.

Önvédelem: Az új verziók önvédelmi funkciója rendszermag szinten ellenőrzi, hogy nem történt-e a szoftver fájljait érintő változtatás.

SysInspector felügyeleti eszköz: A 4.0-ás verziókba integrálásra került az eddig főként gyakorlott felhasználók és rendszergazdák által használt SysIsnspector rendszerfelügyeleti eszköz, amely korábban az ESET honlapjáról volt ingyenesen elérhető. Az alkalmazás részletes adatokat szolgáltat a számítógépen futó folyamatokról, megkönnyítve a rejtett fertőzések korai felderítését.

Rendszerellenőrző CD: Mindkét szoftver támogatja a Rendszerellenőrző CD létrehozását, amely lehetővé teszi a fertőzött rendszerek külső forrásból történő biztonságos ellenőrzését és megtisztítását.

Windows frissítések ellenőrzése: Az új verziók automatikusan ellenőrzik a rendelkezésre álló Windows javításokat. A felhasználó megadhatja, milyen frissítésekről kíván értesítést kapni. Így például ha a kritikus fejlesztések kerültek kijelölésre, a szoftver csak akkor jelez a felhasználónak, ha ilyen fejlesztések állnak rendelkezésre.

Jelszóvédelem a szoftver letelepítése ellen, UAC-támogatás: Amennyiben a beállítások változtatásait jelszóval védjük, a program nem

engedélyezi a letelepítését. Az új verziók rendelkeznek UAC (User Account Control – Felhasználói Fiókok Felügyelete) támogatással is, így bizonyos változtatásokat csak rendszergazdák kezdeményezhetnek.

Teljes képernyős használat esetén letiltható figyelmeztetőablakok: Teljes képernyős használat esetén letiltható lett a figyelmeztetőablakok felugrása, a több felhasználó által használt gépeken pedig a különböző felhasználók egyéni beállításai is elmenthetők. Kikapcsolható grafikus megjelenítés: Kikapcsolható a szoftver grafikus kezelőfelülete, így az új verziók kompatibilisek a vakok és gyengénlátók által használt felolvasóprogramokkal.

Másodlagos ESET Remote Administrator szerver: A nagyobb munkahelyi hálózatokat érintő változás, hogy az új verzió lehetőséget ad egy másodlagos ESET Remote Administrator szerver alkalmazására. Ez megbízható működést biztosít az elsődleges szerver esetleges meghibásodása esetén is.

Mozilla Thunderbird támogatás: A 4.0-ás béta verziók teljes támogatást biztosítanak Thunderbird számára is.

* * * * *

Vírus- és kémprogramvédelem (NOD32 és Smart Security)
ThreatSense technológia: A programok nem csupán felismerik a rejtett fertőzéseket, hanem a továbbfejlesztett tisztítás funkció révén már meg is tisztítják ezektől a számítógépeket.

ThreatSense technológia: A számítógép ellenőrzésénél limitálható a vizsgált fájlok mérete, meghatározható a maximális ellenőrzési időtartam.

Külső adathordozók blokkolása: Letiltható a külső adathordozók automatikus futtatása.
Továbbfejlesztett dokumentum védelem: A korábban már megismert DMON dokumentumvédelmi modul a Valós idejű fájlrendszervédelem részeként került vissza az új verziókba.

Megújult https és POP3 beállítások: Ha a NOD32 vagy a Smart Security új https vagy POP3 kommunikációt észlel, a felhasználó egyenként elfogadhatja vagy elutasíthatja a csatorna ellenőrzését, vagy kérheti, hogy a szoftver minden ilyen esetben végezze el az ellenőrzést.

Kibővített http szűrő: Az előző verzióktól eltérően már nem csak a kizárt és a tiltott címeket adhatjuk meg, de létrehozhatunk egy listát az engedélyezett címekből is, amelyek megadásával az összes listán kívüli cím letiltásra kerül. Ez jelentős előrelépését jelent a felhasználó-biztonság szempontjából, és lehetővé teszi például, hogy meghatározzuk, hogy a felhasználók milyen weblapokat látogathatnak meg.

SSL protokoll szűrő: A szoftverek képesek az SSL forgalom ellenőrzésére. Az SSL kommunikáció részleteit a Haladó beállítások alatt szabályozhatjuk.

* * * * *

A tűzfal modul újdonságai (Smart Security)
Tanuló üzemmód: A tűzfal modulon megmaradt a már jól ismert és bevált automata üzemmód, a felhasználók kéréseinek megfelelően azonban beépítésre került a kivételek megadásának lehetősége is. A tanuló üzemmód (Learning mode) egy olyan speciális funkció, amely segítségével saját magunk „taníthatjuk” a tűzfalat az új kapcsolatok kezelésére. Így vállalati rendszergazdák az eddigieknél könnyebben konfigurálhatják a tűzfalszabályokat.

Levélszemétszűrő fejlesztések (Smart Security)
Címlista importálása: A különböző címlistákat a levélszemétszűrő automatikusan importálni tudja, így a névjegyalbumokban szereplő kontaktokat automatikusan hozzáadhatjuk a megbízható levélküldők listájához.

Az ESET licencpolitikájának megfelelően az **érvényes licenccel rendelkező felhasználók számára ingyenesen elérhető** új változatok számos újítást tartalmaznak mind az otthoni, mind a vállalati felhasználók számára.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/798178

Kommentek:

tomm1971 2008.12.02. 08:17:26

köszi

cworm (törölt) 2008.12.02. 09:17:22

Ez a létrehozható rendszerellenőrző cd nagyon jó ötlet!:)

A minden gyanú felett álló megbízható feladó

2008.12.03. 09:34 | Csizmazia István [Rambo] | 2 komment

Címkék: spam link trükk kártevő feladó

Egy mondás szerint **az anyanyelv legszebb szava** a saját nevünk, és mértéktelenül meg is tudunk sértődni, ha valaki ezt esetleg elvéti, netán elfelejti. Nos, **e gondolatmenet medrében megszületett a spamküldés egy újabb fejezete**.

Utáljuk John Boltont, Jereimias Smitht? **Nem hisszük el, hogy Jackie Hurley igazi levelet küld nekünk?** Még Marilyn Allard is kiveri nálunk a biztosítékot, mint üzenetforrás? Akkor ideje mással próbálkozni. Ezt belátva egy idő után érkeztek is a valamilyen Administrator (Natalia :-) nevében jövő üzenetek. Ugyan ki gyanakodna egy igazi hiteles, korrekt és egységes, tévedést kizáró Administratortól kapott levél miatt? Ki merészelne kételkedni annyira, hogy ne nyissa meg azonnal, gyanakvás nélkül?! Aztán később valamilyen fel sem adott küldemény ügyében jelentkező Admin, Support, stb. ügyintézőtől kaptunk levelet, jött meg sem rendelt hírszolgáltatás keretében "Urgent News" címkével ellátott hírlevél, és **még azt a furmányt is bevetették**, hogy "Mail Delivery Status Notification" címkével is érkezhessen levél - vagyis látszólag általunk korábban küldött, de valamilyen címzési probléma miatt visszapattanó saját üzenet - **benne sokszor kártevővel kattintható linkkel**.

Ezúttal megtalálták a világ legmegbízhatóbb levélküldőjét, akiben álmunkban sem kételkednénk: Én, azaz mi magunk vagyunk azok, legalábbis látszólag. Az érkező spam levelekben ugyan hébe-hóba előfordul még egy két Gulliver, Joachim, Roxie, de a többség mi vagyunk. Szűrjük is ki gyorsan ;-) A már több napja megfigyelhető folyamat semmiképp nem véletlen, a folyamatos kísérletezés bizonyítéka a rossz oldalon. Jól érzékelhető, hogy több mint elegendő számú Öveges professzor mentalitású fejlesztő töri náluk a fejét "Mi lenne, ha..." típusú kérdésekkel a számítógépe előtt.

A **"magunk által küldött" ;-) üzenetek tartalma természetesen már egyértelműsíti a helyzetet**, ott már többnyire a fenti paneleket találjuk: nem létező hibaüzenet az el nem küldött levelünkről, értesítést a sosem rendelt árucikkünkről, etc. Talán nem tévedünk nagyot, hogy **sajnos ebből is meg lesz az az öt százaléknyi kattintás**, ami miatt megéri kéretlen a reklámlevél, a kémprogram és egyéb kártevőterjesztőknek az ilyen megtévesztéseket alkalmazni.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/801033

Kommentek:

L.A. · http://fuggoagy.blog.hu 2008.12.03. 10:28:27

szerintem kipécéztek téged, vagy tényleg te küldöd :)
nekem még soha nem jött ilyen.

jattila 2008.12.03. 17:35:37

rendszeresen kapok ilyet

Kell-e vírusirtó az Apple gépekre?

2008.12.03. 18:16 | Csizmazia István [Rambo] | 2 komment

Címkék: apple bejegyzés antivirus kitörölt

Korábban már irtunk trójaiakról, kodekekről Mac alatt, és hogy ha a felhasználó maga kattint, arra nincs orvosság egy operációs rendszeren sem. Most viszont **maga az Apple tanácsolta, használjunk antivírusprogramot OS X alatt is.**

A dologról magyarul is született blogbejegyzés, amiben hivatkoznak az Apple weboldalára, továbbá **sok remek komment is íródott alant.** Nyilván benne van egyfajta hype és nyomás is a gyártók részéről, de ezzel együtt a végtelenségig biztos nem lehet azt állítani, hogy ide aztán nem kell ilyesmi soha, mert ezt egy mentes platform.

A történet **akkor kezdett érdekessé válni, mikor az eredetileg 2008.12.02.-én módosított** bejegyzés nemes egyszerűséggel eltűnt az internetről :-O

Mivel elég furcsa az eset, így kivételesen minden fázisról teljes képernyőképet mellékelünk, who knows? ;-) Végül letörölt bejegyzés ide, kényes téma oda, anélkül, hogy állást akarnánk foglalni, itt a Barbatrükk, **hogyan nézzük meg a bejegyzést mégis így utólag :-)**

```
Írjuk be a Google kereso ablakba:
cache:http://support.apple.com/kb/HT2550?viewlocale=en_US
```

Linux guru barátokkal beszélgetve úgy látom, **nem derogál nekik időnként belenézegetni a FireStarter logba, néhány hetente CheckRootkit és RKHunter szoftvert frissíteni és futtatni ahelyett, hogy azt mondanák "ugyan kérem, ez nem Windows".** Vigyázni mindenütt kell valamennyire, aztán persze a mérték az már egy másik kérdés. Az Appleblog kommentek között szerepelt, hogy ha egy OS eléggé elterjed akkor elér egy olyan szintet, amikor lassan már megéri rá kártevőt (nem klasszikus vírust, hanem inkább rootkitet, kémprogramot, reklámprogramot) fejleszteni - ez szerintem is igaz lesz, és akkor majd nézhetnek a Dr. House-ok ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/801273

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.01.22. 10:07:21

Lehet, hogy hamarosan indul a vadászidény itt is:
hup.hu/cikkek/20090121/az_eddigieknel_eszrevehetetlenebb_mac_exploitalasi_technikara_figyelmeztet_egy_tanulmany

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.04.22. 14:21:09

Érdekesség:
www.securecomputing.net.au/News/143087,apple-users-at-risk-as-mac-malware-mushrooms.aspx

Érdemes frissíteni a Flash lejátszót

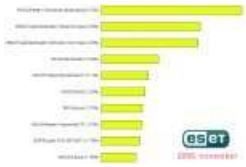
2008.12.04. 22:24 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az ESET **Magyarországra vonatkozó, több százezer hazai felhasználó adatai alapján készült** statisztikája szerint november során **két új kártevő került fel** a vírusok toplistájára. A SWF/exploit.CVE-2007-0071, mely világviszonylatban kizárólag a magyar toplistán szerepelt, **a nem frissített Adobe Flash Playerek sebezhetőségét használja ki**.

A NOD32 antivírust gyártó ESET statisztikai rendszere egyedülálló módon **képes az egyes országokra lebontott vírusstatisztika közlésére** is, így hónapról hónapra követhető a hazánkban pusztító vírusok toplistájának alakulása, mely több százezer magyar felhasználó adatai alapján áll össze. A lista **egyaránt tartalmazza a vírusokat, a kémprogramokat és a kéretlen reklámprogramokat**, azok elterjedtségének arányában.

Novemberben a top10-ben szereplő károkozók **az összes magyarországi fertőzés mintegy 30 százalékáért** voltak felelősek. A **nemzetközi trendhez hasonlóan, az Autorun típusú** – automatikus programfuttató fájlt használó – károkozók megkeserítették a magyar számítógép-felhasználók életét, ahogy a böngésző keresési beállításait módosító Win32/Toolbar.MyWebSearch is. A kéretlen reklámokat megjelenítő **Virtumonde elsősorban Európában terjedt**, és nálunk a lista első helyére került. A hazai top10-ből **ugyanakkor hiányzik a világszerte elterjedt Win32/PSW.OnlineGames** kártevő, mely a számítógépes játékok jelszavait lopja el.



A magyar toplistán a korábbi hónapokhoz képest két új szereplő is helyet kapott. Az új fertőzésnek számító Win32/Patched.BU a C:\windows\system32-ben lévő dmserver.dll állományt módosítja.

A hazai lista **másik újonca, az SWF/exploit.CVE-2007-0071**, kizárólag a magyar top10-ben kapott helyet november során. A károkozó a nem frissített Adobe Flash Playerek sebezhetőségét használja ki. Az óvatlan felhasználók **akár egy fertőzött internetes videó elindításával is megfertőzhetik** számítógépeiket. Esetenként a weboldal-tulajdonosok tudta nélkül, egy rejtett támadás révén kerül fel a káros kód az oldalra, míg máskor a portál üzemeltetőjének aktív közreműködésével.

A szándékosan hibás szerkezetű, **preparált swf fájlok elindításakor a károkozó lefuttat egy kódot**, melynek nyomán különböző fertőzések – például a jelszavak figyelésére szakosodott keyloggerek vagy a rejtőzködő, akár a komputer vezérlését is átvevő rootkitek – kerülnek a felhasználó számítógépére. Érdekesség, hogy a károkozó világviszonylatban már néhány hónappal ezelőtt megjelent, azonban a magyar felhasználóknál csak mostanában kezdett terjedni. **A sebezhetőséget az Adobe Flash Player fejlesztői időközben javították, így a védekezéshez elegendő a programot a 10-es verzióra frissíteni.** A Flash Player verziószámát az Adobe weboldalán, illetve egy flash videóra jobb gombbal kattintva az „About Adobe Flash Player" opció választásával ellenőrizhetjük.

Végül **következzen a magyarországi toplista**. Az ESET statisztikai rendszere szerint novemberben az alábbi 10 károkozó terjedt a legnagyobb számban:

1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a novemberi fertőzések között: 6.47%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET kategorizálása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

2. WMA/TrojanDownloader.Wimad.N trójai
Elterjedtsége a novemberi fertőzések között: 4.56%

Működés: A Wimad.N egy trójai letöltőprogram, amely a Win32/Adware.PlayMP3Z vírust telepíti a PC-re. A kártevő úgy kerül a számítógépre, hogy a felhasználó figyelmetlenül elfogadja a licencszerződést, amellyel egyúttal jóváhagyja a további tartalmak letöltését. Az Adware programok általában azáltal válnak ingyenessé, hogy cserébe bele kell egyezni, hogy reklámokat jelenítsenek meg a gépünkön.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-wimad-n

3. WMA/TrojanDownloader.GetCodec.Gen trójai
Elterjedtsége a novemberi fertőzések között: 4.45%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki .letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files \ VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben, és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: A felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

4. Win32/Patched BU
Elterjedtsége a novemberi fertőzések között: 2.63%

Működés: A Win32/Patched.BU trójai a Windows XP operációs rendszerben, a C:\windows\system32-ben lévő dmserver.dll állományt módosítja oly módon, hogy a fájl eredeti mérete nem változik. A fájl a Logikai Lemezkezelő Szolgáltatáshoz tartozik.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.

Bővebb információ: http://www.eset.hu/virus/toolbar-mywebsearch

5. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a novemberi fertőzések között: 2.17%

Működés: Az Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró-adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/toolbar-mywebsearch

6. Win32/Qhost féreg
Elterjedtsége a novemberi fertőzések között: 2.02%

Működés: Ez a fenyegetés fertőzött e-mail üzenetek mellékleteiben terjed. Futása esetén bemásolja magát a számítógép Windows\System32 mappájába, ahonnan a következő rendszerindításkor igyekszik a DNS, vagyis a Domain Name Service működését megzavarni. Mivel a drivers\etc\hosts fájl tartalmát módosítja, képes teljesen elérhetetlenné tenni bizonyos weboldalakat. Ezenkívül a támadók a fertőzött számítógép felett távolról teljes mértékben átvehetik az irányítást.

A számítógépre kerülés módja: e-mail üzenetek mellékletében terjed.
Bővebb információ: http://www.eset.hu/virus/qhost

7. INF/Autorun vírus
Elterjedtsége a novemberi fertőzések között: 1.87%

Működés: INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja:

fertőzött adathordozókon (akár .mp3 lejátszókon) terjed.

Bővebb információ: http://www.eset.hu/virus/autorun

8. Win32/Adware.Virtumonde.FP alkalmazás
Elterjedtsége a novemberi fertőzések között: 1.87%

Működés: Ez a kártevő szintén a kéretlen alkalmazások táborába tartozik az ESET kategorizálása szerint. Futása közben különféle felnyíló ablakokat jelenít meg. A trójai megkísérel egy távoli szerverhez csatlakozni, és onnan további komponenseket letölteni.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde-fp

9. SWF/Exploit.CVE-2007-0071
Elterjedtsége a novemberi fertőzések között: 1,78%

Működés: A SWF/Exploit.CVE-2007-0071 gyűjtőkategória olyan szándékosan hibás, preparált swf fájlokat jelöl, melyeket arra terveztek, hogy az Adobe Flash Player korábbi, javítatlan verzióiban egy sebezhetőséget használjanak ki. A védekezéshez fontos, hogy az Adobe flash lejátszót a már javított, 10-es változatra frissítsük. Bár a sérülékenységet a fejlesztők már 2008. április 8-án megfoltozták, még mindig rengeteg számítógépen található a régi, elavult és támadható verzió. A hibás fájl segítségével puffertúlcsordulást idézhető elő, amelyet aztán tetszőleges kód lefuttatására lehet kihasználni. A felismerés magát az exploitot azonosítja be, a hordozott kódtól függetlenül.

A számítógépre kerülés módja: böngészéssel vagy levélmellékletben kapjuk.
Bővebb információ: http://www.eset.hu/virus/exploit-cve-2007-0071

10. Win32/Autorun féreg
Elterjedtsége a novemberi fertőzések között: 1,59%

Működés: A Win32/Autorun egyfajta gyűjtőneve a Windows rendszerek alatti autorun típusú automatikus programfuttató fájlt használó károkozóknak. A kártevő az INF/Autorun egy variánsa, de nem az autorun.inf, hanem a hasonló funkciókat ellátó autorun.exe fájlt fertőzi meg. A baj bekövetkezésének egyik jele, hogy a számítógép működése drasztikusan lelassul. Míg az INF/Autorun a szöveges konfigurációs állományokat támadja meg és írja át, a Win32/Autorun csoport alatt azokat a végrehajtható állományokat értjük, amiket az autorun.inf betölt, elindít és lefuttat.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/804740

Kommentek:

Nincsenek hozzászólások.

Itt a Mikulás, gyorsan az ablakhoz!

2008.12.06. 06:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: ünnep mikulás hellókarácsony

Minden kedves Olvasónknak boldog, virgácsokban és vírusokban szegény; egyúttal csokiban és mandarinban gazdag **Mikulást kívánunk :-)**

Az idén sajnos csak egyetlen ember kaphatott ajándékot a Mikulástól a nehéz gazdasági helyzet miatt ;-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben

- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/807079

Kommentek:

Nincsenek hozzászólások.

Cserbenhagyásos gázolás

2008.12.08. 17:30 | Csizmazia István [Rambo] | 2 komment

Címkék: biztonság licenc veszély kezelés sonicwall

Kellemetlen egy szituáció, amikor **pont egy biztonsági program a licenckezelés hibája folytán védtelenül hagyja** a felhasználók gépeit.

Pedig sajnos pontosan ez történt nemrégiben a Sonicwall ügyfelekkel. A licencek kezelését végző szerver hibás működése miatt a múlt héten a tűzfalas és e-mail védelmi megoldások felhasználóinak igazi rémálomban volt része: átmenetileg spam, phising és kártevő szűrés nélkül maradtak. Számos **ingerült hangvételű bejegyzés is született erről a support fórumban**. A ComputerWorldnek jelentette az esetet egy biztonsági informatikus, melyben leírta, hogy a **SonicWall szerver licenckezelője resetelte a felhasználók egyébként érvényes licenckulcsait és emiatt azok érvényteleneknek látszottak**. Szerinte egy olyan szisztéma, amikor egyetlen szerver miatt ilyen mértékben meginoghat a felhasználók biztonsága, elmebeteg fantázia szüleménye.

A SonicWall szóvivője szerint ugyanakor **(vajon miért van az, hogy az embernek ilyenkor déjá vu érzése támad? ;-)** úgy nyilatkozott, hogy csupán **"néhány** licencnél tapasztaltak ilyen reset jelenséget, de a problémát azóta már kijavították. Egy technikai támogatásért felelős mérnök pedig úgy vélekedett, **egy licenckezelő szerver meghibásodásának nem kellene azzal járnia, hogy helyi termékregisztrációs adatok sérüljenek vagy elvesszenek**. Ez utóbbiban azt hiszem, mindannyian egyetérthetünk.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/811305

Kommentek:

r ek (törölt) 2008.12.08. 22:09:

De ja vue = déja vu

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.12.09. 0□:□8:□ □

Szia Fiveeeee!

Pedig írás közben végig déjá vu érzésem volt, hogy ezt a hibát már mintha máskor, egy másik életemben is elkövettem volna, vagy csak hiba van a mátri□ban?

Köszi szépen :-)

Száz barát négy nap alatt

2008.12.09. 11:20 | Csizmazia István [Rambo] | 16 komment

Címkék: profil kísérlet facebook hamis ismerős

Hallatlan tempóban **szaporodnak a sebezhetőségek**, köztük rengeteg ismert és még nulladik napi; már régóta kihasznált és éppen csak feljövőben lévő. Akarjuk - nem akarjuk, ezzel együtt kell élni, **hibamentes kódot egyszerűen képtelenség készíteni**, túl sok az eszkimó. Viszont azok, akik csak legyinteni szoktak a phishing esetekre, nekik **érdemes egy kicsit közelebbről megnézni ezt a social engineeringnek nevezett dolgot egy kíserlet kapcsán**.

Nem mindenki az, akinek mondja magát - ehhez még Arsene Lupin rajongónak sem kell lenni, mindenki megtapasztalhatta már. Emberünk **egy érdekes próbát tett az egyik közösségi portálon**.

Beregisztrált a Facebookra - de megtehette volna bárhol máshol is - és összeállított egy kamu adatlapot. Kellett hozzá egy új e-mailcím, majd jött a hasraütésszerű keresztnév választás - valami jól csengő, hangzatosra volt szükség - és ezt keresztezte aztán a blogjában használt álnevével, **és máris megszületett Dolus Carlsson**. Aztán kell még egy vonzó fotó - esetünkben ez Marcus Vick, 183 cm magas, 93 kg-os amerikai profi footballistát ábrázolja, de sebaj ;-), és máris lehet töltögetni az adatlapot.

Egy-két véletlenszerűen kiválasztott egyetem, középiskola, klub bejelölése csodát tehet. **Máris indulhat a "Kit ismerhetek□" című népi játék**. Az első harminc perc nehezen akart eltelni, de végül szép részeredménnyel zárult: tíz "barát" megszerzése volt a skalp, megtört a jég. **Innentől már olyan ez, mint a kitüntetések száma Brezsnyev mellkasán**: akinek már van, az minden pirosbetűs ünnepen kap egy újabbat, csak a legelsőt olyan pokoli nehéz megszerezni, akárcsak a gazdagoknak az első milliót (legálisan hehe) ;-)

A poént persze már lelőttük a címben - hasonlatosan a Benedek Elek: Hetet egycsapásra című meséjéhez, de tény: **alig négy nap leforgása alatt ennyi ismerősre lehetett szert tenni**. Itt még csak nem is arról van szó, hogy valaki nem ismer minket és téved, amikor azt gondolja, mégis ismer, **hanem ez a profil egy a valóságban nem is létező személyről szól, és mégis vannak ismerősei**. Igen, vannak, és akiknek ugye **Dolus Carlsson például már láthatja is a részletes adatlapját**. És a statiszikák keményen azt mutatják, hogy **az ismerősöktől érkező levelekre, üzenetekre, linkekre aztán már sokkal könnyebben kattintanak az emberek**, sok magyarázni való nincs is ezen.

Nem kell nagy jóstehetség ahhoz, hogy egy iWiW-en elvégzett hasonló történet is nagyjából ugyanilyen "sikert" hozna. **Mondhatják sokan, hogy ebben semmi □j nincsen. Hát ez az, és ennek ellenére mindig csak azt látjuk, csont nélkül és simán működik**. Úgy vélem, a miérteken kellene egy icipict elgondolkozzunk, magunkba néznünk, és valamit másképp csinálnunk...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/812651

Kommentek:

Manyizga (törölt) 2008.12.09. 12:22:4□

Az is hülye, akinek van ismerőse és valódi adata az iwiw-en. :)

dr. □ ilbur Swain 2008.12.09. 12:42:14

a puruttya.blog a myvipen csinált kamu adatlapot, jelölték is rengetegen :|
mondjuk ott nem az elmebajnokok sorakoznak

avejoe □ http:□ostobacsajok.blog.hu□2008□04□14□avejoe□szuletese□es□megdicsoulese 2008.12.09. 1□:1□:48

Én ugyanebben a cipőben járok, csak épp a "párkereső" oldalakon :)

ostobacsajok.blog.hu/2008/04/14/avejoe_szuletese_es_megdicsoulese

b. á. 2008.12.09. 1□:22:22

Részben egyetértek Manyizga véleményével, [antivirus.blog.hu/2008/12/09/szaz_barat_negy_alatt?fullcommentlist=1#c4198734] mondjuk én úgy fogalmaznék, hogy egy adatlapon ne legyenek olyan adatok, amiből túl sok személyesre lehet következtetni, az elérhetőségek közt pedig csak olyan szerepeljen, amire érkező kommunikáció teljesen szűrhető. [Viszont ha kint van egy mobilszámod, az, aki meg akarja szerezni, az életbe nem gondolja majd, hogy van azon kívül másik számod is, ha a neten van egy nyilvános!!!]

Normális ismerősöket felvenni szintén nem kockázat, ha 1. nem tud túl sokat és/vagy 2. nem hülye. Lényeg, hogy ne lehessen belőle veled kapcsolatos, kényes infót kitrükközni rajta keresztül. [legalábbis nagy valószínűséggel]

A WiW-et már rég ellepték a hülyék, attól meg a jó Isten mentsen meg minket, hogy a normálisabb helyeket, mint pl. a facebook.com, megszállják a droidok. Mondjuk már az egészen jó szűrő, hogy az alap nyelve nem magyar.

Golem 2008.12.09. 14:15:22

"Mondjuk már az egészen jó szűrő, hogy az alap nyelve nem magyar."
Mert az alig pár helyen beszélt angol nyelvterületein ugye se droidok, se hülyék. Ekkora egy sznob parasztot! Mi tényleg el vagyunk eresztve hülyékkel.

b. á. 2008.12.09. 14:26:18

Ki lehet forgatni a szavaimat, hát hogyne.

De ha jól belegondolsz, egy magyar anyanyelvű számára a magyar nyelvű site barátságosabb, mint az angol nyelvű. Ha van jobb ötleted arra, hogy miért a sokkal szarabb WiW a gyakrabban használt a magyar anyanyelvűek közt, írd meg.

üdvözlettel
sznob paraszt

P.S. komolyan kevesebb droiddal találkoztam a facebook-on

□ erwolf 2008.12.09. 14:□1:1□

Nem latom a poszt hirerteket? Rengeteg kamu "szemely" van az iwiw-en csomo ismerossel.
Velem is elofordult soxor, hogy bejeloltek olyanok, akiknek a szemelyerol lovesem nem volt. Ilyenkor a legegyszerubb visszaigazolni es par nappal kesobb torolni az illetot. Ez sertodesmentes es nem kell irogatni, mint a gumizsuzsik, hogy "ha bejelolsz, lecccci ird meg, hogy honnan ismersz es lecccci ne jelolj be, ha nem ismersz igazan!".

Az angol nyelv meg aztan tenyleg qrv@nagy szuro...:))

zsolti 2008.12.09. 14: 40

Egyszer bejelölt egy csaj myvipen, 34ezer ismerőse volt. Állítólag fotómodell, mondjuk sose láttam,vagy hallottam róla. Vannak ilyenek,lesznek is.

eklar 2008.12.09. 14:56:14

Ezeknek a közösségi oldalaknak a játékszabályai, az abból eredő kockázatok teljesen világosak. Aki ennek ellenére, saját elhatározásából közszemlére teszi a személyes adatait, majd csodálkozik, hogy azzal esetleg visszaéltek - az egyszerűen hülye. Ha az utcán elibénk toppan valaki, hogy áruljuk el ezt vagy azt az adatunkat, elküldjük a fenébe. Miért nagyobb a bizalom a teljesen ismeretlen és ellenőrizhetetlen terepen, ahol tudván-tudjuk, hogy szinte semmi sem az, aminek látszik?!

roni70 2008.12.09. 15: :58

A fecebook-ot át lehet állítani magyarra...
A postból meg az derül ki, hogy külföldiek voltak azon droidok, akik bejelölték nemlétező emberünket...
Amúgy a facebook-on lényegesen több bejelölést kapok vadidegen külföldiektől... Úgyhogy ez most tényleg teljesen mindegy...

Nowar http: kurkuma.blog.hu 2008.12.09. 15: 8:06

Én azért tartom meg és nem töröltem már réges-régen magam az ilyenről, mert jó információs forrás... Cégeknél kapcsolatot keresni... De, hogy sokaknak az itteni "élet" okoz örömöt... Végül is mi közöm hozzá, ha engem nem cseszeget?

Csizmazia István [Rambo] http: antivirus.blog.hu 2009.0 .0 . 19: 8: 9

Ez is eleg durvoid:
www.zoom.hu/belfold/egy-iwiw-foto-alapjan-kerult-racs-moge-41360.html?ref=hk

Csizmazia István [Rambo] http: antivirus.blog.hu 2009.0 .2 . 16: 6:52

Madarat tolláról, embert Facebook ismerőseiről:
www.technet.hu/techtud/20090324/gyilkost_jelolt_ismerosnek_kirugtak/

Csizmazia István [Rambo] http: antivirus.blog.hu 2009.04.27. 10:1 :50

Mire jó egy ismeretlen állítólagos ismerős a munka világában :-(
index.hu/tech/net/2009/04/27/a_facebook_miatt_rugtak_ki/

Csizmazia István [Rambo] http: antivirus.blog.hu 2009.04.29. 10:57: 4

Azért szerfelett bűbájos, ha ilyen felelős szervezetek sem bírnak a fejükhöz kapni:
hvg.hu/Tudomany/20090429_europai_valasztas_kozossegi_oldal.aspx

Csizmazia István [Rambo] http: antivirus.blog.hu 2009.05.20. 1 :10:25

"Letiltják a hülye neveket a Facebookon" - imígyen szóla a Zindex. Kérdés persze, mi számít és hol hülye névnek. Még egy korábbi munkahelyemen volt Tell Vilmos nevű főnököm, aki sosem tudott taxit rendelni, mert elküldték melegebb éghajlatra és letették a kagylót.
index.hu/tech/2009/05/20/letiltjak_a_hulye_neveket_a_facebookon/

AdWords számla érkezett...

2008.12.10. 15:56 | Csizmazia István [Rambo] | 2 komment

Címkék: google barracuda csalás számla adwords phishing adathalász

Biztonsági cégek megfigyelése szerint egyes bűnözői körök újabban **igen tudatosan az AdWords felhasználókra** utaznak.

A **Barracuda Networks munkatársai figyeltek fel** azokra a kéretlen levelekre, amelyeknek az ügyfelek jelszavainak megszerzése a célja. Maga **a levél úgy néz ki, mint egy hivatalos Google AdWords számla**, azonban a levélben található link **egy kínai szerverre mutat**. Ha a gyanútlan látogató begépeli a nevét és jelszavát, akkor utat enged a csalóknak a bankszámlájához.

A hirdetések fizetését hivatalosan kétféleképpen lehet intézni: vagy az internetes vásárláshoz hasonlóan **megadjuk a hitelkártya adatainkat** és annak biztonsági kódját (cégeknél a költségviselő cég bankkártyáét), **vagy pedig egy adott előre feltöltött egyenleggel gazdálkodunk**, aminek rendszeres pótlásáról, újrafeltöltéséről nekünk kell gondoskodnunk. Az utóbbi esetben maximum annyit bukhatunk, amennyi ez a kvóta. **A veszélyesebb az első eset**, amikor is a bankkártya adatok birtokában **a teljes összeget is eltulajdoníthatják**, és csak a bankkártya letiltásával vethetünk véget az ámokfutásnak.

A Barracuda többezer email üzenet átvizsgálása után jutott erre a felismerésre, valamint azt is észlelte, hogy **az ilyen csalárd levelek száma az utóbbi időben mintegy megtízszereződött**. Az átlagos adathalász forgatókönyvöz képest ebben kevés újdonság van, de ha a hirdetések szokásos céges ügyintését nézzük, **kevés helyen intézi az AdWords szolgáltatás fizetését MCSE, CISA vagy CEH minősítésű biztonsági munkatárs ;-).**

A konstrukció és az alapötlet mindenesetre ötletesnek és működőképesnek látszik, ezért a veszélyt nagyon is valóságosnak érezhetjük.

Ajánlott bejegyzések:

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás

- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/815139

Kommentek:

amitlatok (törölt) · http://amitlatok.blog.hu/ 2008.12.12. 18:00:51

Azok a régi szép idők, mikor még volt Adsensem.
Tiltólistára kerültem. Most a blogomhoz regisztrálnék újra, de kéne valaki, aki ezt megteszi. Segítetek?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.15. 22:09:50

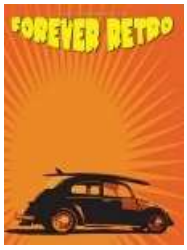
Szia!
Ez mit jelent, hogy tiltólistára kerültél, mi történt? Rosszul gondolom, hogy az új regisztrációhoz csak egy új email cím kell?

Retrospektív

2008.12.11. 11:49 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: test eset positive av comparatives minősítés advanced fales

Érdekes ága az antivírus programok tesztelésének az a módszer, amellyel **megállítva az adatbázis frissítést egy adott dátumnál** a későbbi hónapok folyamán megjelent kártevőket vizsgáltatjuk velük. Itt a vírusirtók ugyebár nem támaszkodhatnak a víruslaborban azóta feldolgozott és elkészített minták egyedi kódrészleteire, hanem **kizárólag a proaktív elemző heurisztikájukra vannak utalva**.



Az AV-Comparatives időről időre megvizsgálja ezt a képességét a versenyzőknek, és ilyenkor **egy adott napon befagyasztva a virusirtó programok frissítését a régi, több hónapos adatbázissal** rontanak neki tesztállományoknak. Esetünkben ez a 2008. augusztus 4.-i adatbázisállapotú tizenhat különböző vírusvédelmi program csörtéjét jelenti a 2008. augusztus 4. és 31. között beérkezett vírusmintákat tartalmazó tesztkészlettel.

A mostani riport kapcsán **érdemes egy picit elmélkedni az eredményekről** is. Tegyük fel, én egy AV motor vagyok, kezemben "tiszta állomány" feliratú táblával. Jön a tesztkészlet - benne fertőzött és tiszta állományokkal -, **és én mindegyiknél felemelem a táblát. Valószínűleg nem végeztem túl jól a munkámat**, mert bár igaz, hogy minden tiszta állománynál igazam lett, de nem ismertem fel a fertőzötteket. Ha megfordítjuk mindezt, és a "Fertőzött állomány" táblát ragadom magamhoz, és megintcsak gondolkodás nélkül emelem fel minden fájl esetében, **akkor igaz, hogy 100%-ban észleltem a kártevőket, de rettentően magas (minden tiszta fájl esetén) False Positive, azaz vakriasztást okoztam**. Nyilván, ez egy erőteljes leegyszerűsítés, de a felismerés hatékonysága optimális esetben az lenne, hogy a végsőkig kihasznált valódi felismerés egyúttal nem okozhatja a False Positivok számának emelkedését.

Akik kezdetektől követik a Vírusok Varázslatos Világa sorozatot, azok emlékezhetnek, pont a legelső cikkben volt szó arról, hogy **némely program annyira paranoid heurisztikát tartalmaz**, hogy egy sima Windows Calc.exe zsebszámológép alkalmazás UPX-szel való tömörítés után már kiveri náluk a biztosítékot. Nyilvánvalóan **nagy hiba minden futásidejű tömörítéssel rendelkező fájlt gyanúsként kezelni**. De mitől lesz gyanús egy fájl? Vannak a futásidejű becsomagolásnak is olyan **gyanúra okot adó ismérvei**, ami tiszta állományokban nemigen fordulnak elő:

- **többszörösen csomagolt állomány**: miért többször is, ha nem pont a felismerés megzavarása a cél
- közismert **feketelistás tömörítővel** készült állomány pl. Morphine
- egyedi fejlesztésű és **összezavart kódú tömörítővel** készült állomány
- olyan kisméretű fájl, amit **a mérete miatt nem lenne szükséges tömöríteni**, hacsak nem a pont a felismerés megzavarása a cél

A heurisztikát egyébként már körüljártuk egyszer jó alaposan a VVV 9. epizódban.

Mert **mit is okozhat egy vakriasztás?** Először is jó nagy pánikot. Aztán vannak esetek, amikor a hiba folytán akár az operációs rendszer elemeire történik a riasztás, ekkor előfordulhat, hogy **a törölt vagy karanténozott állományok miatt sérülhet a rendszer**, sőt akár működésképtelenné is válhat. Az idei évben több hasonló incidenssel is találkozhattunk, amelyek komoly riadalmat okoztak a felhasználóknál. Például a TrendMicro és az AVG is kiadott olyan hibás vírusszignatúra frissítést, **amely a Windows legális és tiszta állományaiban vélt felfedezni kártevőt**. Nem véletlen, hogy az AMTSO is komolyabb hangsúlyt fektet a tesztelési feltételek szigorítására, pontosítására.

Végül a 2008. novemberi teszt eredményeiről. A **NOD32 itt megszerezte az elérhető legjobb Advanced+ minősítést, és esetében jól látható**, hogy bár voltak termékek, amik magában a felismerési rátában ugyan jobban teljesítettek, viszont ezekhez szinte minden esetben nagyobb, sőt néhány esetben durván nagyobb hamis riasztás is tartozott.

Mr. False Positive :-)

A kettőt nem lehet egymástól elvonatkoztatni, ezt már a korábbi táblaemelési "clueless" kísérletünknél láthattuk. És természetesen azt is meg kell jegyezni, ennek a tesztnek **az eredménye önmagában egyedül nem minősít** egy terméket: például A jobb mint B, **viszont az ilyen tesztek eredményeinek hossszú távú egybevetése mindenképpen segít kialakítani, árnyalni** az egyes programok teljesítményéről alkotott képünket.

Forrás: http://av-comparatives.org/seiten/ergebnisse/report20.pdf

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/797358

Kommentek:

Nincsenek hozzászólások.

Ezüst érem

2008.12.12. 11:39 | Csizmazia István [Rambo] | 2 komment

Címkék: krisztián éves ezüst érem av comparatives összesítés pars

Nem csak Pars Krisztián kapott egy ezüst érmet, hanem **ezúttal a NOD32 vírusirtó** is.

Szoros küzdelemben ugyan, de **idén csak második lett a NOD32 az AV-Comparatives** éves összegzésében, **szemben a 2006-os és 2007-es évekkel, amikor az ESET programja lett az első**. A két retrospektív és két kézi keresést vizsgáló tesztsorozatot felölelő teljes esztendőt összefoglalva értékelő riportot ezen a linket lehet elolvasni.

Nem lehet mindig nyerni, ezúton gratulálunk az AVIRA-nak, **reméljük jövőre hasonlóan szoros versenyben megint a NOD32-t** választják majd az év vírusirtójának.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/818717

Kommentek:

tumtum 2008.12.14. 08:46:06

Gratulálok. De ha olyan ügyesek vagytok, segíthetnétek nekem. Tegnap erre jártam, olvasgattam és közben (milyen hülye vagyok), rákattintottam a postás képetekre. Hátha kiír valami vicces, vírust kaptál, feliratot. Nos, nem írt ki, de azóta, ahányszor bekapcsolom a gépet, a nod 32-m mindig karanténba helyez egy trójai módosulatot. Lehet ez csak véletlen is, de máshol, idegen helyen nem jártam. A fájl neve:
c:\windows\system32\drivers\restore.sys
Sajnos nagyon keveset értek hozzá, s nem tudom, mit tehetek.

tumtum 2008.12.14. 13:19:49

Na szóval, azóta a karanténból kitöröltem, s nem jelentkezett megint. Különben tényleg jó ez a vírusírtó, megfog mindent.

A piszkos tizenkettő

2008.12.16. 10:01 | Csizmazia István [Rambo] | 4 komment

Címkék: frissítés 12 top exploit secunia

Nem a Dirty Dozen folytatása vagy remakeje következik, hanem egy olyan összeállítás, amelyben **az idei esztendő 12 leggyakrabban támadott alkalmazása** van csokorba szedve.

Nos ezek voltak 2008-ban a ZDNet cikke alapján az exploitokkal leginkább támadott programok a Bit's9 szerint:

1. Mozilla Firefox: 2008-ban a **Mozilla tíz olyan sebezhetőséget is befoltozott**, melyek révén a támadók távolról tetszőleges fájlt futtathattak a gépen puffer túlcsordulási és emiatt átvehették a vezérlést. A hiba kihasználása szándékosan hibás szerkezetű URI (Uniform Resource Identifier) linkek, dokumentumok, JavaScript kódok segítségével történt.

2. Második helyen a szintén kedvelt célpont, az **Adobe Flash és az Adobe Acrobat állnak, a Bit9 információi szerint csak az idén 14 olyan biztonsági rés** befoltozására kényszerültek a fejlesztők, melyekkel ugyancsak puffertúlcsordulás segítségével tetszőleges kód lefuttatása vált lehetővé távolról végrehajtva. A teret ehhez zömmel a nem megfelelő input validáció és a használt paraméterekkel való "játszadozást" adta.

3. Harmadik **VMware Player, Workstation és egyéb virtualizációs termékek**. Olyan jelentősebb hibák szerepelnek itt, mint illetéktelen jogosultság szerzés a jó öreg directory traversal útján :-), ActiveX puffer túlcsorulással távoli kódvégrehajtás és DoS. Érdemes még itt megjegyezni, hogy igen-igen **kevesen vannak azok, akik a valódi PC-jük mellett a virtuális gépeiket is naprakészentartják a biztonsági frissítések** telepítésével.

4. Negyedik helyen találjuk a Sun Java fejlesztő és runtime környezetet (JDK, JRE). **A nem frissített rendszerekben a sebezhetőségek miatt könnyen előidézhető távolról végrehajtható kód létrehozás, törlés és persze végrehajtás** is a nem megbízható alkalmazásokon keresztül. A lista szerint itt is tíz ilyen sérülékenységet jegyeztek.

5. Szinte meglepődünk, hogy "csak" az ötödik helyen találjuk **az Apple QuickTime, Safari és az iTunes alkalmazást** ;-) A QT folyamatosan az egyik legnépszerűbb exploit lehetőség, amelyet távoli kódvégrehajtásra kihasználnak például állítólagos kodekhiány miatti videofájlok ürügyén, és ugyancsak távoli kódvégrehajtás és DoS támadás is lehet a végeredmény. A Windows alatt futó Safari böngészőkliensben három kihasználható hiba éktelenkedett, míg a korábbi foltozatlan iTunesnál MITM (Man in the Middle) támadási módszerrel lehetett operálni.

6. A lista hatodik helyén **a Norton termékek állnak** a 2006 és 2008 közötti verziókkal: puffertúlcsordulási hiba tetszőleges távoli kódfuttatási lehetőséggel.

7. Érdekes módon a közvetlenül utána **szintén egy vírusirtó áll, a Trend Micro OfficeScan szoftvere**, melyben négy különféle puffertúlcsordulási hibát is felfedeztek.

8. Nyolcadik helyet érdemelték ki a Citrix termékek, ahol illetéktelen jogosultság szerzésre nyílik mód manipulált Cisco VPN Client, Blue Coat WinProxy, SafeNet SoftRemote és HighAssurance Remoteinterface parancsok útján, **a végeredmény itt is távoli kódvégrehajtási lehetőség lehetett**.

9. Kilencedik helyen az Aurigma képfeltöltő rendszer áll a kiterjesztett képrinformációkon keresztül elérhető távoli kódvégrehajtásával.

10. Tizedik **a Skype alkalmazás, amely széles körben használt** és igen népszerű ingyenes VOIP szolgáltatást nyújt: itt scripteléssel lehetett saját kód végrehajtására bírni.

11. A Yahoo Assistant nálunk talán kevésbbé ismert, itt **memóriakezelési problémák kihasználásával lehetett** távolról kódok futtatni.

12. És végül a listát **az MSN Live Messenger zárja**, ahol a távoli támadók megtalálták annak a módját, hogyan szerezzenek meg jogosulatlanul kontakt információkat, és hogyan létesítsenek jóváhagyásunk nélkül audio- illetve videócsatlakozást.

Hogy **mit lehet tenni, hogy a "piszkos tizenkettő" ne árthasson nekünk?** Frissíteni, frissíteni, frissíteni:-) A sebezhezőségeknél persze **kettőn áll a vásár**: először is **a gyártónak kell minél gyorsabban a javítófoltot elkészítenie illetve megjelentetnie**. És persze az érem másik oldala, hogy **a felhasználóknál el kell érni, hogy ők pedig minél hamarabb ezeket le is futtassák**. Jót teszünk magunknak, ha Windowsos gépünket a Secunia Personal Software Inspectorral (PSI) is rendszeresen átvizsgáljuk, és a programokra vonatkozó javaslatokat megfogadjuk.

· **1 trackback**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/825117

Trackbackek, pingbackek:

Trackback: A Chrome, a Safari és a Firefox a legsebezhetőbb böngészők 2010.12.04. 22:24:09

Az Internet □xplorer durván lemarad a sebezhetőségek számá

Kommentek:

penge™ · http://www.thevenusproject.com/ 2008.12.16. 11:14:05

Hm... Nekem ezek közül csak Java Runtime van a gépemen. (Már ha a QT Alternative nem hordozza a QT sebezhetőségeket).

Némelyik ezek közül nem is meglepő. FF, MSN, Skype, Adobe...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.16. 12:01:15

Szia Penge!
Nem egyszerű a dolog, van aki kénytelen haszálni bizonyos dolgokat. Például ha iPhoneja van, jön a QuickTime. Én is QTA fun vagyok, de a szifon miatt kényszerhelyzetbe hoztak ;-)

Ha a munkahelyi policy megkívánja a Skype és/vagy MSN kapcsolattartást, akkor a Skype helyett nincs más alternatíva, az MSN helyett legalább van Pidgin és hasonlók. Aztán ahhoz is kell egy bizonyos fajta tapasztalat, hogy az ember mellőzze/kiváltsa legalább az Adobe PDF olvasót. Szóval egy átlag user szemével nézve (talán a Citrixes és VMWare-s cuccokat kivéve) elég riasztó lehet ez a kép, hiszen szinte mindent használt ezekből :-)

fabatka 2008.12.18. 13:18:17

Mintha a 9. hiányozna :) De az is lehet, hogy csak én nem találtam meg...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.18. 20:44:22

Szia Fabatka :-)

Milyen kilences hiányzik, de hát ott van az ;-)

Éles a szemed, mint a sasé. Köszi szépen, javítottam.

Miért romllikl el minden?

2008.12.17. 14:24 | Csizmazia István [Rambo] | 1 komment

Címkék: microsoft hiba explorer biztonság internet tévedés murphy exploit elromlik

A kézenfekvő választ Murphytől idézhetjük erre, és **kétséget kizáróan megállapíthatjuk, igaza volt :-)**

Emailben ajánlottak egy érdekességet a figyelmembe, **ami a Google Earth-szel kapcsolatos, de azért kicsit túl is mutat rajta**. Ha elrándulunk az Északi Sarkra (North Pole), láthatunk fotót is, amely arról tanúskodik, hogy nem volt könnyű oda eljutni.

Ám kisvártatva meglepődve láthatjuk, hoppá, mennyi további fénykép is van itt kérem, hát ez szinte hihetetlen. Hú, mondom, milyen sokan fotóztak az északi sarkon... Sorban nyitogattam a képeket. Aztán rövid úton rájöttem, hogy **_valószínűleg_ ide kerül minden olyan kép, aminek a feltöltésénél az emberek elrontják a koordináták beírását**. (fogalmam sincs, pontosan hogyan megy a feltöltés, de szinte tuti, hogy így van).

Még régebben hallottam egyszer a boldogult Szabad Európa Rádió Forgószinpad című műsorában (egyik kedvencem volt), amikor Franciaországban egy gyanútlan fogyasztót az első nulla frankos fizetési felszólítás utáni (kuncsaft nyaralni volt éppen) második be nem fizetett nulla frankos csekk után le is kapcsolták az illetőt a közműről. A **magyarazáskodásban aztán az szerepelt, hogy éppen most tértek át számítógépes adatfeldolgozásra**, és hát ezért csúszott be ez a fura hiba.

Elromlásról, elrontásról szól a napok óta izgalmat okozó (Linux és OS X rulez :-) Internet Explorer exploit is, ahol **állítólag tévedésből, véletlenül hozták nyilvánosságra a sebezhetőséget** konkrétan kihasználó kódot a kínai biztonsági kutatók azt hivén, hogy az már egy javított. De persze az is lehet, hogy gyorsan és nyomott áron MS részvényt akartak csak venni ;-), és a végén majd azt mondják: pardon. Az MS javítás állítólag szerdán, azaz ma már elérhető lesz. Az eset jól példázza, hogy **az ember vagy előidézi vagy megoldja a problémát, különben csak szimpla tereptárgy :-D**

Mindenesetre **minden számítógépfelhasználónak** fel kell kötnie a felkötendőt, hiszen a biztonsági cégek 2009-es jóslatait olvasva olybá tűnik, a sakk, foci, TV nézés mellett az exploit készítés és terjesztés is össznépi elfoglaltsággá válik sajnos: mindent támadnak, ami szembe jön. **Nem csak a számítógépes közeg szenved az állandó lopásoktól**, a való életben is ezt látjuk: ami fémből van és nincs lebetonozva, annak annyi. Még a Jézust ábrázoló babát is ellopják a templomból, helyére egy sütőtököt csúsztatva, ami **annyira meghökkentő és pofátlan, mint amikor Piszkos Fred Delhiben kilopta a háromezer éves Buddha rubin szemét**, és egy sorompó piros üvegjelzőjével helyettesítette. Nagy botrány lett, mert amikor a Buddha belsejében fellobogott az örömtűz, az Isten szeme azt hunyorogta a hívők felé, hogy: "Stop!... Stop!... Stop!"

A templomban mindenesetre GPS jelöléssel próbálkoznak megóvni tárgyaikat, mi pedig a számítógépeinknél **igyekszünk megóvni adatainkat, jelszavainkat a 2009-es esztendőben is**.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/827753

Kommentek:

gothmog 2008.12.17. 17:53:16

a panoramio-n én a "bökjél rá a térpéken" -vagy ilyesmi lehetőséget szoktam használni. Most nem emlékszem van e lehetőség a koordináták beírására, de a mapsen bejelölni sokkal egyszerűbb.

Kémprogram iPhone-ra évi 100 dollárért

2008.12.19. 14:47 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: apple iphone kémprogram flexispy

Ezt is megértük, december 21-én érkezik meg **az első kereskedelmi termékként kapható kémszoftver** az Apple iPhone okostelefonjára.

Mindjárt kétféle programra is felhívja a figyelmet az F-Secure blogja, ebből az egyik csak feltört készüléken működőképes. A másik hirdetés pedig mindössze **évi 99 USD összeg fejében egyszerű telepítést, észrevétlen működést**, továbbá teljes hozzáférést kínál a telefonhívások és SMS-ek listájához, valamint **az áldozat pillanatnyi GPS koordinátáinak követési lehetőségét is** ígéri. A Flexispy neve nem ismeretlen az érdeklődők előtt, más platformokon már korábban is elérhető volt a sokak szerint a legális és illegális határmezsgyéjén egyensúlyozó szoftver.

Az egyik érdekes kérdés mindenesetre az lesz, **mit kezd az Apple az így kialakult helyzettel**. A saját határköébe tartozó AppStore alkalmazásai közül **vaskézzel kigolyóznak minden olyan programot**, ami az üzleti érdekeiket a legcsekélyebb módon is sérti (például többet tud, mint a hivatalos változat, vagy a piaci érdekeiket veszélyezteti. Érvényes mindez a függetlenítés és a jailbreak körüli helyzetre is, ahol a szoftverfrissítések egyik célja éppen ezek megnehezítése volt.

(A programokra szándékosan nem mutatunk linkkel, nem akarunk ezzel is hozzájárulni a látogatottságuk emeléséhez.)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/831692

Kommentek:

Nincsenek hozzászólások.

Karácsonyi ajándékok vírusíróknak és irtóknak ;-)

2008.12.22. 14:16 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: játék vírus karácsony ajándék xmas trójai kártevő hellókarácsony mikróba

Napok óta olvashatjuk az Indexen a tárgykörben születő általános összefoglalókat, ezért úgy látjuk, **itt az ideje, hogy a mi saját testhezálló**, akarom mondani témánkbavágó ajándékok skáláját felvázoljuk, igyekezzünk az elképzelt lehetőségeket egy picit szélesíteni, illetve ehhez tippeket tudjunk adni.

Az alapötletet a gyermekszoba.blog.hu mai posztja sugallta, ahol a 10 ezer forint feletti kategóriában egy komplett trójai falovat láttunk potom 50 ezer forintért. **Innen már egyenes út vezetett a mai bejegyzéshez ;-)**

Hasonlóan fábók készít ötletes figurákat és készleteket a svéd Brio cég, ahol vírusokat is találhatunk, de **akár vírusos postafiókra is bukkanhatunk** a darabok között :-) Akik forintért szeretnének rendelni, nekik a Kópé Fajáték üzletében a helyük.

Plüss vírusok és bacillusok - igaz, ezek nem számítógépes vírusok, de akkor is vicces - a Giant Microbestől rendelhetőek.

Aki geekeknek való adventi naptárban gondolkodott, az így december 22. felé valószínűleg már eléggé elkésett.

OS X-eseknek pedig mit is ajánlhatnánk mást, **mint a Newton vírust :-)**

Ha minden kötél szakad, és már az idő szűke is fojtogatja torkunkat, nyomtathatunk Alex Dragolescu romániai vírusfestményeiből **egy szép képet, amit aztán bekeretezve átnyújthatunk**. Egy low budget CD keretben elhelyezett MyDoom portré biztosan felejthetetlen ajándék lesz :-)

Aki pedig nem ajándékozni, hanem csak játszani szeretne, annak ajánlhatjuk a Viruskiller flash játékot.

Kellemes Karácsonyt kívánunk Mindenkinek!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/836526

Kommentek:

Nincsenek hozzászólások.

Befoltozott biztonsági rés

2008.12.27. 09:50 | Csizmazia István [Rambo] | 1 komment

Címkék: patch security smart eset secunia

A **Secunia weboldal** karácsony előtt tette közzé, hogy az ESET biztonsági promjában szereplő biztonsági rést befoltozták.

Az ESET Smart Security integrált programcsomagjában előfordult sebezhetőség, amelyet illetéktelen jogosultság megszerzésére lehetett kihasználni, immár ki lett javítva. Eredetileg **egy preparált kártékony kód segítségével lehetett** manipulálni, de a 3.0.684 (vagy ennél későbbi) verziószámmal rendelkező változat már nem tartalmazza a hibát, amit a Secunia még így is a **viszonylag alacsonyabb prioritású "Less critical" kategóriába** sorolt be.

Érdemes tehát a biztonság kedvéért a programot az új változattal felülfrissíteni, amely már magyarul is elérhető a weboldalról.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/833286

Kommentek:

nando950 2008.12.30. 20:48:20

Tisztelt Blogíró !

A napokban sajnos egy igen különleges hibával, fertőzéssel találkoztam, immáron 2 alkalommal, és gyanítom, hogy az Ön cégének termékét is érzékenyen érinti a probléma.

Jelenség:
Operációs rendszer (XP prof. sp2) gond nélkül indul. ESET SS telepítve, napi frissítés, kézi frissítés is gond nélkül lemegy. Internetezni lehet, (notebook vezeték nélkül csatlakozik hálózathoz) bár a böngésző megnyitása előtt is folyamatos aktivitás a W AN-on keresztül. Weboldalak rendben bejönnek (már amelyik), bár kicsit lassú. (XP frissítés már kikapcsolva, hátha, de nem). Már előzőleg telepített egyéb védelmi rendszerek, keresők: Spybot S , malwarebytes anti malware. Ezek már nem frissítenek, weboldalaik blokkolva, el sem indulnak a programok. A SS kívül semmi antivírus nem indítható, telepíthető, blokkolva minden. Teljes keresés negatív eredmény. Process vizsgálatakor, semmi idegen, a SS advanced módban network con-ban semmi idegen. Megpingelve bármi weboldalt, minden 127.0.... IP-re átirányítva. ostok között semmi utalás a tiltottakra. Nincs kimutatható rootkit, (azért F SK /mbr lemegy, hátha, de nem). ESET többször újratelepíthető, semmi (Nélküle sincs használható eredmény). ComboFi nevezet prg sem futtatható. yakorlatilag semmi antivír az ESET SS-n kívül nem futtatható. Továbbra is folyamatos aktivitás a W AN-on.
Csökkentett módban minden ugyanez. TEMPek természetesen kipucolva, S STEM32-ből minden gyanús eltávolítva (megjegyzem, semmi e tra)

yakorlatilag az első gépen teljes rendszer újratelepítés segített, formázással. Most a második gépen már csak túra az egész, válaszkeresés.

Igazándiból nem tartom magam agytrösztnek, de eddig minden problémával egy jól bejáratott rutin+prg szerint sikerült megbirkóznom, mindig volt egy árulkodó folyamat, dll, stb. amit sikerült megfogni, kisz rni. e most semmi. Tényleg semmi.

Egy esetleges továbblépésre kérnék tanácsot. agy vmi programra, akár diagnosztikai, akár antispy, antivir.

Előre is köszönöm és megfogadom, kipróbálom a felmerülő ötleteket, javaslatokat. Reflektálok mindenre, amire tudok.

Sikeres MD5 hamisítás

2008.12.30. 18:40 | Csizmazia István [Rambo] | 43 komment

Címkék: ssl hacker hamis md5 tanúsítvány

Na jó, nem az SSL-t, hanem egészen pontosan sikeresen hamisították a biztonságos weboldalak egyik aláírási módját. Kétszáz darab clusterbe kötött PS3 és **két éles eszű hacker kellett** a mostani mutatványhoz.

Alex Sotirov és Jacob Appelbaum a 25. Chaos Communication Congress keretében bemutatott előadásában rukkolt elő azzal, hogy **sikeresen hamisítottak olyan SSL (Secure Socket Layer) tanúsítványt**, melyet a manapság széles körben használt modern böngésző kliensek teljességgel megbízhatónak ítéltek. Módszerük a jelenleg alkalmazott CA (Certificate Authority) **MD5 kódolási algoritmus gyengeségét használta ki**, és ezzel sikerült a hamis tanúsítványt elfogadtatni például a Microsoft Internet Explorerben és a Mozilla Firefoxban.

Man in the Middle módszerrel már eddig is lehetett trükközni a tanúsítvánnyal, de **ilyenkor még leleplező volt az ujjlenyomat**, ami árulkodott a buherálásról.

Hosszú távon valószínűleg a tanúsítványoknál nem fognak többé MD5 algoritmust használni, hanem a sokkal erősebb SHA-2, illetve a közelgő SHA-3 nyújtja majd a megfelelő megoldást. És hogy addig mi vár ránk? Biztosan lesz még részünk pár kellemetlen meglepetésben.

· 1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/849014

Trackbackek, pingbackek:

Trackback: BuheraBlog 2008.12.31. 02:53:02

Nem törték fel az SSL-t...Reménykedtem, hogy nem erre jövök haza, de nem volt szerencsém... Szóval a helyzet az, hogy a CCC-n volt egy előadás, melyben azt mutatta be egy több nemzetközi egyetemről és kutatóintézetből összeállt csapat, hogy bezony ma már…

Kommentek:

EZT IS NÉZD MEG KISPOFÁM..... (törölt) · http://tudtad.blog.hu 2008.12.30. 20:32:21

Ezek a hacker-ek :)

sajt · http://sajt.tumblr.com 2008.12.30. 20:53:44

Ez a kulcs nem a debianos problémából volt? Mert úgy könnyű... Ha meg nem, akkor ez tényleg elég ciki. Kérdés, hogy ez az egy eszköz eddig is megfelelő biztonságot nyújtott-e? Ugyebár tökéletes védekezés nincsen, a lényeg az, hogy a töréshez szükséges erőforrások ára több legyen, mint a megszerezhető javak összege.

kékféltégla 2008.12.30. 20:55:41

asszem kimegyek a garázsba, azt behozom a 200 PS3-am, úgy néz ki jó még valamire..

terran 2008.12.30. 21:03:52

a ps3 egyébként rohadt jó cucc kutatásokhoz használt számítógépeknek a benne lévő sokmagos, sok célra felhasználható chipek miatt.
az én egyetemen ha jól tudom kettőt használnak ilyen célokra.

Noinfo (törölt) 2008.12.30. 21:06:46

"Feltörték az SSL-t". Ujságiró-e vagy? Illene kicsit pontosabban és talán kevésbé szenzációhajhászan fogalmazni. MD5 collision gyártás meg már régóta ismert.

AzHofi 2008.12.30. 21:13:37

Nem baj, az éles eszű hecklerek letöltötték a scriptet, lefuttatták a haveroktól kölcsönvett játékautomatákon, és a végén kiírta, hogy hacking.... done. Végefőcím.

Szőke Kapitány 2008.12.30. 21:22:03

kb. :D

Lóri Vérkutya · http://lorimennimaraton.com 2008.12.30. 21:24:06

Nem az SSL-t törték fel, csak az egyik olyan algoritmust törték fel, amit használ. Az MD5 gyengeségére meg már 2004-ben felhívták a figyelmet, 2006-ban pedig sikerült olyan kettő darab azonos md5 hash-el rendelkező file-okat előállítani. Aki ezek után még bármilyen olyan alkalmazásban használja, ahol a biztonság szempont, az meg is érdemli. A jelenlegi SSL szabványban a tanusítványoknál nyugodtan lehet használni az SHA-1 algoritmust, amihez jelenleg nincs még semmilyen "törés", tehát az ilyen tanusítványok használata teljesen biztonságos.

Legközelebb talán legyen egy kicsit kevésbé "kamu" a cím...

Szőke kisfiú 2008.12.30. 21:37:14

Most találtam 20 millát az ágy alatt... legalább már tudom, hogy mire költsem. Veszek 200 ps3-at, és már marháskodhatok is.

Vajon nagyker hozzá lehet jutni ekkora mennyiségnél?

de miért pont 200?
És ha valakinek csak 190 van otthon?

agyvihar · http://agyvihar.blog.hu/ 2008.12.30. 21:49:39

Nem kell ahhoz sok pénz. Elég ha van egy botneted zombigépekkel, és akkor azokon is futtathatod.

kyanzes (törölt) 2008.12.30. 21:53:11

Következő cél legyen mondjuk egy 1024 biten titkosított kulcs. Bár lehet, hogy a nap hamarabb fogy ki hidrogénből, semmint hogy feltörjék a nyavajások. Érdemes már vacsi előtt elkezdeni a faktorálást, hacsak nem akad a hátizsákban egy kvantumszámítógép.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.30. 22:10:48

Jogos a két pont, de "Az MD5 ütközés ismét újra előtérbe került vala ottan" nem lett volna elég ütős cím ; -)

A dolog az átlag juzer szemével nézve viszont azt jelenti, a továbbiakban nem elég bambán kulcsokat meg lakatokat vizslatni a böngészőben a biztonságos kapcsolathoz.

Akinek meg csak 190 PS3 van otthon, magára vessen :-)

rodimus_prime 2008.12.30. 22:16:47

Át lehet böngészőben valahogy állítani az MD5-öt valamilyen SHA-ra? Csak érdekelne, de nem tudom hol lehet, vagy hogyan FF alatt. Valaki tudna segíteni?
Köszencs

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.30. 22:29:14

Akár ez, akár MITM támadás van, akkor vagyok én a Jani, ha mindig ellenőrzöm belépés előtt x plusz kattintással az SHA-1 ujjlenyomatot is. Szerintem az az igazi kérdés, hogy rajtad és rajtam kívül hány ÁTLAGFELHASZNÁLÓ fogja megtenni ugyanezt, ha egyáltalán érti ezt az egészet.

molnibalage 2008.12.30. 22:30:14

Mi az az SSL? El tudná valaki magyarázi egy nekem egyszerűen?

lolcode · http://isten.aldja.szalaiannamari.at 2008.12.30. 23:05:50

@molnibalage: secure sockets layer
vagyis egy titkos kapcsolati reteg a kommunikacioban ami olvashatatlanna teszi a kommunikaciot a harmadik fel szamara. roviden.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.30. 23:08:36

Ha egy weboldalon belépsz, ha nincs titkosítás (és nem használsz VPN-t sem), akkor az adatait clear textben közlekednek, ami nem szerencsés. Továbbá nem lehetsz biztos abban sem, hogy oda lépsz be, ahova szeretnél. Az SSL ebben segít: az adat mások számára nem olvasható, nem manipulálható, és hiteles.
wiki.hup.hu/index.php/SSL

Bambano 2008.12.30. 23:11:35

Melyik ssl-t törték fel? a 128 bitest vagy a 2048 bitest?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.30. 23:14:00

Ilyen ARP poisoningos mókát én is csináltam már, és simán lehetett látni a megfelelő tanúsítványt is az "áldozat" gépén, csupán egy helyen lógott ki a lóláb: az újjlenyomat nem stimmelt, magyarul végig nullák szerepeltek benne. Ilyenkor még az ismert IP címet is hiába ellenőrzöm (pl. showip plugin), mert az akár stimmelhet is, egyedül az ujjlenyomat mutatja meg a csalást.

Machiavelli 2008.12.30. 23:46:38

Ha két hacker ilyet tud, akkor képzeljétek el, hogy pl az NSA mire képes, amikor majdhogynem korlátlanok az erőforrásai és a költségvetése több, mint a Magyar Államé...

rodimus_prime 2008.12.30. 23:47:20

Már bocs, csak azzal, hogy így elbeszélgettek egymással, mi addig nem leszünk okosabb. Mert kb. Nulla dedós leírást mondtatok most, hogyan is lehet ssl-nél sha algoritmust használni, meg ezt az ujjlenyomatot is megnézni :=(

lifelike 2008.12.30. 23:50:06

hogy lehet vpn-t csinalni? nemreg egy ingyenes wifit uzemelteto ismeros vigyorogva mutatta hogy snifferrel miket szed ossze a nala hotspotozo emberektol...
msn chat szovegek+kepek+videochat, meg jelszavak orrbaszajba

szeretnem elkerulni ezt

Ralesk 2008.12.30. 23:58:23

@rodimus_prime: a SHA-1 (vagy SHA-2...) használata nem a te dolgod, hanem azé, aki a tanúsítványt a weblap részére kiállítja. Ha valamely komoly website 2004-5-6 óta IS még mindig csak MD5-ös lenyomatú certtel rendelkezik, az hülye.

Bambano 2008.12.31. 00:06:24

@lifelike: vpn-t? hova?

molnibalage 2008.12.31. 01:32:35

Akkor újabb amatőr kérdés. Honnan tudom, hogy akkor én most titkosított adatkapcsolattal nyomulok vagy sem?

PuruttyaIrto (törölt) 2008.12.31. 01:45:43

BushDoctor: miért ha egy közepes cég első embere mond valamit, akkor abban vakon bízni kell?

Szenzációhajhász módon elferdíti a valóságot ez a kis komisz denisz. De te csak nyalj be neki ha jól esik.

heliox 2008.12.31. 01:47:17

"MD5 titkosítási algoritmus gyengeségét használta ki"

Az MD5 *nem* titkosítási algoritmus, hanem lenyomatkészítő.

Az MD5 algoritmus 2008. január 1-óta Magyarországon nem használható tanúsítványokban.

Ha eltekintünk a cikkíró hozzá nem értésétől a cikk (vagy inkább az esemény) üzenete a következő:

Volt egy algoritmus, amit már elavultnak tekintett a szakma, mert úgy gondolták, hogy hamarosan gyerekek is képesek lesznek törni, ezért be lett tiltva a használata hivatalos tanúsítványokban. És most tényleg tudják törni.

Csak ámulunk és bámulunk, hogy tényleg meg lehet csinálni, amire mindenki azt mondta, hogy hamarosan meg lehet csinálni. "Hogy mire nem képes a modern tudomány!?!"

Megjegyzem: 2009. január 1-tól már az SHA algoritmus eddig szokásos legkisebb lenyomat mérete sem használható, csak míg az MD5 rögzített mérettel dolgozott, addig az SHA-ban ez paraméter.

the as · http://thelongestlistofthelongeststuffatthelongestdomainnameatlonglast.com/ 2008.12.31. 03:52:54

azok utan ez az egesz teljesen lenyegtelen, hogy mindenfele olcsossl szolgaltatok 15 perc alatt adnak tanusitvanyt akar paypal.com nevre is domain ellenorzes nelkul, amit boldogan lehet hasznalni, es teljesen valos, jol mukodo tanusitvany, browserekben elfogadott kiadotol.

atleta.hu · http://www.atleta.hu 2008.12.31. 03:54:23

> Jogos a két pont, de "Az MD5 ütközés ismét újra előtérbe került
> vala ottan" nem lett volna elég ütős cím ; -)

Marpedig az a feltetel az index fooldalra kikeruleshez. Valahogy te mindig ilyen felrevezeto cimekkel kerulsz ki veletlenul. :(Miert kell hulyiteni a nepet? Arra ott vannak a hozza nem erto, jol megfizetett indexes ujsagirok. Aki meg nem erti, az akkor sem erti, ha nem hivod titkositasi algoritmusnak az MD5-ot. Sot, az eddig sem ertette, es ez utan sem fogja. Az ilyen bejegyzesek meg csak novelik a katyvaszt a fejukben.

klacus 2008.12.31. 04:00:28

Nna ezért is érdemes a pénzért elbattyogni a bankba, az életednek a számítógép ne az értelme, hanem része, eszköze legyen.

Mi annak idején azért tanultunk a vírusok lélektanáról, hogy jobban tudjunk védekezni ellene, a fél osztály 3 hét múlva már képes volt olyan kódot írni amit az akkori keresők nem vettek észre. Nem tudom, hogy ez hova vezet...

atleta.hu · http://www.atleta.hu 2008.12.31. 04:13:30

Ehh, internal server error 500, bocs...

@klacus: > Nem tudom, hogy ez hova vezet...

Pl. az ocska viruskergetok fejlodesehez. Ha az osztalytarsaid nulla tanulassal kepesek voltak valamire, akkor a kifejezetten ezzel foglalkozo szakemberek evekkel, vagy evtizedekkel azelott tudtak ezt. Mellesleg a bank, ahova elbattyogsz az pont ugyanezekkel a modszerekkel kapcsolodik a tobbi bankhoz. Raadasul az alairasodat meg a szemelyidet meg mindig nagysagrendekkel olcsobb es egyszerubb hamisitani. De mindenki abban hisz, ami neki kenyelmes.

klacus 2008.12.31. 05:08:03

atleta.hu · www.atleta.hu 2008.12.31. 04:13:30

Amit írsz részben igaz. A virtuális dolgokkal azért csak pont annyi a baj, hogy virtuálisak. A mai világban az emberek 99,9 %-a nincs felkészülve a számítógépes csalások ellen.

A rendőrség pl képtelen ezt helyi szinten kezelni, ahogy a dolgok fejlődnek még vagy 20 év kell, hogy valami legyen. Továbbá írni olvasni a nagy többség tud

De ezzel a többség, a teljesség igénye nélkül, mit kezd?
mov edx,len
mov ecx,msg
mov ebx,1
mov eax,4
int 0x80
mov eax,1
int 0x80
section .data
msg db 'Hello, world!',0xa
len equ $ - msg
Üdv.

Amadeo 2008.12.31. 05:40:02

Nna. Én a címoldalról jöttem:) Nem bánom a kicsit átverős címet, megint megtudtam valamit. És igen, értem. Igaz, nem bölcsész vagyok:)

mavo · http://mavo.blog.hu 2008.12.31. 06:37:26

"Ha valamely komoly website 2004-5-6 óta IS még mindig csak MD5-ös lenyomatú certtel rendelkezik, az hülye. "

Ott a pont, igen. Teljesen mellékesen megjegyzem, hogy kb. két, de lehet, hogy inkább már három éve olvastam először arról a hibáról, amit valószínűleg most felhasználtak, csak akkor még nem volt hozzá megfelelő mennyiségű megfelelő sebességű eszköz egy kupacban.

A címmel egyébként nem az a baj, hogy blikkfangos, vagy hogy csúsztat, ugyanis egyáltalán nem csúsztat.

Hanem konkrétan nem igaz. Egy antivírus szakértőtől egyébként tulajdonképpen nem is gáz, ha nem tudja, mi a pontos különbség egy layer és egy algoritmus között, de azért jobban tette volna, ha legalább egy picit elgondolkodik a dolgon, mielőtt az év egyik legdurvább baromságát írja ki címbe.

Ha valami olyasmit ad címnek, hogy "Vigyázat, sikeresen hamisították a biztonságos weboldalak egyik aláírási módját", az is ölég blikkfangos cím, és még fedi is a valóságot, maximum arról lehetne vitázni, hogy az egyik legelavultabbat, mert attól a veszély még kvázi valós.

uzo 2008.12.31. 08:58:56

Nekem 2 éve tanították egyetemen az SSL működését, és az MD5 hibáját. Szóval az SSL nincs feltörve. Az MD5 van feltörve, de az meg már rég:)

kikezekazemberek 2008.12.31. 10:00:47

En is a fo oldalrol jottem, szerintem sincs baj a cimmel, nekem, mint laikusnak, teljesen ok, megint tanultam valamit.

Asszem 2008.12.31. 10:54:29

Én is. Laikus, címoldal, tanultam, asszem értem, bár én bölcsész voltam, de már elmúlt.

szilárdan... · http://www.flickr.com/photos/haazee 2008.12.31. 11:45:25

@klacus: azért ez durva volt, ugye tudod? Hozzak valami régi mainframe-es kódot még az ESZR időkből? ;)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.31. 11:50:47

Szia Mavo!
Köszi a hozzászólást, építőnek érzem, és hallgattam is a véleményedre.
BUÉK!

z8 2008.12.31. 11:54:41

a blog cime tényleg rossz lett..

TBC 2009.01.01. 09:35:46

Ha ez lenne a legnagyobb ferdítés a címlapra kerülő blogok és cikkek címében, az már rég ideális lenne. Sajnos manapság nem az a lényeg, hogy korrekten informáljuk a népet, hanem az, hogy minél hangzatosabb címmel adjuk el művünket. A legtöbb hangzatos cím mögött már a cikk elolvasása nélkül is tudom, hogy a cikk pontosan a címnek az ellenkezőjéről szól. (Ezt úgy általánosságban mondtam, nem erre a posztra értve. Ez még az elnézhető kategória.)
Ami a téma lényegét illeti: tény, hogy nincs feltörhetetlen rendszer. Nincs feltörhetetlen titkosítás, nincs hamisíthatatlan aláírás. Ráadásul minél összetettebb egy algoritmus, annál valószínűbb, hogy idővel találnak benne valami kiskaput.
A legnagyobb gond csak ott van, hogy a felhasználók tojnak rá, hogy pl. egy tanúsítvány érvénytelen, ugyanúgy folytatják tovább a böngészést. Erre már a főSulin is jól rászoktatják az embereket, amikor valamely rendszerüket - ETR, miegymás - érvénytelen tanúsítvánnyal üzemeltetik. Persze az útmutatóban szépen leírják, hogy ne törődjünk vele, ha nem érvényes, folytassuk nyugodtan... Akkor miről beszélünk?... Sokakban ez fog megmaradni, hogy "akkor nyomni kell egy folytatást", és az eszükbe sem jut, hogy épp így verik át őket. Mert egy szó nem esik ilyesmiről.

klacus 2009.01.02. 22:31:51

szilárdan... 2008.12.31. 11:45:25

Nosza :-))

atleta.hu · http://www.atleta.hu 2009.01.05. 01:47:55

@klacus: > Amit írsz részben igaz.

Ha csak reszben igaz, akkor vitatkozz vele. Ezt a filozofalgatast csak a vita (illetve a beismeres) eloli kibuvonak tudom tekinteni :). Ahogy irtam, digitalis alairast meg mindig nagysagrendekkel nehezebb hamisitani, mint valodi, nem 'virtualis' papirokat es alairasokat. Marpedig ha ez igaz, akkor ezek a megoldasok biztonsagosabbak. Persze a technika es a gepek (meg a matek) fejlodesevel mindig ujabb algoritmusokrol derul majd ki, hogy nem eleg erosek, de ez a Moore torveny ismereteben azert annyira nem meglepo.

> A virtuális dolgokkal azért csak pont annyi a baj, hogy virtuálisak.

Rizsa :). Az informacio mindig is informacio volt, csak a szamitogepes korszak elott kevesek ertettek meg, hogy a lenyeg ott rejtozik, hogy a bizonyitas, alairas, level, stb. az mind informacio, anyagtalan avagy 'virtualis' dolog. A penz is az, meg a kiralyi pecset is, csak nem latszik rajtuk elsore. Mi konnyu helyzetben vagyunk, nem kell nagyon okosnak lennunk, hogy ezt felismerjuk. A korabbi korok gondolkodoinak nehezebb dolga volt.

> A mai világban az emberek 99,9 %-a nincs felkészülve a számítógépes csalások ellen.

Az emberek nagy szazaleka semmilyen csalas ellen nincs felkeszulve, soha (ajanlott olvasmany Kevin Mitnick: A megtevesztes muveszete). Paradigma valtasok kozeleben pedig nyilvan tobbeket konnyeb beszopatni. (Gondolom a penz megjelenesekor konnyebb volt azt hamisitani, a mult szazad elejen ugyanez ment a valtokkal, itthon a bankkarya megjelenese utan egy szetszerelt atjatszos magnoval lehetett OTP kartyat masolgatni, stb.)

Vége az évnek, BÚÉK!

2008.12.31. 16:53 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: buék new happy year

Az **utolsó pillanatban** még egy gyors bejegyzés, értékelünk, kívánunk, semmi extra, ilyesmi...

Mozgalmas év volt, és a sablonszerű (Kellér Dezsős) válasz is megállja a helyét. Milyen év volt a 2008-as? Rosszabb, mint a tavalyi, de **még mindig jobb, mint a most következő:-)** És ezt a kártevő helyzetre is nyugodtan érthetjük. Villám statisztikánkban szereplő főbb tételek: 202 idei poszt, a NOD32 53. Virus Bulletin 100% díjának megszerzése, 56 (ha jól számoltam) kiadott Microsoft biztonsági javítás, 26 ezer fekvőtámasz és 296 - nagyrészt a Margitszigeten - lefutott km ;-)

3...2...1... Minden Kedves Olvasónknak fertőzésmentes, biztonságos és Boldog Új Évet Kívánunk!

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/850546

Kommentek:

Nincsenek hozzászólások.