

Nincs Karácsony kártevős képeslap nélkül

2011.01.03. 21:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [karácsony](#) [xmas](#) [képeslap](#) [trójai](#) [kártevő](#) [kéretlen](#) [zeus](#) [üdvözlőlap](#)

Törzsolvásóink már jól ismerhetik az **üdvözlőlapos** témát, ezekről [Psycho macska](#), vagy [akármilyen macska](#), no meg [tréfás kutya](#) és [karácsonyi köszöntés](#) formájában is írtunk már. Az ünnep most újra aktualitást adott ennek a dolognak.



Nyilván az ilyen önfeledt kattintgatások soha nem szerencsések, és **az sem lehet mentség, ha látszólag a Fehér Ház a feladó**. Habár ha valaki alaposan megnézi, esetleg elgondolkodhatna azon, mi köze a Fehér Háznak a [phonedevolverskd.com](#) címhez, de félé, ezt kevesen teszik meg. **Ha pedig a megnyitás nem otthon, hanem a munkahelyen történik**, az rögtön felveti a biztonsági képzés, oktatás, ellenőrzés hiányosságait is. Jó volna azt írni, hogy ez már egy olyan régi, olyan ismert, olyan nyilvánvaló dolog, hogy biztosan senki nem látogatott el a linkekre, de sajnos ez valószínűleg sosincs így.



A támadásokhoz használt **sebezhető PDF, Word és Excel állományok** segítségével igyekeztek a delikvens gépét a Zeus trójai egy variánsával megfertőzni és a botnet táncrendbe meginvitálni. Ez esetünkben a **jelszavak ellopását és a fertőzött gépről származó dokumentumok egy belorusz szerverre való feltöltését** jelentette - természetesen a tulajdonos tudta nélkül.



És itt jön be az érdekesség: a **különböző kormányhivatalokban, fontos és stratégiai munkahelyeken is rendre akadt olyan kíváncsi érdeklődő**, aki aztán így kiszivárogtatott különféle dokumentumokat - kicsit hasonlóan, mint [annak idején a Sircam](#), [ami a fertőzött PC-n mindig felkapott véletlenszerűen egy fájlt](#), ami lehetett bérjegyzék, bizalmas feljegyzés, bármi és már postázta is az addressbookban található embereknek.



Egy korábbi hasonló jellegű incidensnél a támadóknak 75 ezer számítógépet sikerült megfertőzniük, amelyek részben kormányzati, illetve magáncégek gépeit érintette. Ha csak annyit sikerülne elűteni a fejekbe, hogy **minden hasonlót előbb dobjanak be egy VirusTotalba, már ezzel is szebb jövő elé néznénk**. De persze a kéretlen levelek, linkek, mellékletek munkahelyi gépeken való totális ignorálása sem lenne ostobaság, erre azonban sajnos [szemlátomást még várni kell pár ezer esztendő](#).



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)

- [Akiknek a Captcha kínszenvedés](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2557731>

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.

Windowst frissíteni=MENŐ

2011.01.05. 14:25 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [microsoft](#) [spam](#) [frissítés](#) [hamis](#) [steve](#) [lipner](#)

A módját azonban érdemes helyesen megválasztani. Ez történhet kézzel indítva, futhat a háttérben automatikusan, de sosem úgy, hogy kérést email üzenetben kapjuk a ZIP állományt a biztonsági frissítéshez.



Kártékony levélmelléklettel érkező email terjed az internetizén, szerencsére nálunk csak azok lehetnek veszélyben, [akik megfelelő színvonalú angol tudással rendelkeznek](#), amellyel akár egy Ice-T számot is meg tudnak érteni. Az üzenet egyébként **látszólag Steve Lipner, a Microsoft egy biztonságért felelős igazgatójától érkezett** - na persze, én meg vagyok az angol királynő meg E.T. egyszerre - és arról értesíti a nagyérdeműt, hogy **egy ajajaj igen nagyon szerfelett fontos biztonsági patch érkezett**, és legyünk olyan jók, hogy a mellékelt KB453396-ENU.zip nevű frissítést saját biztonságunk érdekében mihamarabb lefuttatjuk.



Persze [az esetleges futtatás egy autorun-os kártevővel gazdagít bennünket](#), ha esetleg nem rendelkezünk naprakész vírusvédelmi programmal a számítógépünkön és [egészséges gyanakvással a fejünkben](#).



Összefoglalva érdemes tehát alaposan megjegyezni, hogy **emailben nem igazán érkezik** Microsoft biztonsági javító folt, **ezért azt megnyitni, sőt futtatni nem igazán hasznos szabadidős tevékenység** - legalábbis amíg piros hó nem esik, magyarul sohasem.

 Tetszik  10 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Majdnem mindenki átverhető adathalászzal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2562153>

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](#).



[Van_mikrohullámú_sütőtök? 2011.03.03. 16:53:38](#)

vicces, pedig vannak akik még ennek is behasálnak...

Mondjuk a magyar felhasználók, nem csak azért védettek, mert nem tudják mit akar az ürge, hanem azért is, hogy láthatóan ez egy .enu patch és az ugye nem megy a magyarított rendszeren :)

Lovon és trapézon, na meg mobilról is

2011.01.07. 18:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [blog.hu optimalizált mobilra nézet olvashatóság](#)

Mostantól **kényelmesebben lehet majd okostelefonról olvasgatni** a blog.hu-s tartalmakat, köztük minket is. Az [antivirus.blog](#) szeretetkesztőség ;-) nem akart kimaradni a jóból, emellett szívünkön viseljük olvasóink szemének egészségét, így hát rögtön megmutatjuk, milyen is lett a mobilnézetünk.



A mellékelt képeken a régi Tesco gazdaságos állapotot **hasonlíthatjuk össze az új, mobil sablonra optimalizált verzióval**. Ez magyarul az oldaldobozok nélküli, nagyobb betű méretes, gyorsabban töltődő mobil nézetet jelentik, amihez az elsők között készítettük el a szükséges mobilsablon képeket. Az új elrendezés miatt egy iPhone esetében gyakorlatilag **feleslegessé válik az állandó nagyítgatás, hiszen enélkül is jól olvasható** a szöveg, szemet erőltető műtyürek helyett pedig emberi méretű gombok segítik a navigálást.



Hogy meg legyen a helyes viszonyítás, a képeket a valós pixel méretben mutatjuk, vagyis ez semmilyen nagyítást nem tartalmaz. Természetesen olvasgatás közben a lap alján lévő [mobil/teljes] opció segítségével tetszés szerint **bármikor oda-vissza válthatunk a mobil és a hagyományos régi kinézet között**.



Reméljük, a jövőben [ezen hasznos újítással a jobb olvashatóság és a kényelmes kezelés miatt](#) további okostelefonos olvasókat nyerünk meg, és üdvözölhetünk majd az [antivirus.blog](#) hasábjain. Köszönet a fejlesztőknek :-)



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2567519>

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.

Jövőnéző

2011.01.10. 11:25 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [magyar jóslat adatok 2011](#) [nod32](#) [eset](#) [havi threatsense](#) [vírusstatisztika](#)

Pillantás bele egyenesen az üveggömbbe, ahonnan megpróbáljuk kiolvasni az ESET szakértőinek segítségével, vajon mi is várható majd 2011-ben vírus és kártevő fronton. Havi statisztikánkból pedig az is kiderül, hogy decemberben a vírusírók is pihentek.



Ha valaki jósnőhöz megy, nem igazán hat hitelesen, ha a csukott ajtón ez áll: "Előre nem látható okok miatt zárva". Szerencsére az ESET szakértői ennél sokkal konkrétabb és részletesebb jövőképről számolnak be. Szerintük az internet 2011-ben sem lesz biztonságosabb hely, és összegyűjtötték, hogy milyen fenyegetésekkel kell majd szembenéznünk.

Mobil vírusok: Az okostelefonok növekvő népszerűségének köszönhetően a mobil készülékeket érő támadások 2011-ben várhatóan megtöbbszöröződnek. A bűnözők számára az egyre növekvő piac jó terepet kínál, mivel a mobil biztonsági szoftverek használata még nem tartozik a felhasználói kultúra alapelemei közé.



Zombik támadása: Az ESET adatai szerint a botnetek mérete a számítógépeket zombivá tevő fertőzések számával együtt folyamatosan növekszik. A bűnözők a hálózatok irányítására a legkülönbözőbb csatornákat - például a Twittert - használják. Jó hír, hogy a biztonsági vállalatok egyre nagyobb sikereket érnek el a nagyobb botnetek lekapcsolásában, de ennek ellenére számolni kell a hálózatok számának növekedésével.

Vírusok Mac-en: A Java/Boonana.A tavaly novemberi megjelenésével egyértelművé vált, hogy az OS/X rendszerek elterjedésének köszönhetően a Macintosh számítógépek felhasználói már vonzó célpontot jelentenek a bűnözők számára. Annak ellenére, hogy az Apple operációs rendszere szigorú biztonsági beállításokat tartalmaz, a kevésbé hozzáértő felhasználók bedőlnek a megvesztő kártevőknek, és maguk kapcsolják ki azokat a korlátozásokat, amik megakadályoznák azok terjedését.



Mérgezett keresők: A legnagyobb keresők találati listájának eltérítése vagy mérgezése már 2010-ben is elterjedt volt. A technika lényege, hogy a bűnözők különböző keresőkifejezésekre optimalizálnak weboldalakat, majd megvárják, hogy ezek felkerüljenek a keresők találati listájának elejére. Miután ez megtörtént, megfertőzik őket, és rajtuk keresztül a felhasználók számítógépeit. Ugyan a keresők folyamatosan próbálják kiszűrni a mérgezett oldalakat a találati listájukból, a nagyobb volumenű támadásokkal szemben sokszor tehetetlennek bizonyulnak.



Fertőző közösségi oldalak: A közösségi oldalakon az adathalászok rendszerint valamilyen vicces, érdekes üzenettel és képpel vagy videóval keltik fel a felhasználók érdeklődését, majd egy alkalmazás segítségével megpróbálják megszerezni személyes adataikat. A problémát az jelenti, hogy lehetetlen megkülönböztetni, hogy egy adott bejegyzést valóban az ismerősünk írta ki saját üzenőfalára, vagy az egy kártevő működésének köszönhetően került oda. A támadások hatására a Facebook több beállítást is elérhetővé tett, melyek segítségével szabályozhatjuk, hogy a különböző alkalmazások készítői milyen adatainkhoz férnek hozzá. Ezeket azonban a felhasználóknak kell aktiválniuk, amire a legtöbben nem fordítanak kellő figyelmet. Az ESET szakértői folyamatosan figyelmeztetnek a Facebookon megjelenő új kártevőkre a <http://www.facebook.com/biztonsag> oldalon keresztül.



Vírustoplista - 2010 december

Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik a hazai felhasználók számítógépeit. Csak a számértékek változtak, de a top tíz kártevő sorrendje ugyanaz maradt decemberben is. Nincs semmiféle érdemi elmozdulás az előző havi listához képest, maradt a tizből nyolc trójai, és **változatlanul a Conficker féreg tartja a listán vezető pozíciót.**



A toplistán az előző hónapban felkerülő két trójai jelenthet csak viszonylagos újdonságot. Ezek közül az első a Win32/HackMS alkalmazás. Ez eredetileg egy Microsoft programokhoz készített kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. Míg a másik trójai a Win32/RegistryBooster alkalmazás, amely a hamis antivírus programokhoz hasonlóan a felhasználót valótlán riasztásokkal igyekszik rábeszélni a „program” fizetős változatának megvásárlására.

Mindenesetre kíváncsian várjuk, Magyarországon mikor kerül le végre az első helyről az abszolút csúcstartó Conficker féreg. Ez más országokban - Németországban, Ausztriában vagy az Egyesült Államokban például már meg is történt.

Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2010 decemberében a következő 10 károkozó terjedt a legnagyobb számban, és volt együttesen felelős az összes fertőzés 19.58%-ért.



1. Win32/Conficker féreg

Elterjedtsége a decemberi fertőzések között: 5.89%

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 eljárashívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárason 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.



A számítógépre kerülés módja: 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>



2. Win32/PSW.OnLineGames trójai

Elterjedtsége a decemberi fertőzések között: 2.71%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozóknak rootkit komponensei is vannak, melyek segítségével igyekeznek állományaikat és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatok titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



3. Win32/HackMS trójai

Elterjedtsége a decemberi fertőzések között: 2.57%

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítésekor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>



4. Win32/Tifaut trójai

Elterjedtsége a decemberi fertőzések között: 1.74%

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csrsc.exe és autorun.inf néven. A kártékony EXE fájl automatikus lefuttatásához külön bejegyzést is készít a rendszerleíró-adatbázisban. Működése során több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21tifaut>



5. Win32/Shutdowner trójai

Elterjedtsége a decemberi fertőzések között: 1.64%

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>



6. Win32/VB féreg

Elterjedtsége a decemberi fertőzések között: 1.47%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



7. HTML/ScrInject trójai

Elterjedtsége a decemberi fertőzések között: 1.08%

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



8. Win32/Mebrook trójai

Elterjedtsége a decemberi fertőzések között: 0.97%

Működés: A Win32/Mebrook.K trójai elsődleges célja, hogy további számítógépeket fertőzzön meg. Ehhez az ideiglenes (Temp) mappában létrehoz egy <szám>.tmp nevű fájlt, valamint a rendszerleíró-adatbázisba számos bejegyzést készít, illetve módosítja azokat, ha már léteznek. Ezenkívül megkísérel a google.com webcímrre is csatlakozni. Működése során tönkreteszi a merevlemez partíciós tábláját.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21mebrook>



9. Win32/RegistryBooster trójai

Elterjedtsége a decemberi fertőzések között: 0.94%

Működés: A Win32/RegistryBooster alkalmazás a hamis antivirus programokhoz hasonlóan hamis riasztásokkal igyekszik rábeszélni a felhasználókat a „program” fizetős változatának megvásárlására.



A számítógépre kerülés módja: Fertőzött weboldalról települ, vagy a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/registrybooster>



10. Win32/KillProc trójai

Elterjedtsége a decemberi fertőzések között: 0.57%

Működés: A Win32/KillProc trójai a fertőzött számítógépen különféle kártékony állományokat hoz létre a Documents and Settings mappában, emellett rendszerleíró-adatbázis bejegyzések létrehozásával gondoskodik arról, hogy a számítógép újraindítása után is automatikusan lefuthasson. Fő célja, hogy a megtámadott gépről adatokat szerezzen meg, és naplózza a billentyűleütéseket.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/killproc-a>



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Dropbox csálival terjedtek a kémprogramok](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2573506>

Kommentek:

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

Nincsenek hozzászólások.

Háromszoros élvezet az adathalászkoknál

2011.01.12. 15:21 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [mobil](#) [email](#) [phishing](#) [adathalászat](#) [trusteer](#)

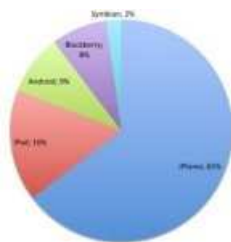
Az asztali gépek felhasználóihoz képest háromszor nagyobb valószínűséggel esnek áldozatul adathalász támadásnak az okostelefonosok egy friss tanulmány szerint.



Az emberek többsége szereti folyamatosan, illetve napközben többször is ellenőrizni elektronikus levelezését, és mivel az **okostelefonok mail- illetve böngészőkliensének korlátozott a funkcionalitása**, illetve hogy **a kijelzőn való helyspórolás miatt csak szűkebb információk láthatóak** - nos mindezek együttesen is okai lehetnek annak, hogy a mobilosok védtelenebbek, nagyobb veszélyben vannak.



A vizsgálat során számos **adathalászzal is foglalkozó webszerver logját elemezték** a szakemberek. A [Trusteer szerint az iPhone, Blackberry tulajdonosok](#) lassan már **többször nézik a levelezésüket hordozható eszközeikről, mint az asztali PC-jükről.**



És a kis képernyőn **nem mindig láthatják a levelek pontos feladóját teljes emailcímmel**, illetve a hivatkozott weboldalak címei is manipulálhatóak, emiatt pedig nehezebben tudják felismerni, kontrollálni az ilyen incidenseket. A felmérés eredménye szerint egyébként **nyolcszor több iPhone tulajdonost csapnak be, mint Blackberryst.**



Emellett az is megfigyelhető, hogy a **mobilos levélolvasáskor igen jellemző a sietség és kapkodás** - amíg a busz, metro, villamos megjön, még gyorsan megnézem, megválaszolom - és ezek is nagyban elősegíthetik az adathalász csapdába való besétálást.



Mobilon lehetőleg sose kattintsunk kéretlen linkekre, ha pedig esetleg mobilról bankolunk (ami azért eléggé ellenjavalt), akkor legalább mindig kézzel írjuk be vagy a könyvjelzők közül vegyük az ehhez szükséges URL-t.



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Ez történik a weben egy perc alatt](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2578265>

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.

Anyád napja

2011.01.14. 11:40 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [internet diák tanár cyber zaklatás bullying](#)

Sajnos régóta ismert, hogy **az iskolákban csak cyber bullying** - ezt leginkább [számítógépes eszközökkel elkövetett zaklatásnak](#), vagy lelki terrornak fordíthatnánk - eléggé elterjedt szabadidős tevékenység, és [néha az áldozat öngyilkossága is előfordul miatta](#). A híradásokból az is jól látszik, a tanárok ilyesfajta zaklatása sem ritka.



Az már szinte nem is számít újdonságnak, ha valamilyen [lövöldözés történik egy amerikai oktatási intézményben](#), ez [Magyarországon ha nem is példa nélküli, de szerencsére ritka](#). A tanulók **virtuális kiközösítése, zaklatása** azonban már **gyakrabban** előfordul, és időnként a tanárok is célkeresztbe kerülhetnek.



Egy friss híradás szerint egy nevadai iskolában, Carson Cityben [az egyik 12 éves tanuló szervezett a tanáraik ellen ilyen elektronikus támadást](#), aminek még nevet is adott: "**Attack A Teacher Day**". Barátaihoz és osztálytársaihoz intézett felhívást - mintegy száz tanulóhoz - hogy csatlakozzanak és együtt hajtsák végre azt. Tizennyolcan jó bulinak tartották - egyikük még azt is írta, hogy halál rá - és **válaszukban támogatásukról biztosították a középiskolás lányt**.



Hatukat azonban a tervezett nap előtt felkeresték a hatóságok és letartóztatták őket. A lányok azzal védekeztek, hogy **mindez csak ártatlan tréfa volt, és a rendőrség szükségtelenül túl komolyan vette azt**. Egy angliai iskolai szervezet, az ATL felmérése szerint [a tanárok mintegy 15 százaléka szenvedett már el 2009-ben valamilyen számítógépes zaklatást](#) tanulóiktól vagy azok szüleitől, **negyedüket pedig vádolták már meg hamisan**.



Hogy **a tanárok helyzete úgy általában véve is egészen más**, mint mondjuk jó húsz-harminc éve, az jól kiderült abból, amit [Bodó Balázs mesélt](#) valamelyik Hacktivity-n. A diákok ma már nem csendben ülnek, hanem előadás közben folyamatosan neteznek, csetelnek, messengereznek, facebookoznak, sőt **valós időben ellenőrzik a tanár mondandóját a Google-val és beszélnek, ha szerintük esetleg téved valamiben**. Egy biztos, a tekintélyre nehezebben, **de legalábbis merőben másképpen** tudnak szert tenni, mint évekkel korábban.



Az is nyilvánvaló, hogy [bárminek a fotóival vissza lehet élni, hamis profilt](#), vagy az illetőt rossz színben feltüntető álhíreket lehet létrehozni - [ebből a hamis pedofilvád a legdurvább](#) -, vagy üzenetekben fenyegetni is könnyű, és **ezeket pusztán technikailag megakadályozni gyakorlatilag lehetetlen**. Antivírus nem véd ellene, maximum a feltöltött, megosztott személyes adataink alapos szűrésével, és a közösségi portálokon a megfelelő biztonsági beállításokkal védekezhetünk valamennyire.



Azt mindenki döntse el maga, hogy ezek a változások mennyiben jók, mennyiben újak, mások mint régen: **a Facebookos lejáratások csupán átvették a székre tett rajszög helyét, vagy egy egészen új irányt vett a tanár-diák viszony**, amit valamilyen szinten muszáj kordában, egészséges határok és törvényes keretek között tartani.

Ha valaki ismer idevágó megbízható magyar adatokat, statisztikákat, kommentelni ér.



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Akiknek a Captcha kényszerű](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2582658>

Kommentek:

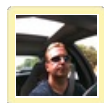
A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói tartalomnak minősülnek, értük a [szolgáltatás technika](#) üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a [Felhasználási feltételekben](#).

Kravitz 2011.01.14. 16:55:02

"Tizennyolcan jó bulinak tartották - egyikük még azt is írta, hogy halál rá - és válaszukban támogatásukról biztosították a középiskolás lányt."

:DDD

Igen komoly f*szverés, hogy egy 300millióos országban kivonul a SWAT, mert pár kamasz aszonta, "aBakónéfulladjonmeg!!!!".



Benkovics Tomi 2011.01.15. 07:13:31

itt mindenre kivonulnak.... csak kiálts a gyermekedre, egy szomszéd hívja a zsarukat... szvsz ez igaz...



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.01.15. 09:09:47

Szia Kravitz! Üdv a blogon :-)

Egyetértek veled abban, hogy mindent a helyén kell kezelni, és mondjuk alaptalan fenyegetéseknél gondolhatjuk, inkább a gyilkosokat, rablókat üldöznék.

De ... hehe, ugye érezted, hogy lesz egy de is? Szóval szerintem mindez nem ok arra, hogy ha nem világháború van, gyilkosok üldözése, akkor a kisebb dolgokra nem kell egyáltalán figyelmet fordítani. Gondolj csak a szeméttelésre, vagy a kutyaürülékre az utcán. Ezek is kezelni kell, hogy ne járjunk benne térdig.

A másik pedig az, hogy szerintem az a helyes hozzáállás, ha valaki akkor is tud empatikus lenni, ha nem vele történik a baj, nem őt magát fenyegetik. Itt van például ez a vicces videó:

auto.indavideo.hu/video/Hulye_kamionsofer

Ha megnézed, lehet, hogy még nevetsz is, esetleg megrökönyödsz. De ha ő miatta, vagy egy hasonló alak miatt végtelenül meghalna a csecsemőkorú gyereked a feleséged szembejövő vétlen kocsijában, már nem is tartanád annyira viccesnek. Az érett gondolkodás közvetlen saját veszteség nélkül is objektíven értékeli.

Úgyanígy ha valakire rászállnak, és ki akarják csinálni, az nem jó dolog, még ha nem is a te lányod, vagy a tanár mamád az, aki sírva jön haza az iskolából. Amikor valaki felakasztja magát, akkor utólag meg mindenki okos, hogy miért nem tettek valamit, miért figyeltek jobban.

Abban neked is és Tominak is igaza van, hogy mindez az USA-ban (ne rakd a macskád a mikróba) már túlzás szinten működik, sőt van is már swatting nevű terminus technicus arra, ha valakire ártatlanul úgynevezett "viccből" küldenek ki kommandósokat.

www.virushirado.hu/hirek_tart.php?id=1215

Ennek ellenére mindig minden egyes esetet érdemes megnézni, ahogy a nincs olyan bombariadó, amit ne ellenőriznének, bármelyik fenyegetés végződhet rosszul, ha nem ellenőrzik.

Amikor az App viszi a lakcímet, telefonszámot

2011.01.17. 12:40 | [Csizmazia István \[Rambo\]](#) | [8 komment](#)

Címkék: [facebook](#) [lakcím](#) [app](#) [telefonszám](#) [otthoni](#)

Ha valamivel lehet élni, akkor sajnos visszaélni is lehet. Nincs ez másként a Facebook alkalmazásokkal sem, itt is [rendszeresen felbukkanak kártékony kódokat terjesztő](#), vagy éppen enyveskező fejlesztők.



Miután [a Facebook a fejlesztők felé elérhetővé tette User Objectként a felhasználók lakcímét és mobiltelefonszámát](#) is, emiatt **Graham Cluley** szerint rosszindulatú támadók még soha nem voltak képesek ennyire egyszerűen olyan csalárd alkalmazásokat készíteni, amivel ezek megszerezhetők számukra.



Az ilyen személyes adatösszegyűjtések célja [sok esetben SMS spam küldése, vagy az információk értékesítése harmadik fél számára](#) - a vevők pedig általában reklámküldők. Szerencsére az adott felhasználó jóváhagyó kattintása után - [egyelőre?](#) - csak a saját lakcím és telefonszám (kapcsolattartási információ néven) kerül kiolvasásra, és nem az összes baráté, ismerőse.



A jótanács a "Nem kapsz két pofont a kocsmában, ha nem is mész oda egyáltalán" mintájára: **ne adjuk meg lakcímünket és otthoni vagy mobil telefonszámunkat**. Ha esetleg korábban mégis megadtuk, íme az égi jel arra, hogy most jól kitöröljük. Kivéve persze ha a kénytelen reklámajánlatok nagy barátai vagyunk.

 Tetszik  20 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](#)
- [Majdnem mindenki átverhető adatahalászával](#)
- [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/2589732>

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](#).

Civitas Fidelissima 2011.01.17. 14:51:04

A mobilszámomat nekem pont azért kérte el regisztráció után a fb, hogy ne kelljen állandóan megerősíteni a beállításaimat. Azaz szinte kötelezett a megadására a kényelmes használatért cserébe. Hogy is van ez?

MetálFater (törölt) 2011.01.17. 14:59:51

De a legjobb, ha nem is használjuk a Facebook nevű, - egyébként semmi értelmes dologra nem használható - alkalmazást.

Én, és az ismerőseim olyan jól megvagyunk nélküle!

tsimike 2011.01.17. 15:01:02

Mi az a fb? Milyen jó hogy nincsenek ilyen gondjaim...

Shmoo 2011.01.17. 15:07:17

@Civitas Fidelissima: Kényelem vagy biztonság... hmmm...

@MetálFater: Ízlések és pofonok. Nekem pl. kifejezetten jó, megkönnyíti a kapcsolattartást egy halom külföldi ismerőssel, volt (külföldi) osztálytárrsal.

De lakcímet, mobilszámot publikussá tenni a neten? Pf...

magyar bucó 2011.01.17. 15:36:56

Se lak címem, se telefonszámom nincs megadva a fész búknak.

Aki mégis kiszedi belőlük, az meg is érdemli. :)

is 2011.01.17. 16:24:36

@Civitas Fidelissima: en nem adtam, aztan megsem kell semmit soha megerositenem. ugyhogy ugy van ez, hogy teged atvagtak, te meg beszoptad.

raadasul a kényelmes használat az relativ, es minden kényelem a biztonság rovasara megy. de tudod mit: rendkívül kényelmes életet biztosítok neked: bevasarolok helyetted, es bepakolom a hutodbe a kaját. csak add oda a lakaskulcsod, meg mindig tolem vasarold a kajadat. belemennel?



numlockholmes 2011.01.18. 21:40:42

Ez a lakcím-lenyúlódsi máshol is előkerül az informatikában - még hozzá az Androidos telefonoknál. A feltelepített Androidos Appok bizonyos jogosultságokat kérnek. Sokszor láttam olyan külső forrásból származó alkalmazásokat, amelyeknél követelmény volt az internet hozzáférés mellett, hogy hozzáférjen a GPS adatokhoz hogy tudjon telefonhívást indítani vagy épp a telefonkönyv bejegyzésekhez akart hozzányúlni - pedig csak játékok voltak.

Megtudhatják a tartózkodási helyed, a barátaid telefonszámát és akár a Te költségeidre a nevedben küldhetnek reklámot az ismerőseidnek sms-en keresztül.

Az más kérdés, hogy a lakcímeddel mit tudnak kezdeni? Mondjuk, hogy Makkosmárián tengetem az unalmas életem? Szerintem az semleges az adat tolvajok számára.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.01.19. 08:11:10**

Ideiglenesen leállították ugyan a dolgot talán a titakozás miatt, de gondolom az értékes reklámbevételek reményében előbb-utóbb megy majd tovább a dolog:

www.huffingtonpost.com/2011/01/18/facebook-home-addresses-phone-numbers_n_810173.html

Kártékony antivirus linkek - villám őrjárat 3.

2011.01.19. 14:00 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [link hamis antivirus](#) [kártékony patrol](#)

Egyfajta röpke "Link Patrol" keretében teszünk időnként kisebb őrjáratot hamis vírusok, a hamis vírusot terítő linkek nyomában, különösebb sallangok, terjedelmesebb tiszteletkörök nélkül. Már a spájzban vannak az Antivirus Studio 2010 és 2011 programok.



Nem csökken a roham hamis vírusok terjesztői részéről. Már [megemlékeztünk a 2011-es évjáratról](#), és persze arról sem szabad elfeledkezni, hogy nem csak vírus, [hanem egyéb célú: hamis lemezkarbantartó, adatmentő](#), halász, vadász, madarász, [szerzői jogvédelmi fenyegetős](#), és még a jó ég tudja milyen ezerfejű hidra formájában találkozunk vele. Egy a lényeg, [a teljes verzióért pénzt követel](#).



[Nincs ez másként az Antivirus Studio esetében sem](#), a belépés díjtalan, a kilépés bizonytalan - [akár a Grand Hotel nevű műintézményben](#). Hogy kitűnő széklábak vannak-e vagy ötőrai gabona pálinka, erről végképp nincs tudomásunk. Ami viszont van, [Augiász istállója a Registryben, felpattanó ablakok, kézi gyomlálás, egyedi remover kapálógépek kényszerű bevetése, szenvedés](#) a teljeskörű leszedéssel, tisztítással. Már szinte látjuk lelki szemünkkel, hogy [a következő kamuprogram neve talán stílszerűen Rogue Antivirus Detector 2011 lesz ;-\)](#)



Mit lehet tenni? Van-e még reménye az emberiségnek vagy katapultáljunk a Holdra? **Valódi megbízható gyártótól származó antivírust, internet biztonsági csomagot használjunk; ha telepíteni akarunk valamit, azt közvetlenül a fejlesztők weboldaláról töltsük le; rendszeresen frissítsük a rendszerünket és minden új programnak nézzünk alaposan utána.**



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.](#)"**



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

Kommentek:

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

sorsolo 2011.01.22. 13:03:11

lehetséges az, hogy a "system tool" nevű fake antitivirus program az eset smart securities teljesen friss változatát kilövi és telepíti magát?

azt hiszem, hogy a skipscreen.com oldalról kaptam a fertőzést, ahonnan az egyébként létező (skipscreen nevű) firefox plugint akartam letölteni (az igazi plugint korábban meglegedéssel használtam, s most egy újratelepítés miatt akartam újra letölteni). amikor láttam, hogy az oldalról letöltött file kiterjesztése exe (nem pedig xpi), akkor már tudtam, hogy ez nem az, mint amit én akarok, ezért nem futtattam, de ekkor már késő volt. az eset logjában találtam kb. 10 bejegyzést: egy néhány perces időintervallumban 2-5 másodpercenként próbált bejutni, gondolom 10-szer sikeresen verte vissza az eset a támadást, de 11-edszerre meghátrált.

nem 100%, hogy erről az oldalról kaptam a fertőzést, de az biztos, hogy egy teljesen friss antivir adatbázissal rendelkező 4.2-es eset smart securities volt szolgálatban, amikor egyszercsak az antivir távozott a memóriából, a kártevő meg elkezdte a saját üzeneteit küldözgetni, blokkolni majdnem minden program futtatását, stb. bőven info róla itt: www.2-spyware.com/remove-system-tool.html

nekem szerencsém volt, mert csak az egyik xp felhasználói fiókot fertőzte meg, a másik accountról belépve viszonylag egyszerűen el tudtam távolítani.

szóval érdemes anti-malware, anti-spyware programot is futtatni az eset mellett? 2-3 év alatt mindig megvédett az eset, egyetlen alkalommal sem kaptam fertőzést, igaz eddig a 3-as verzióját használtam. most álltam át a 4-esre, és szinte azonnal kaptam egy kártevőt. érdemes visszaállni? a 4-es rosszabb??



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.01.23. 10:08:45

Szia Sorosolo!

A skipscreen.com-ra én is gyorsan elmentem, de már "nem volt szerencsem", csak XPI-vel talalkoztam. Olyan tomegben fertoznek mar meg weboldalakat, hogy gyakorlatilag barhol lehet kartevoval talalkozni, nem csak xxx, meg warez helyeken.

Szerintem a 4.2, vagyis mindig a legfrissebb változatot érdemes használni, és egyfelől a beállítások szigorításával tudsz játszani (valós idejű védelem, kiterjesztett ehurisztika használata, stb., másrészt batran lehet mellette pl. Spyware Terminator, A-Squared, SpyBot SD programokat használni, nem akadnak össze.

sorsolo 2011.01.23. 20:40:48

szia István!

köszönöm a választ.

megnéztem, még mindig ott van a skipscreen oldalán az exe, bár a noscript láthatatlanná teszi, illetve linuxos gépről sem láttam tegnap. ha megnézed az oldal forrását, abban biztosan megtalálod a hivatkozást a dl.skipscreen.com/files/SkipScreen-Setup.exe fájlra. ezen a részen keresd:

"Never download music without it.
add to firefox
(Windows OS) other platforms"

az anti spyware programokkal együtt használt eset rossz hír számomra, amennyiben arra utal, hogy ezekkel szemben nem ad teljes védelmet az eset. a félgigas memóriával bíró 1.6-os celeronom erőforrásainak túl nagy részét emészténé fel két védelmi program, akkor inkább kockáztatom a spyware beszerzését, és a tarsolyomban tartok egy gyorsan helyreállítható windowst (azaz image fájl a windows rendszert tartalmazó partícióról).

üdv!



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.01.27. 14:01:40

Megnéztem ezt a skipscreen.exe-t, de a VirusTotal szerint ez látszólag nem fertőzött, 23-án sem, és ma sem.

www.virustotal.com/file-scan/report.html?id=5069715cdb642761aef2e117d15d7e38fc40981ab5da7cc374a6513b79e2569a-1296123202

Az exe WinXp és Win7 alatti alaposabb elemzése szerint sem a naplózott hálózati aktivitás elkapott csomagjaiból, sem pedig a módosított/létrehozott Registry kulcsok, módosított/létrehozott fájlok nem utalnak vírusra, nem látszott gyanús, vagy határozottan káros aktivitás.

Volt benne egy weboldalhoz való csatlakozás, ez a zugo.com valamiféle parameterezhető kezdőoldal szolgáltatás lehet, közelebből sajnos nem ismerem, de például az Fsecure Browsing protection itt tisztának jelöli:
browsingprotection.f-secure.com/swp/result?x=ZYZDCr5xcl-1LCkE1O8GOL3jqK1yBfXeZj6j0asFHUg

Itt van még egy halom online vizsgálati eredmény is, ezek sem mutattak kártevőt az exe-ben:

camas.comodo.com/cgi-bin/submit?file=5069715cdb642761aef2e117d15d7e38fc40981ab5da7cc374a6513b79e2569a
www.virustotal.com/file-scan/report.html?id=5069715cdb642761aef2e117d15d7e38fc40981ab5da7cc374a6513b79e2569a-1295816268
anubis.iseclab.org/?action=result&task_id=181677a098ea103d461b0e680a261eecf
virusscan.jotti.org/en/scanresult/99ac00e6ada965d0cbbbe78cd7a886fe1d7ac272
virscan.org/report/82ba7fc4f421f13680c990fc63a3d261.html

sorsolo 2011.01.28. 20:20:23

köszönöm, hogy utánanéztél. ezek szerint valahonnan máshonnan kaptam a fertőzést. ez volt a gyanús, mert a firefox pluginek a legritkább esetben exe formátumúak. egyébként még mindig kicsit gyanús a skipscreen, mert ma már meg sem jelenik nálam a skipscreen.com oldal. azt írja:

"

Bejelentett támadó weboldal!

A(z) skipscreen.com címen működő weboldalról bejelentés érkezett, hogy támadó weboldal, ezért a biztonsági beállítások alapján a böngésző a hozzáférést nem engedélyezi.

A támadó weboldalak megpróbálnak olyan programokat telepíteni, amelyek személyes adatokat lopnak el, a számítógépet mások megtámadására használják, vagy károsítják a rendszert

Egyes támadó weboldalak szándékosan terjesztenek ártó szoftvereket, de sok olyan van, amelyet a tulajdonosa tudta vagy engedélye nélkül használnak ilyen célra.

"

szóval nem tudom, hogy mi az igazság. az biztos, hogy a friss 4.2-es eset átengedte neki az irányítást. ez az, ami az eddigi (hamisnak bizonyult) biztonságérzetemet egy kicsit megcincálta...

Assange a social engineering új szupersztárja

2011.01.21. 13:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [abuse](#) [malware](#) [julian](#) [rogue](#) [wikileaks](#) [assange](#)

Szinte **nem is értjük, miért nem hamarabb csaptak le rá a kártevőterjesztők.** A [hamis RIAA szerzői jogi email](#) után a jövőben már azon sem fogunk majd csodálkozni, ha Wikileakses tartalmak olvasása ürügyén kapunk hamis jogi fenyegetést, és persze mellé **egy okosba elintézhető egyszerűsített bírságot.**



A Technet számolt be arról, hogy [telefon hívogatnak fel véletlenszerűen embereket \(angol nyelvterületen\)](#) és azt közli velünk a gépi hívás, **hogy a Wikileaks oldalak olvasása miatt 25 ezer USD, vagy börtön várhat ránk.** Ám minő meglepetés, **van módja a büntetés elkerülésének,** az pedig egy megadott ismeretlen telefonszám felhívása, és ott [egy jelentősen alacsonyabb összeg átutalása](#) nyújtja a [bűnbocsánati búcsúcédulát](#) - amit persze el is hiszünk nekik, hiszen olyan kedvesen mondják.



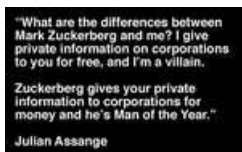
Természetesen **a számítógépek sem maradhatnak ki mindebből.** [Amíg van, aki mindenre kattint, ami mozog,](#) addig meg lesz a csalásokból, kártevőterjesztésből élő bűnözők betevője, nem fáradnak hiába.



Az F-Secure blogja írta meg először, hogy **Assange nevével visszaélve böngészés közben egy olyan trójai kártevő terjed,** amely a Jegyzettömb (Notepad) alkalmazás orosz változatát tölti le a megfertőzött gépekre, majd **azt megnyitva egy állítólagos Julian üzenetet jelenít meg a képernyőn.** Bizonyos, hogy nem ez az utolsó ilyen próbálkozás, és érdemes lesz továbbra is óvatosabban kattintgatni a kéretlen tartalmakra.



Az nyilván **sokaknak lehetett felemás élmény, hogy hiába szavaznak a népek jóval többen az Év Embere versenyben Assange-ra, azt mégis Zuckerberg nyerte** meg. Ennek persze több és mélyebb oka is van, amikbe most nem megyünk bele, helyette zárásként inkább Juian erre való frappáns reagálását mutatjuk be.



Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás

+1 0

Tweet

Ajánlott bejegyzések:



- [A PRISM szeme mindent lát](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2601871>

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.

Realitás lehet az Androidos botnet

2011.01.24. 16:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [malware támadás](#) [trójai](#) [android](#) [botnet](#) [rootkit](#)

Egy biztonsági kutató hamarosan egy hacker konferencián fog beszámolni ezirányú sikeres kísérletéről, melyben bemutat egy saját fejlesztésű rootkitet.



Ha valamennyi pénzt kellene betolnunk egy fogadóirodában a közeljövő legsikeresebb mobiltelefon platformját megjósolandó, valószínűleg sokaknál az Android lenne ez a bizonyos nagy jövő előtt álló OS. Ha ehhez hozzávesszük azt a klasszikus véleményt, miszerint [kártévők mindig arra a platformra jelennek meg, amelyik egyfelől tömegesen elterjedt](#), és piaci részesedése meghaladja a legalább 35%-ot, másrészt dokumentációja is széles körben hozzáférhető.



A [következő heti Shmocon konferencián](#) többet fogunk tudni, érdemes lesz [figyelni Georgia Weidman előadását](#), bemutatójában megfertőz majd több fajta Androidos készüléket, távolról vezérelve pedig spam küldésre, DoS támadásra fogja azokat észrevétlenül kihasználni.



[Voltak már korábban is eredményes próbálkozások az előző esztendőben](#), alkalmazások suttymóban [elsusogták a fejlesztőknek](#) a fizikai koordinátáinkat, [orosz bűnözők emeldíjas SMS hívogatással keserítették](#) meg a felhasználók életét, míg nem is olyan régen pedig az derült ki, hogy [Kínában kiterjedt kémkedés folyt](#) az Androidos telefont használók személyes adatai után. **Aki Android rendszerrel akar kísérletezni, játszodozni, de nincs ilyen telefonja, kényelmesen megteheti ezt a Google oldaláról ingyenesen [letölthető Android Emulátorral](#).**



Visszatérve a kártévőkre, a végeredmény valószínűleg az lesz majd, hogy **az antivirus gyártók szép lassan mind megjelennek ezen a platformon is**, amin egy idő és sok nyilvánosságra hozott incidens után senki sem fogja azt gondolni, felesleges biztonsági programot futtatni. Vagy más szavakkal: **széleskörű elterjedtsége okán az Android lehet az okostelefonok Windowsa**, amit minden kártévőterjesztőnek érdemes lesz (anyagilag megéri) majd támadnia.



5 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Tízből öt kártévő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)
- [25-ször több a mobilos kártévő](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2609419

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.

SMS spam a Nokiától

2011.01.26. 15:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [nokia](#) [sms](#) [csalás](#) [nyeremény](#)

Megszokhattuk már, hogy [minden jó késve ér ide;-\)](#) Ám über jó hír, hogy a [2009-es e-mail lottóhoz hasonló](#) "Az ön mobiltelefonszáma nyert" típusú bullshit végre itthon is kapható, forintért, csak most, csak nekünk.



Aki korábban azt gondolta, [magyar telefonba csak magyar SMS spamet](#), az most rádöbbenhet, az igazság odaát van. Lassan már burkolt reklámmal fogják vádolni, aki egy konkrét cégnevet túlságosan gyakran emleget. A [sok Nokia dobozos történet](#) után most **a cég állítólagos 40 éves évfordulójára szervezett nyereményjátékon nyertünk 600 ezer fontot**, azaz 190 millió forintot, amely a mostani nehézkesen fungáló gazdasági helyzetben persze nem hangzana éppen rosszul, ha igaz lenne.



De sajnos a [353 87 kezdetű szám tulajdonosáról, illetve annak varangyosbékaszerrű rinocéroszba oltott felmenőiről](#) már sok epés bejegyzést találni az interneten, és persze **az is egy jó kérdés, a Nokia cég nevével visszaélő szöveges üzenet hogyan landolhatott a mi magyarországi nem publikus számunkon.**



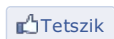
Vagy a jó öreg véletlenszám generátor a felelős, vagy pedig valamelyik **weboldal, webáruház kezelte lazán, vagy éppen adta el pénzért a regisztráltak részletes személyes adatait.**



Az már csak hab a tortán, hogy **a Nokia nem is 40 éves**, hanem [eredetileg \(na tudja valaki egy hangszóróért?\) 1865-ben alapították](#). Egy apró kicsi logikai érdekességgel lett még színesebb a mai poszt, ahol is **az eredeti Nokias hírben, amely 2009. március 6-án íródott, a cikktesten belül egy link már egy 2010. február 22-i hírre mutat**. Na ezt csinálja utánunk a nyomtatott sajtó, még időgéppel sincsenek sehol ;-)



A SMS spamek küldőinek (itt most a cenzúrázott, 18-as karika nélküli változat következik ;-)) többek közt szívesen a homlokákhöz szorítanánk valamilyen [messzi távolba elrepítő buszjegyet](#), a piros golyóstollról most egyelőre nem beszélünk.



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)

- [Safe mód a Mechagodzilla ellen](#)
- [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/2614687>

Kommentek:

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

Nincsenek hozzászólások.

De igen, többször is, és ugyanabba a folyóba

2011.01.28. 12:50 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [spam](#) [social](#) [facebook](#) [jelszó](#) [csalás](#) [engineering](#) [kryptik](#) [koobface](#)

Igen, lehet :-). A számítógépes megtévesztések, csalások, vírusok, kártevők evolúciójának egyik jellegzetessége, hogy miközben [számuk elképesztő mértékben gyarapszik](#) és mindig egyre új változatok bukkannak fel, **a korábbiak ezzel együtt sosem tűnnek el teljesen, hiszen a régieknek is marad mindig valamennyi esélye.**



Ha pedig nem vírusirtóval felismerhető kódról, hanem újra felbukkannó [social engineering trükkéről van szó](#), akkor **sokszor ez a matematikai esély nem is annyira kicsi.** Írtunk már korábban [sokféle csalásról, próbálkozásról, banki adathalász levelekről](#), sőt a mostani módszer elődje is terítéken volt már, de **a célcsoport gyaníthatóan akkor sem azon gondolkodott el igazán, vajon érkezh-e az új jelszó egy kéretlen levél EXE mellékleteként.**



A mostani "vadonatúj" kampánylevélben [arról tájékoztat bennünket látszólag a Facebook csapata, hogy accountunkat feltörték.](#) Ezért hát éppen itt az ideje megváltoztatnunk a jelszavunkat valamilyen bonyolultabbra - az persze igaz, ha nagyon fapados az a password, akkor könnyen kitalálható, mint azt láthattuk olyan jelentős és híres politikusok esetében is, mint [Sarah Palin](#), vagy [Szerencsés István](#) - ám az már kevésbé szokványos, hogy **a levél mellékleteként küldjék el az újat egy ZIP-ben.** Jön az 5 százalék, kattint és ezzel valóban igazzá válik a levél: most már tényleg feltörték, [mi magunk indítottuk el a kártevőt, nyomtunk önként és dalolva entert.](#)



Egyik előző életemben együtt laktunk a megboldogult idős drága nagymamával, akinek az volt a szokása, hogy boldog-boldogtalan ismeretlen embereket beengedett (nyilván szeretett beszélgetni). Ezért aztán egy sokadik ilyen alkalom után megbeszéltük ezt, és megígérttem vele, a továbbiakban amíg mi dolgozunk és nem vagyunk otthon, addig nem enged be senkit, bárki csöngessen is. Egyetlen nap telik csak el, hazamenve megint ott ül egy vadidegen valaki, aki mikor meglátott, jó érzékkel nyomban el is köszönt, és sietve távozott. Kértem tőle, [mondta-e vagy nem mondta én teneked](#), hogy ne engedj be senkit, bárki csöngessen? Mire azt válaszolta "Így is volt, de ő kopogott fiam".



Szóval érdemi és jelentős változást a megtévesztés fronton egyesegyedül az hozhat, ha **a gondolkodásunk módja mechanikus helyett alapvetően óvatosabb, gyanakvóbb lesz, ellenkező esetben az emberiség megérett a végső pusztulásra, és már nincs semmilyen további reménye.**



16 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Dropbox csalival terjedtek a kémprogramok](#)



A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2619821>

Kommentek:

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

[eltorzult valóságérzékelés 2011.01.28. 20:25:54](#)

[@almokvaloravalnak](#): pöcs szpemmer



[Skj Joe 2011.01.28. 20:39:50](#)

a vírus az egyik legrégebbi élőlény,
persze ettől még nem kell szeretni :)
én se szeretem

[biga156 2011.01.28. 20:54:07](#)

Én szeretem őket. Az elmúlt tíz évben nagyrészt abból éltem, hogy a júzerek gépéről pucoltam őket. Külön öröm volt, mikor valami újjal találkoztam, ami akár egy-két, vagy akár három teljes napi melót is jelentett nekem :) Felüdtő volt az egyébként mindennapos szimpla "tömegvírusok" írtása közben :)

Szóval én szeretem őket, elszórakoztatnak és mellé pénzt is hoznak a házhoz :) De az én gépeimen "valamiért" soha nincsenek vírusok ;P



[Nomante 2.0 2011.01.28. 21:18:08](#)

Bezzeg régen mikor One_half és társai szennyezték a rendszereket, azok még kérdezni sem kérdezgettek:)

Egyébként egy jó vírusírtó az ilyen "ingyensörörökélet.exe"-nél már sikongat, szóval egy józan paraszti ésszel megáldott user, nem tölti le. A többi meg akkor is letölténe, ha világító zöld betűkkel írná ki hogy "vírus vagyok, töltsél le engem és kapsz egy mazsi-drazsit mellém"

Sőt van még ennél is rosszabb fajta...

Erre hadd legyen egy személyes tapasztalatom. Egyik barátomnak szarakodott a gépe, ha már nála jártam egyik nap megnéztem. Nos a srácnak kb 2000 óta van gépe kb. nézegetem a gépét, gyors egy helyzetjelentést a msconfig-ból h. mik indulnak együtt a windowssal... hát volt egy pár gyanús elem. Mondom neki...

- Te s a vírusírtód nem fogdossa meg ezeket a szarokat? Mit használsz.
- Én? semmit. Minek az csak lelassítja a netet!

2000 óta van gépe, online játékokkal játszik, szóval átlagos user. Én azért felraktam neki egy ingyenes vírusírtót.

szóval igen, vannak ilyenek is :)

[nyomasek_bobo • http://sopron.e-cafe.hu 2011.01.28. 22:29:52](#)

A posttal egyet értek, a nagymamás történet különösen tetszett, de azért publikálás előtt át lehetne olvasni, mert néhány "n" betűvel mintha több lenne itt-ott.

Ki fél ma? Aki kérdez: az Opera Software

2011.01.31. 19:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [opera biztonság online felmérés](#)

Igaz ezúttal nem az Astoria szálló halljából jelentkeznék, továbbá nincs benne klasszikus zenei opera sem (amelynek fő lényege, hogyha valakit leszúrnak, az utána még legalább tíz percig énekel) de ennek ellenére a dolog mégiscsak érdekes.



[A norvég cég egy tanulmányt készített](#), amelyben arra voltak kíváncsiak, hogy a számítógépfelhasználók világszerte milyen online incidensektől félnek leginkább, szerintük kitől kell legjobban féltetniük online viselkedésük részleteit, ki próbálkozik titokban ennek kikémlelésével.



[A felmérési eredmények azt mutatják, hogy az online biztonságuk miatt](#) legjobban az amerikaiak aggódnak (35%), míg Oroszországban csak 14%, sőt Kínában ez az arány mindössze 7%. És mennyire érzik biztonságosnak a jelszavukat (kutyuska56 rulez:-)? Ebben a kérdésben az amerikai megkérdezettek bizonyultak a legmagabiztosabbnak, csaknem **61 százalékuk érzi úgy, hogy "nagyon biztonságos" az általa használt password**, míg például a kínai felhasználók csupán 25%-a gondolja, hogy megfelelően erős jelszava elegendő védelmet nyújt számára - tudnak valamit :-). Az **amerikai felhasználók többsége jobbára a saját kormányától félti bönészési adatait**, míg például a japánok inkább a webáruházakkal szemben bizalmatlanok - lehet, hogy tapasztalat?



A felmérés még **olyan apró érdekességeket is** felszínre hozott, hogy az amerikai felhasználókra nagyon jellemző, hogy kényszerűen ügyelve rendszeresen törlik böngészési előzményeiket, míg az **oroszok szeretnek egyszerre többféle (nyilván nem valósidejű) antivírus és biztonsági programot** használni. Bár őket [sok esetben a cirill betűs billentyűzet kiosztás is megvédi](#) ;-). Az is érdekes, hogy a megkérdezettek nagyjából **egyforma mértékben tartanak egy közlekedési balesettől és hogy egy internetes csalás áldozatává válnak**, sőt az összes kockázat közül ez kapta a legtöbb szavazatot: 25-27 százalékban.



Ha pedig már kutatásnál, felmérésnél tartunk, [egy érdekes bejegyzést lehet olvasni](#) Mikko Hypponen oldalán, aki azt tervezi, hogy a **PC vírusok 25. születésnapján felkeresi azt a Pakisztánban élő testvérpárt, akik annak idején elindították a Brain vírust a floppy lemezeiken**, és interjút tervez velük készíteni. A weboldalon már folyik a brainstorming, **lehet tehát ötletelni, kérdéseket javasolni ehhez a tervezett beszélgetéshez**.



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivírusok - villám őrjárat 8.](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2628075>

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.

Talált password-ök osztálya

2011.02.02. 19:35 | [Csizmazia István \[Rambol\]](#) | [24 komment](#)

Címkék: [jelszó password pillanat megfelelő csere botnet waledac](#)

Van aki pénztárcát talál, más kutyát vagy macskát, ezúttal azonban biztonsági kutatók félmillió elkóborolt email accountot leltek a Waledac botnet cache területén. Az eset kapcsán nem árt megjegyezni, hogy biztonságunk érdekében a naprakész Windows frissítés és a pöccre induló antivírus program használata **mellett a megfelelő jelszókezelésre is érdemes alapos gondot fordítani.**



Aki korábban is követte az eseményeket, emlékezhet rá, hogy [az ESET kutatói már 2009-ben eljátszottak a botnetes Waledac kártevővel](#), és a forgalom elemzésével méregették többek közt a botnet spamkibocsátási képességeit. Sebastian Bortnik egy blogbejegyzésében a Waledac kártevővel üzemelő botnet méretét **akkor még 20 ezer gépre becsülte, teljesítőképességét pedig napi 3 milliárd kiküldhető spamre tette.** Az alapos technikai elemzés emellett azt is kimutatta, hogy **a Waledac valójában a Storm utódjának tekinthető, és fejlesztésénél figyelembe vették az előd kijavítandó hibáit is**, például amíg a Storm csak 64 bites RSA-kódolási algoritmust használt, addig a Waledac már ebben is előrelépett, és egyéb tekintetben is folyamatosan továbbfejlődött.



Később, 2010 májusában aztán [a Microsoftnak nagy gyomrost sikerült bevinnie](#): jogi lépésekkel elérte, hogy a Waledac botnetet irányító szerverek doménneveit, illetve ip-címeit az internetszolgáltatók átadják nekik. Ezzel a komoly fegyverténnyel pedig **egyenes út nyílt a zömmel Kínában, hamis személyi adatokkal regisztrált domainek letiltására.** Bár a Waledac nem a legnagyobb botnet, az akkori méretét így is 50 ezer zombigépre becsülték.



Mai hírünk apropója pedig az, hogy [számítógépes kutatók a Waledac forgalmi adatainak elemzése közben rábukkantak százezer ellopott FTP, és mintegy ötszázezer email név-jelszó párosra.](#) **A bűnözők ezeket remekül tudják használni**, az FTP jelszavakkal weboldalakra keresztül lehet kártevőket terjeszteni, exploitokat becsempészni, de a blackhat SEO módszereket is könnyen be tudják így vetni, [mérgezve ezzel a keresési találatokat](#); míg az email accountokat főleg a spamterjesztés terén tudják jól hasznosítani.



A hírt olvasva felvetődhet - és reméljük fel is vetődik sokakban - hogy **ez egy égi jel, és talán ez a megfelelő pillanat egy önként és örömmel végzett jelszócsere**re, aki esetleg eddig ezt nem tette volna meg.



Ami lehetőleg **NE legyen könnyen kitalálható, ne legyen egy bites, és legyen egyedi: magyarul ne ugyanazt használjuk különböző belépési helyeken.** És az se baj, ha negyedévente-félévente ohne zsinég, **érzékeltető biztonsági incidens nélkül is reflexből rendszeres időközönként cseréljük.** Ne könnyítsük meg lustaságunkkal senki dolgát, [küzdjenek csak meg](#) a postaládánkban található atomtitkokért ;-)



4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2633770>

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](#).

[amodent 2011.02.02. 22:08:04](#)

Munkahelyemen a domain policy havonkénti jelszóváltozást ír elő, ami miatt mindenki nagyon gyenge jelszavakat használ, kitalálható változásokkal (pl. 123jan, 123feb, stb.). Mindig mondom a rendszergazdának, hogy legyen inkább ez fél, esetleg egy év követeljük meg az erős jelszavak használatát, mert szerintem a gyenge jelszavakat kevesebb mint egy hónap alatt lehet törni, az igazán erőseket viszont egy év alatt sem. Tapasztalataik szerint mi a vállalható kompromisszum csereintervallum/erősség vonatkozásban?

[Droli • http://nivo.blog.hu 2011.02.02. 22:21:20](#)

[@amodent](#): ugyanez volt az én régi munkahelyemnél, ott annyi változtatással, hogy a rendszer minden hónap végén követelt egy új, régivel nem egyező jelszót, azt az illető beállította, majd pár óra múlva ment a rendszergazdához, hogy vissza tudná-e állítani a régit, mert az újat elfelejtette :-)))

[delvideki 2011.02.02. 22:30:26](#)

Szerintem meg nem jelszó kell, hanem jelmondat :)

Nem kell bele speckó karakter - a hossza kárpótol ezért -, viszont könnyű megjegyezni. Persze ne közmondást vélasszunk, nehogy dictionary alapon törjék :)

[randomgenerator 2011.02.02. 23:15:18](#)

Én még a userneveim sem tudom megjegyezni. Ami webes cucc mind a firefoxomban van. Szép tanácsok, de betarthatatlan. Inkább lenne smartcard a személyi, és akkor használnánk azt mindenhol...

[randomgenerator 2011.02.02. 23:17:34](#)

Bocs a dupláért, épp megszámláltam, jelenleg 72 jelszót tárol a firefoxom.

[forgodssake 2011.02.02. 23:31:12](#)

en is a mondoka alapon torteno jelszo/jelmondat hive vagyok, de nem hiszem el h van elo ember a rainmen en kivul aki képes lenne az en esetemben:

6 email

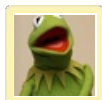
2 blog

paypal, szamla, ugyfelbelepo rendszer

es a szamtalan forum(kapasbol 20 kedvenc van a jobboldalon mentesben

jelszot megjegyezni.

ez így elsore is (ha a posztolo javaslatat megfogadnam es nincs 2 egyforma jelszo) 31 db jelszo fejbentartasa es harmohavonta csereje lenne ami nekem megugorhatatlan feladat.



[viktor134 2011.02.02. 23:47:17](#)

@Droli:

a haiv változtatás általában a következő jelszó előtagokat jelentette nálunk az usereknél:

januar

februar

marcius

aprilis....

ennyi. :)

[S.E.A.T. 2011.02.02. 23:54:08](#)

Szerintem a legjobb egy saját "algorithmus" használata.Nehezen feltörhető jelszavakat eredményez, de bárhol és bármikor vissza tudod fejteni magadnak.

pl.: felhasználónév első 3 karaktere visszafelé, a középső karakter nagybetű + születési év utolsó 3 karakterének értéke + az adott oldal címenek 3., 5. betűje + a hozzátartozó e-mailcím szolgáltatójának első 2 karaktere

felhasználó: Béla

Szül.: 1976

Oldal: antivirus.blog.hu

E-mail: bela@email.hu

Jelszó: lEb22tvem

Amikor változtatni kell, akkor meg átirod a kis logaritmust és ennyi.

[S.E.A.T. 2011.02.03. 00:08:32](#)

@S.E.A.T.: illetve be lehet tolni még egy karaktert a változtatások miatt.

Vagyis a normál: lEb22tvem

a következő hónapban: lEb22tvemX

a következő hónapban: lEb22tvem

a következő hónapban: lEb22tvemX

Tetszés szerint lehet fejleszteni, hozzáadni, levenni adatokat, de így akár évek múlva is emlékezhetsz a jelszavadra.

[rexlibris • http://rexlibris.blog.hu 2011.02.03. 05:21:20](#)

mindenhová más jelszó,

időnként változtatni,

a felem káptalan,

dédapám meg turmixgép és vasaló egyben.

[Bikfenc 2011.02.03. 07:51:37](#)

Nem számoltam össze de vagy 86 jelszavam biztos van (10-12 e-mail, 6 honlap, ftp, bank, hírlevelek, stb.)

Kinek mi a tapasztalata a jelszókezelő programokkal?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.02.03. 08:17:25**

A kommentek fényében árnyalnám egy kicsit a képet. Nyilván esete válogatja, melyiknél hogyan érdemes eljárni.

Értelemszerűen mindenhol nem éri meg ez a plusz fáradság. Mondjuk az Egyesült Cziczamicza Művek Babapiskóta és Pálkás Czumi webshopjában elegendő lehet évente, vagy akár sosem jelszót cserélni. Ha viszont a keresztnévünk James, és a vezetéknevünk ráadásul Bond, vagy esetleg a munkánk révén mások (pl. konkurencia) számára értékes információk forognak a levelesládában, (lásd mellékelt linket a Propelleres ember incidensénél), akkor szinte szükséges rossz ez. Ha valaki alulbecsüli az erős jelszót, akkor jön a Sarah Palin effektus.

Értékén kell kezelni ezt a dolgot, arányosan a védendő információ értékével. Például ha már bankkártya adat is van egy regisztrációnál a hozzátartozó háromjegyű biztonsági kóddal, ott már biztosan érdemes a negyedéves serénykedés. Ha már ott lapul a net egyik sötét bugyrában az accountunk egy elloptott és eladott csomagban, mire a rosszember eladja a vevőnek, legalább van egy kis minális esély, hogy esetleg felkoppanjon az orcája a változtatás miatt.

Akinek pedig nem szabadon választott, hanem a munkahely által előírt a rendszeres svéd torna a jelszavakkal, ott gyaníthatóan megemelkedik a Postit rendelési kvóta, vagy a kommentekben említett január, február, etc jön a képbe.

Mighty 2011.02.03. 09:21:06

Nálunk bár szintén havi rendszerességgel kell jelszót változtatni, viszont rendkívül szigorú szabályok vannak: az utolsó 24 jelszóval nem egyezhet, kell benne lennie kis/nagy betűnek, számnak illetve speciális karakternek. A hossza sem lehet ha jól emlékszem 10-nél rövidebb.

TIN modell (törölt) 2011.02.03. 10:12:00

Kizárólag a szerver root, SQL root passokra ügyelek, ezeknél a username is vmi komplex dolog rövidítése (és a kispadlás molyette hátsó sarkában a 200 éves subák alatt is el van rakva, miután egyszer egy hetes kirándulás után gondokat okozott a root jelszó felidézése, s akkor kissé le voltam izzadva ...: D). A többinél 50-80 pass között, pedig már nem fórumozok, az FF ment, mert még úgy is halál van.

Többen írják a fórumot, de az égre, egy fórumjelszón, mondjuk egy indexes fórumra gondolva, Wágner pribékjeivel, ahol a sok elmebeteg moderátor kénye-kedve szerint félnaponta kirootolja a semmibe a fél userkört, oda minek raktok bonyi jelszót?

Szeretnék avatart a hozzászólásaim mellé! 2011.02.03. 11:08:53

[@Bikfenc](#): Password Safe nevű toolt ajánlom. Enterprise környezetben is megállja a helyét. Néhány feature:

- autotype funkció: a legtöbb rendszerbe/weboldalra be tudsz lépni úgy, hogy nincs se copy/paste, se bonyolult jelszó begépelés (te magad sem látod a jelszót)
- tud szólni, ha lejár a jelszó (céges környezetben le szokott járni)
- titkosított adattárolás. Mondjuk ha a mesterjelszavadat elfelejtetd, akkor vége a dálnak
- tud neked jelszót generálni, az ehhez tartozó szabályokat te adhatod meg
- a jelszavakat csoportokba lehet szervezni (pl. Blogok, munkahely, otthon, stb.)
- gyors, kisméretű tool

Hátránya: ha több gépről dolgozol, akkor mindkettőről el kell érned az adatbázisodat. Én egyelőre paranoiás vagyok ahhoz, hogy az adatbázisomat időnként feltegyem a netre.

Jelenleg majd 200 jelszót tárolok benne s még soha semmi gondom nem volt a használatával.

Elérhető itt: pwsafe.org

Szeretnék avatart a hozzászólásaim mellé! 2011.02.03. 11:29:18

[@Mighty](#): Mondjuk ez a normális.

Nálunk még a minimum password age is be van állítva, azaz egy napon csak egyszer változtathatsz: ezzel elkerülhető a jelszó körberotálása, majd így visszaállítása az eredetire pár perc alatt.

@S.E.A.T.: az algoritmusos módszer sem rossz, de ha megváltoztatod az algoritmust, akkor már azt is fejben kell tartanod, hogy hol milyen algoritmust használsz.

Nekem a Password Safe módszer jött be: sok jelszavamat sohasem láttam, mégis mindenhol különböző és cserélem is őket...

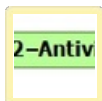
Mighty 2011.02.03. 12:11:48

@Szeretnék avatart a hozzászólásaim mellé!: Ha elég erős mester jelszót választasz, akkor mitől félsz? Én a keepass-os adatbázisomat a dropbox-szal szinkronizálom a gépeim között. Keepass-ban pl lehet használni a mester jelszó mellett egy keyfile-t is, amit rádobsz egy pendrive-ra (megfelelő számú backup mellett persze).

Comandante en Jefe • <http://local.blog.hu/> 2011.02.03. 12:32:34

@Mighty:

Ilyenkor garantált, hogy az alkalmazott felírja egy postitre, és a monitor szélére ragasztja a jelszót. (Esetleg a fiókba vagy az asztal lapjára alulról...)



www.nod32-antivirus.hu • <http://www.nod32-antivirus.hu> 2011.02.03. 13:01:42

a nod32 vírusirtóknál nincs jobb a világon



www.panda-online.hu 2011.02.03. 13:02:38

panda security szoftvert mindenkinek és akkor nem lesz senkinek se gondja !

Sieg 2011.02.03. 13:33:05

Mielőtt tényleg azt hinnénk, hogy az "erős jelszó" majd hűdebiztonságos lesz, nem árt tudni, hogy a jelszavakat túlnyomó többségében keyloggerek lopják. Ezeknek meg tökmindegy, hogy 123456 a jelszavad, 20 karakteres random generált vagy egy kisregény.

Nem a bonyolult jelszótól lesz a rendszered biztonságos, hanem attól, hogy nem hagyod, hogy megfertőződjön.

Szeretnék avatart a hozzászólásaim mellé! 2011.02.03. 22:38:06

@Sieg: a keyloggernek tényleg mindegy, mi a jelszavad, de minden más esetben jó, ha erős.

Na igen, a védelem. Eleinte baromságnak tartottam, hogy a cégem minden munkaállomásra is personal firewallt tetetett fel (nem választható módon természetesen), de manapság már teljesen elfogadom, hogy ez a természetes. A naprakész, rendszeresen scannelő vírusirtó mellett persze.

Szeretnék avatart a hozzászólásaim mellé! 2011.02.03. 22:39:51

@Comandante en Jefe: Kivéve, ha az asztalodat is rendszeresen ellenőrzik és jó alaposan seggbekúrnak, ha bizalmas információt tartasz ott (pl. jelszavakat).

A megoldás: Password Safe (pwsafe.org)

Szeretnék avatart a hozzászólásaim mellé! 2011.02.03. 22:42:34

[@Mighty](#): mint írtam is: paranoiás vagyok. :)
Egyszer talán majd elmúlik...

Nyomtalanul, de most tényleg?

2011.02.04. 16:30 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [frissítés](#) [botnet](#) [védekezés](#) [zeus](#) [spyeye](#)

A [botnetekkel kapcsolatosan](#) sok a megválaszolatlan kérdés, gyaníthatóan készítők kiváló számítógépes szakemberek, és rendületlenül dolgoznak, folyamatosan fejlesztenek a háttérben. Ám a megfertőzöttek mondjuk így passzív viselkedése is érthetetlen valahol.



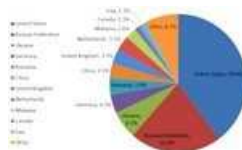
A sötét oldal profi, állandóan tesztel, fejleszt, legutóbb már arról lehetett olvasni, hogy a legtekintélyesebb Zeus botnet és a [Spyeye trójai malware kit egységesített](#) adminisztrációs felületről vezérli a szerencsétlen akaratnélküli zombigépeket a nagyvilágban. **Láttak statisztikák napvilágot arról, melyik országban mekkora az ilyen botnet fertőzte gépek aránya**, és ezekből jól láthatóan **az Egyesült Államok területén van a legtöbb ilyen**. Arról is van adat, hogy **a kétéves szolgáltatók és esetleges kiiktatásuk** is lendíthet a jelenség elleni küzdelemben, noha **a jogi lépések megtétele nyilvánvalóan nehezekebb és jóval lassabb**.



Vajon mi kellhet ahhoz, hogy ezek [a hihetetlen nagy számok egy kicsit csökkenjenek](#), ha teljesen megszűnni nem is fognak. A piaci torta legnagyobb szeletét kétségkívül a Windows uralja, és bár korábban hallhattunk [Maces zombi gépekről](#) és [Linuxos botnetekről](#), ezek egyelőre inkább ritka műszaki érdekességnek tekinthetők, kísérleti próbálkozásnak, **semmint tömeges fenyegetettségnek**. Ennek legfontosabb indoka, hogy az "Érdek a világ ura" alapján **a kártevőket is a hatékonyság és a pénzszerzés optimalizálásának jegyében írják, azt teszik, ami ezer százalékosan megéri, megtérül**.

OS	Percentage
Windows	74.00%
Mac OS X	10.00%
Linux	10.00%
Android	4.00%
Other	2.00%
Windows XP	1.00%
Windows Vista	1.00%
Windows 7	1.00%
Windows 8	1.00%
Windows 10	1.00%
Windows 11	1.00%
Windows 12	1.00%
Windows 13	1.00%
Windows 14	1.00%
Windows 15	1.00%
Windows 16	1.00%
Windows 17	1.00%
Windows 18	1.00%
Windows 19	1.00%
Windows 20	1.00%
Windows 21	1.00%
Windows 22	1.00%
Windows 23	1.00%
Windows 24	1.00%
Windows 25	1.00%
Windows 26	1.00%
Windows 27	1.00%
Windows 28	1.00%
Windows 29	1.00%
Windows 30	1.00%
Windows 31	1.00%
Windows 32	1.00%
Windows 33	1.00%
Windows 34	1.00%
Windows 35	1.00%
Windows 36	1.00%
Windows 37	1.00%
Windows 38	1.00%
Windows 39	1.00%
Windows 40	1.00%
Windows 41	1.00%
Windows 42	1.00%
Windows 43	1.00%
Windows 44	1.00%
Windows 45	1.00%
Windows 46	1.00%
Windows 47	1.00%
Windows 48	1.00%
Windows 49	1.00%
Windows 50	1.00%

Visszatérve oda, ha valakinél gyanú, világvége van a gépen és azt mentesíteni kell, akkor mi történik? Letölti az ember valamelyik vírusirtó **legfrissebb változatát, és/vagy az online detektálással csinál egy teljes vizsgálatot** (szükség esetén [lefuttatja az egyedi mentesítő](#) segédprogramokat). Vagyis ha azt vesszük, hogy természetesen nincs 100 százalékos védelem, akkor is volna legalább 9x% esély, ha mindenki használna naprakész védelmet. Amit persze trükkökkel, vagy **frissítetlenül, agyonfertőzötten a kártevők megpróbálhatnak kikapcsolni**, de legalább [a kiindulási alaphelyzet már egy viszonylagosan biztató stabil védelem volna](#).



Ehhez persze [a Windows frissítések](#) automatikus lefuttatására is rá kellene könyökölni. Ez **megadhatná mondjuk a 95%-os biztonságot, és legyen mondjuk 4% az óvatos, tudatos felhasználói viselkedés, ezzel máris tarthatnánk 99%-nál, ennél pedig gyakorlatilag nem várhatunk többet**. Ami persze árnyalható és durván lerontható, ha valaki napi 16 órában próbálja kihívásszerűen megdönteni a warezoldalak látogatásának gyakorisága, valamint a minél nagyobb számú keygen kipróbálása nevű Guinness rekordokat.



[Lehet persze mindig sültgalambként mástól várni az erőfeszítést](#), ez azonban **garantáltan nem lesz elég a saját odafigyelés nélkül**. [Nyomtalanul. De hónapokig-évekig? Valóban?](#) Vagy csak teszünk rá nagy ívben. Vajon ha valaki észrevenné, hogy idegenek ki-bejárnak a lakásában, vagy csak **ilyen esetek tömegéről hallana, ami másnál történt, vajon nem lenne ez elég ok arra, hogy ellenőrizze saját magánál is a zárat?**



Mégis ugyanígy botnet fronton a saját számítógépében miért nem teszik meg ugyanezt, mondjuk havonta: vajon nem én vagyok "LAPTOP_SMITH_AB5D3E79"? A fékeket is ellenőrizzük időnként, pedig nem is vagyunk autószerelők. **Tényleg [okosabbak vagyunk-e](#), mint egy ötödikes vagy semmivel nem vagyunk jobbak, mint a képen látható húsevő növény áldozata?**



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2637581>

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](#).

[Droli](#) • <http://nivo.blog.hu> 2011.02.08. 00:16:34

István, lehet számot kérni? :-)

Szóba hoztad itt a Linuxot - te mit javasolsz a Linux-felhasználóknak? Kell-e rá vírusirtó (mármint olyan, mely linuxos kártevőt keres, nem Windows-osat), vagy egyéb biztonsági "segédeszköz"? Annyi mindent lehet olvasni erről a neten, pro és kontra, szívesen olvasnám végre egy szakértő véleményét.

A poszthoz: Itt a "hard" megoldást kellene választani, azaz valahogy elérni, hogy minden Windowsos gépre fel legyen telepítve egy védelmi rendszer (lehet ingyenes is, lehet fizetős is), automatikus frissítésre beállítva, hogy az egyszeri felhasználónak még csak törődni se kelljen vele (aztán akinek nem tetszik, leszedi, és újat rak helyette). És pont, és nincs vita. Nem tudom, hogyan lehetne elérni, de el kellene, mert szerintem ha forintosítanánk a kártevők által okozott károkat, meglepődnénk. Olyan lenne ez, mint egy kötelező védőoltás, amit mindenki megkap. Persze ez sem szüntetné meg teljesen a jelenséget, de a 95%-os biztonsági szint legalább meglenne :-)

Önök kérték, mi teljesítjük I.

2011.02.08. 18:55 | [Csizmazia István \[Rambo\]](#) | [3 komment](#)

Címkék: [linux](#) [virus](#) [macintosh](#) [veszély](#) [globális botnet védekezés](#)

"Lehet számot kérni?" - hangzott a kérdés, ami egész pontosan azt jelentette, hogy lennének alkalmi kérdések. Hát miért is ne. Időnként lesz ilyen válaszoló rovart is, adhoc jelleggel, esetleg, ambulánsan és akkor [küldjük is a kért zeneszámot mindenkinek](#), aki szereti és remélhetőleg egyúttal híján van a megértéshez szükséges nyelvtudásszintnek ;-)



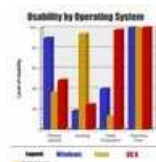
A kérdéseket eredetileg kommentként kaptuk, és mivel úgy véljük, a válasz esetleg netalántán másokat is érdekelhet, megérdelne akár egy önálló posztot is, valamint válaszolni is hosszasan volna érdemes, ezért történik hát mindez.



"Szóba hoztad itt a Linuxot - te mit javasolsz a Linux-felhasználóknak? Kell-e rá vírusirtó (mármint olyan, mely linuxos kártevőt keres, nem Windows-osat), vagy egyéb biztonsági "segédeszköz"? Annyi mindent lehet olvasni erről a neten, pro és kontra, szívesen olvasnám végre egy szakértő véleményét."



Már többször is szóba hoztuk a különböző operációs rendszerek kérdését, sőt [az egyik Vírusok Varázslatok Világa, a 11-es cikk](#) részletesebben is foglalkozott ezzel a témával. A rendszeres olvasók még emlékezhetnek arra is, hogy a [könyvének megjelenése kapcsán Magyarországra látogató Ször Péterrel is készítettünk egy interjút](#), amelyben többek közt erről, pontosabban az alternatív operációs rendszerekkel kapcsolatos véleményere voltunk kíváncsiak.



Összefoglalva - és mindenfajta OS sovinizmust, flamewart száműzve, és tartós száműzetésben tartva - a veszély és a kártevők darabszáma is mindenképpen a Windows rendszereken a legnagyobb. Léteznek ugyan kis számban kísérleti (PoC) vírusok és férgek, de ezek nem terjedtek el széleskörben. Sőt, Macintoshon és Linuxon a klasszikus vírus, ami fertőz, terjed, gyakorlatilag nem is nagyon létezik. Ennek oka a rendszer kedvezőbb felépítésében (vess össze egy Linuxot mondjuk egy klasszikus Outlook Express levelező rendszerben a Windowsra jellemző elrejtett fájlkiterjesztéssel érkező levélmelléklettel, ami például egy XP-n rendszergazdai jogokkal lefut és zúz), és a széleskörben el nem terjedtségében egyaránt gyökerezik (amíg [a bűnözői csoportok ahova néznek, Windowst látnak, és dől a pénz](#), nincs okuk, érdekük változni). Persze az sem Szentírás, hogy ezek a viszonyok, arányok kőbe vésve sosem változhatnak majd meg a jövőben, de [egyelőre ez a pálya](#).



Ám mindez nem jelenti, hogy vírusirtó - vagy pontosabban kémprogram és kártevőirtó komplett biztonságialkalmazás, rootkit detektor felesleges lenne. A rootkitek elsőként Unix rendszerekben jelentek meg, és mind OS X, mind Linux platformra léteznek kereső programok, például a [ChkRootkit](#) és az [RKHunter](#), amelyek több tucat ilyen már ismert rootkitet képesek észlelni, és ezt használati szokások függvényében hetente-havonta érdemes is lehet ellenőrizni. Hogy [milyen forgalom jár ki-be egy gépen, az még bonyolultabb dolog](#), tűzfal szabályok és naplózás nélkül gyakorlatilag ellenőrizhetetlen viszonyokról beszélünk. És végül vannak a trójai programok, amik bármikor, bárhol felbukkanhatnak, amikor a felhasználó gépi be az admin jelszót, hogy [igen, akarom és telepítem azt a kodeket](#), az ellen (hacsak már

nem egy régi darab, és detektálja valami program) nincs védelem, user ellen nincs orvosság.



Vagyis kellhet biztonsági csomag akkor, ha tudni akarjuk, hogy mi történik a gépünkben, megosztott könyvtárak és levelezéseink tartalmát bár nálunk nem csinál semmi bajt, nem akarjuk a Windowsos gépek felé fertőzötten továbbküldeni, stb. A különböző gyártók - köztük az ESET is - elkészítette a Macos és Linuxos verziót, így egy vállalatnál már le tudják fedni az összes platformot, de szerintem túlás nagy veszélyekkel, növekvő számú vírusokkal ijesztgetni. És kedvenc vesszőparipám is jöhet a végére, a felhasználók képzése, tudása, biztonság tudatos viselkedése az igazi Ultima Ratio, enélkül jó social engineering trükkökkel megspékelve minden gépet tönkre lehet tenni pár megbízhatatlan program telepítésével.



"A poszthoz: Itt a "hard" megoldást kellene választani, azaz valahogy elérni, hogy minden Windowsos gépre fel legyen telepítve egy védelmi rendszer (lehet ingyenes is, lehet fizetős is), automatikus frissítésre beállítva, hogy az egyszeri felhasználónak még csak törődni se kelljen vele (aztán akinek nem tetszik, leszedi, és újat rak helyette). És pont, és nincs vita. Nem tudom, hogyan lehetne elérni, de el kellene, mert szerintem ha forintosítanánk a kártevők által okozott károkat, meglepődnénk. Olyan lenne ez, mint egy kötelező védőoltás, amit mindenki megkap. Persze ez sem szüntetné meg teljesen a jelenséget, de a 95%-os biztonsági szint legalább meglenne"

Ha azt gondoltad, ez a könnyebb és egyszerűbb téma, hááát :) A kötelező használatnál elvileg jó lehet, ha például az internet szolgáltató a kezdésnél adott ideig "ingyen" adja a védelmet az új ügyfélnek. Ennek a rendszernek ellentmond, hogy bár egy globális világérdek valóban amellet szől, hogy mindenkit védjünk meg, jól láthatóan mindenki a saját érdekét, a saját cége profitját védi, lásd a nem legális MS Office nem kap biztonsági frissítést, stb. Persze az is igaz, adnak ingyen Security Essentialt, ami olyan, amilyen.



Voltak bizonyos kísérletek, amik Ausztráliában igen szimpatikusan a felvilágosításban, az oktatásban jeleskedtek, lásd Zombi Tudatossági Hét. Ugyanitt szorgalmazták az ISP-k körében - legjobb tudomásom szerint eleinte önkéntes jelleggel - egy olyan rendszert, ami figyelmeztetné vagy kitiltaná a fertőzött gépek tulajdonosait. Mivel itt már az ISP valamilyen szinten belenéz a forgalomba, sokaknak visszatetsző ez a módszer. Hiába lenne haszna - kevesebb zombi - ha közben mondjuk adatokat gyűjt a BSA, ASVA, stb kinek is, mert ha egyszer elindul a nézegetés, ellenőrzés, akadálya és gátja később ennek már semmi. Félő, hogy inkább a pénzt hozó szerzői jogi büntetések, semmint a vírusmentes gépeket eredményező fertőzött gépeket kiszűrő rendszer lesz (vagy már van) majd titokban a végeredménye.



Szerintem erre is a képzés, oktatás hozhatja meg az áttörést, iskolai tantárgy kellene, hogy legyen, és aki nem tanulja meg a leckét, az alul marad az evolúciós versenyben (spammelnak a nevében, kiüritik a bankszámláját, ellopják a személyazonosságát).



Ahogy ma már a nyelvtudás nem extra, hanem alapkövetelmény, az autóvezetés nem ördögi találmány, ezeknek a dolgoknak is el kell jutni egy olyan hétköznapi szintre, hogy egy ECDL vizsga már ne csak a Word megnyitásról szóljon, hanem ahogy más országokban tanítják a pénzzel való bánásmódot, a virtuális térben való biztonságos mozgásban is mindenkinek alaphoz tudnia kell majd az ökölszabályokat. Ha nem magáért tanulja meg, akkor az is lehet, hogy majd azért fogja, mert csak így kap állást, vagy a munkahelyén ezt megkövetelik tőle.



És ami a Bruce Schneier könyvben is volt a Terror fejezetben, amikor egy magáncég túl nagy jogosítványt kap bármilyen jó cél érdekében (terrorizmus ellen, botnetek ellen, csak a mi érdekünkben, és különben is) az mindig visszaéléshez vezet egy idő után. Mellette szólna viszont az, ha mindenhol lenne ilyen szűrés, védelem, jól lerövidülne a zombik életciklusa, vagy ha elkezd szokatlan viselkedést produkálni (20 helyett 20 millió levelet küld egységnyi idő alatt), akkor sikerülne hamarabb leleplezni, mentesíteni, gazdit figyelmeztetni. Ha az ISP csinálja, nem a kliens, akkor mindez persze függene a földrajzi helytől is, mert például egy vietnami, indonéz, ukrán, stb. ISP-re gyakorolt nyomás lehet akár eredménytelen, míg egy fejlettebb jogrendszerrel rendelkező országban akár maga az ISP is érdekelt vagy versenyhelyzetben lévő lehet, és azt akarná, hogy piacképes jó híre érdekében mihamarabb megszabaduljon a kétes vagy kártevőterjesztő domainektől, a kártékony forgalomtól.

 Tetszik  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](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [25-ször több a mobilos kártevő](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2646406>

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](#).

Droli • <http://nivo.blog.hu> 2011.02.08. 22:54:19

Köszönöm, nagyon hasznos és érdekes volt :-)

Droli • <http://nivo.blog.hu> 2011.02.09. 12:13:17

Ja, a "ki mire használja az operációs rendszert" ábrához: anno valaki azt írta egy fórumon, hogy ő azért használ linuxot, mert azzal nyugodt szívvel megnézheti a kártevőkkel teli pornóoldalakat is :-))))))

(Nekem is Linuxom van amúgy (Ubuntu), de nincs összefüggés :-)

[GA Web Media Group Admin](#) • <http://www.gawebmediagroup.blog.hu> 2011.02.09. 20:00:27

alternatív op. rendszer

mennyire szomozú, h 1 cég ennyire dominánsá vált h a többi már csak alternatív terméket kínálhat

tudom nem épp újkeletű gondolat de mégis.

Újra támadnak az Autorunos vírusok

2011.02.10. 12:10 | [Csizmazia István \[Rambol\]](#) | [6 komment](#)

Címkék: [magyar adatok](#) [nod32 eset](#) [havi threatsense](#) [vírusstatisztika](#)

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



Nincs jelentős érdemi elmozdulás a vezető pozíciónál, magyarul a Conficker féreg szokásos módon tartja a listán első helyét, és ezúttal vadonatúj szereplők sem bukkantak fel. Mindazonáltal **úgy tűnik, az Autorunnal kapcsolatos kártevőknek mégsem inthetünk teljesen búcsút**, hiszen alig két havi szünet után újra a toplistán köszönhetjük őket. Természetesen a Conficker féreg egyik fertőzési módszere is éppen az Autorun, de természetesen ez nem egyedi példa, hiszen a bűnözők **más kártevők esetében is előszeretettel használják ki, hogy a legtöbb felhasználó nem tiltja le** az automatikus futtatást a Windows operációs rendszerek alatt.



Az Autorun vírus terjedését megkönnyíti, hogy rendszeresen használt külső adathordozókon terjed, ez pedig lehetővé teszi, hogy a legváratlanabb helyeken bukkanjon fel. Így nem csak a megszokott USB kulcs, memóriakártya, külső merevlemez, fényképezőgép, MP3 lejátszó jöhet szóba, hanem például Ausztráliában és Németországban több nyilvános fotókidolgozó automata is megfertőződött. Így azok a felhasználók, akik az utcán vagy a bevásárló központokban USB kulcsaikról vagy memóriakártyájukról feltöltötték oda fotóikat, az előhívott papírképeken kívül rögtön egy vírussal is gazdagabbak lehetnek.



[Az Autorun vírus terjedésének csökkenéséhez kiemelt figyelemre volna szükség](#), tovább az is fontos lenne, hogy a felhasználók teljesen kikapcsolják a külső adathordozók automatikus futtatását Windows operációs rendszer alatt. Ám úgy tűnik, vagy nem törődnek ezzel a veszélyforrással, vagy pedig nem szívesen mondanak le erről a kényelmi funkcióról. Aktuális jó hír lehet, hogy [mintegy tíz évnyi szenvedés után a Microsoft végre belátta, ideje lépnie a jó ügy érdekében](#).



Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2011 januárjában a következő 10 károkozó terjedt a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 22.71%-ért.



1. Win32/Conficker féreg

Elterjedtsége a januári fertőzések között: 5.72%

Előző havi helyezés: 1.

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 eljárashívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárásen 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.



A számítógépre kerülés módja: 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>



2. INF/Autorun vírus

Elterjedtsége a januári fertőzések között: 3.31%

Előző havi helyezés: -

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozónak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.



A számítógépre kerülés módja: Fertőzött adathordozókon (akár MP3-lejátszókon) terjed.

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



3. Win32/HackMS trójai

Elterjedtsége a januári fertőzések között: 2.72%

Előző havi helyezés: 3.

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítésekor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>



4. Win32/PSW.OnLineGames trójai

Elterjedtsége a januári fertőzések között: 2.33%

Előző havi helyezés: 2.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományait és működését a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatokat titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



5. HTML/ScrInject trójai

Elterjedtsége a januári fertőzések között: 1.94%

Előző havi helyezés: 7.

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



6. Win32/Shutdowner trójai

Elterjedtsége a januári fertőzések között: 1.78%

Előző havi helyezés: 5.

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>



7. Win32/Tifaut trójai

Elterjedtsége a januári fertőzések között: 1.60%

Előző havi helyezés: 4.

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csrsc.exe és autorun.inf néven. A kártékony EXE fájl automatikus lefuttatásához külön bejegyzést is készít a rendszerleíró-adatbázisban. Működése során több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21tifaut>



8. Win32/VB féreg

Elterjedtsége a januári fertőzések között: 1.44%

Előző havi helyezés: 6.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



9. Win32/Mebrook trójai

Elterjedtsége a januári fertőzések között: 0.98%

Előző havi helyezés: 8.

Működés: A Win32/Mebrook.K trójai elsődleges célja, hogy további számítógépeket fertőzzön meg. Ehhez az ideiglenes (Temp) mappában létrehoz egy <szám>.tmp nevű fájlt, valamint a rendszerleíró-adatbázisba számos bejegyzést készít, illetve módosítja azokat, ha már léteznek. Ezenkívül megkísérel a google.com webcímre is csatlakozni. Működése során tönkreteszi a merevlemez partíciós tábláját.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21mebrook>



10. Win32/RegistryBooster trójai

Elterjedtsége a januári fertőzések között: 0.89%

Előző havi helyezés: 9.

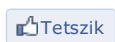
Működés: A Win32/RegistryBooster alkalmazás a hamis antivírus programokhoz hasonlóan hamis riasztásokkal igyekszik rábeszélni a felhasználókat a „program” fizetős változatának megvásárlására.



A számítógépre kerülés módja: Fertőzött weboldalról települ, vagy a felhasználó maga telepíti.

Bővebb információ:

<http://www.eset.hu/tamogatas/viruslabor/virusleirasok/registrybooster>



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



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2650222>

Kommentek:



prof. Perselus Piton 2011.02.13. 20:46:34

Nem tudom, nekem mim van, de nem éri el a gép a Windows Update oldalt, márpedig az jót nem jelent :-S És nehezen vagy egyáltalán nem lehet leállítani...kijelentkezik, de csak megy tovább "a Win. leáll" képernyővel...

A Nod és az online scan sem talál semmi említésre méltót...ilyenkor mi a teendő? Elállítottam volna valamit vagy vírus-féreg-egyéb cucc?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.02.14. 11:21:29**

Hello prof!

Ilyen jelenséget vírus nélkül is lehet produkálni, nekem például a wireless kártyám hülyül meg időnként. Vagy a rendszervisszaállítással tudtam kísérletezni, vagy újratelepíttem a driverét, és akkor általában meg bírt gyógyulni.

Ha nem volt a probléma megjelenése óta új harver/szoftver telepítve, lehet gyanakodni kártevőre is. Én azt javasolnám, csinálj egy Sysinspectoros logot .ZIP-be, és küld be a support gilisztá sicontact ponty hu címre, és abban majd többet lehet látni, hogyan, miért és egyáltalán,



prof. Perselus Piton 2011.02.14. 13:13:40

@Csizmazia István [Rambo]:

Szia Rambo!

Elvileg elküldtem, gyakorlatilag nem tudom, hogy jól csináltam-e meg...de majd kiderül...



prof. Perselus Piton 2011.02.15. 12:31:02

Folyt.:

A fájlküldés sikeres volt, de nem hozott eredményt ha jól értelmeztem, akkor nem vírus volt, csak egy ajtónyitogató, így nem látszott)...de távsegítségben egy nagyon kedves, türelmes fiatalember megoldotta a problémát: KÖSZÖNÖM, KEDVES BALÁZS :-)) (add át neki Rambo, légyszíves) és köszönöm Sicontact :-))

sorsolo 2011.02.24. 16:16:44

Kedves István!

Az ESETben a múltkor csalódtam, mert beengedett egy fertőzést. Most néztem, hogy a PCWorld tesztjén is elég szépen elhasalt. A 2011. februári angol nyelvű újságban olvastam az összehasonlítást, de itt is meg lehet nézni:

www.pcworld.com/article/214660/eset_smart_security_42.html

Azt hiszem, az utolsó, összegző mondat magáért beszél:

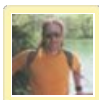
"Eset Smart Security 4 features such a rare combination of poor security and a baffling settings system that it's impossible to recommend, no matter how fast it is."

(Az Eset Smart Security 4-et a gyenge védelem és az érthetetlen beállítások miatt lehetetlen bárkinek is ajánlani - függetlenül attól, hogy mennyire gyors.)

Az újságban egyébként egy 10-es listán azt hiszem a 8. lett, tehát az is igaz, hogy még mindig van nála rosszabb vírusirtó... :(

A magam részéről már le is cseréltem. Számomra elfogadhatatlan, hogy ÖTSZÖR több kártevőt engedjen be, mint a legjobbak (pl. Norton).

Kíváncsi lennék mi a véleményed az ESET mélyrepüléséről. A 3-as ESET szerintem egy élvonalbeli termék volt, a 4-est meg úgy tűnik a szakértők is csupán a "futottak még" kategóriába sorolják.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.02.28. 11:48:59**

Szia Sorsolo!

> Az ESETben a múltkor csalódtam, mert beengedett egy fertőzést.

Hogy mennyire véd egy program, az attól is függ nagyban, milyen beállításokkal használjuk, és sok esetben ez nem egyelő a gyári, alapértelmezett beállításokkal. Azt is tudjuk, hogy 100%-os védelem nincs, de ettől függetlenül a beállításokon valóban sok múlhat, ez egy említést mindenképpen megérdemel. Ezenkívül egyetlen olyan terméket sem fogsz találni, amiről valahol valaki valamikor rosszat ne írt volna, vagy fórumokban nem mondaná, hogy ez egy hulladék, az nekem beengedett egy fertőzést, amaz nem elég jó. És mellesleg nem fogsz egyetlen olyan programot sem találni, amelyik garanciát nyújtana arra, hogy a jövőben sosem fog beengedni egyetlen fertőzést sem.

> Most néztem, hogy a PCWorld tesztjén is elég szépen elhasalt.

> A 2011. februári angol nyelvű újságban olvastam az

> összehasonlítást, de itt is meg lehet nézni:

Először is úgy vélem, vannak fontosabb tesztek és van a többi. Örülök minden egyes sikernek, de szakmailag nyilván azokat a tesztek tartom fontosabbnak, amelyeket szakemberek végeznek az AMTSO elvek mentén. Ebből a szempontból nekem többet ér a 66-ik VB100, mint ez. Magyarul: fordítva, ha a PCW díj lenne meg, de a VB100 meg nem, akkor azért kevésbé lennék boldog ;-)

Megnéztem az általad jelzett PCWorld "tesztet" és az alábbiakat gondolom erről. A címsorban érdekes módon ezt lehet olvasni: "Would you buy this Antivirus & Security Software? YES34 NO7" Az olvasók tehát nem okvetlenül osztják ezt a "népítéletet". Szóval végig olvasva a szöveget olyanok szerepelnek benne, minthogy például a Normal mód és a Haladó mód között csak és kizárólag az az egyetlen különbség, hogy feltűnik a Tools. Nos, ez nem igaz, hiszen a részletes beállítási lehetőségek is csak a haladó módban jelennek meg, az ablak jobb felső sarkában: "Felhasználói felület, Beállítások, Eszközök, Súgó". Emellett jól látszik az is, hogy a Normál mód bal oldali Beállításokat választva azt írja az alsó sor: "Hozzáértő módban minden beállítási lehetőség elérhető". Magyarul, ha egy teszt a precizitás nevű tantárgyból csupán ennyit mutat, akkor számomra nem releváns. Azért minden ilyen érdekes olvasmány, mindig figyelek rá, meg is próbálom jó Herbert Spencer tanítvány módjára megfejteni, a többiek miért azt gondolják, amit gondolnak, esetleg mit kell nekem tanulnom belőle. De harakirit azért nem követnék el miatta semmiképpen, és sosincs olyan, hogy mindenhol mindig csak jót írjanak valakiről, gondolj a molnár, a fia, és a számár mesére. Félreértés ne essék, ha csupa jót és szépet írnának, nyilván jobban örülnék, de az eredményt akkor is helyén kezelném egy szakmailag alaposan definiált, módszertanilag hiteles, például egy AV-Comparatives teszthez képest. Szerintem a fejlesztők is így tesznek: egy sikertelen VB100 után válságértekezlet van, azonnali teendők megbeszélése, egy sikertelen magazin teszt után szomorkás kávéivás után mindenki teszi tovább a dolgát.

> Azt hiszem, az utolsó, összegző mondat magáért beszél:

> "Eset Smart Security 4 features such a rare combination

> of poor security and a baffling settings system that

> it's impossible to recommend, no matter how fast it is."

Ez majdnem olyan jópofa mondat, mint a South Park sorozat bevezetőjében, hogy "megtekintését semmilyen korosztálynak nem ajánljuk".

> Kíváncsi lennék mi a véleményed az ESET mélyrepüléséről.

> A 3-as ESET szerintem egy élvonalbeli termék volt, a 4-est

> meg úgy tűnik a szakértők is csupán a "futottak még"

> kategóriába sorolják.

Az "elfogulatlan" véleményről már fentiekben beszéltem. A sebességben valóban volt visszaesés a korábbi verziókhoz képest, és a versenytársak közül többen is rákapcsoltak erre korábban általuk kritizált "gyorsaság" nevű dologra, ami egyben azt is bizonyítja, az Eset fejlesztői jó nyomon jártak. Ennek ellenére azért a Nod még így sem lett utolsó, még ha a leggyorsabb címet most nem is birtokolja, azért az élbolyban ott van. Bízom benne, hogy a következő 5.0 verzióban minden ezzel kapcsolatos tapasztalat, kritikát megszívlelnék a fejlesztők, és a program visszatér méltón régi nagy híréhez. Ha erről később lesz majd további konkrét információ, be fogok számolni róla a blogon. Remélem nem veszik el a bizalmad az ESET-ben, és minden kérdésre sikerült válaszoljak.

Valentin nap, én így szeretlek

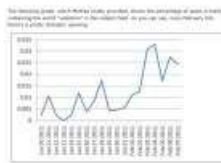
2011.02.14. 15:40 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [nap szerelem email valentin képeslap bálint féreg kártevő ecard elektronkus](#)

Az utóbbi tíz évben nem múlt el úgy a szerelmesek napjaként ismert februári dátum, hogy valamilyen kártékony kóddal ne próbálták volna megfertőzni a gépünket. Az, aki londoni fogadóirodáknak már feltette a havi fizetését arra, hogy az idén az ilyen eléggé el nem ítéhető támadások elmaradnak, nos az semmiképp nem nevezhető az emberi természet komoly ismerőjének.



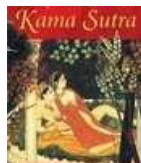
Az ünnepek közül ez egy igen [súlyos időszak, remek alkalom a kártevőterjesztőknek](#), és remek alkalom a trójai vagy kémprogramra áhító nagyközönségnek ;-). [Idén sem maradtak adósaink](#) a kártevőterjesztők.



Ezúttal egy telefonon terjedő fertőzésről kaptunk híradást. A [kéretlen MMS-ekben érkező love_mms.rar](#), amely egy telepíthető **jimm2010.JAR** nevű csomagot tartalmaz, amely szintén tartalmaz valamit: egy Trojan:Java/Jifake.A nevű trójai kártevőt. Különböző weboldalakon is megjelent már ez az állomány, nyilván ez pedig a mobilböngészés közben okozhat majd gondot.



A Sophos beszámolója pedig egy [Kamasutra témájú fertőzött Powerpoint állományra](#) hívja fel a figyelmet, amely fájl, vagy linkje szintén kéretlen emailben érkezhethet hozzánk, és **megnyitása egy hátsóját nyitó trójait ajándékoz nekünk a jeles nap alkalmából**.



Kétféle ember van: aki a többieket csoportokra osztja, és aki nem. aki megnyitja a kéretlen üzenetek mellékleteit, és aki nem. **Jó lenne** legalább az arányokon némileg javítani valahogy.



De hát [amíg ilyen édi-bédi kutyuskák, csücsörítő cuki szívecskék, ungyuri-bungyuri hörcsögöcskék érkeznek, mit lehet tenni?](#) Úgy tűnik, sokakra lehet igaz a klasszikus Oscar Wilde-i mondás, miszerint: "Mindennek ellen tudok állni, csak a kísértésnek nem". **Addig is használjunk naprakész vírusvédelmet és kéretlen üzenetek tekintetében ápoljunk szoros intenzív barátságot a Delete gombbal...**

Tetszik 8 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2660053>

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.

Angry Birds, Angry Users

2011.02.16. 14:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [market trójai](#) [android kémprogram](#) [kártékony](#)

Mindig van új a nap alatt, ha az a tét, hogy valami hívogatóan csábító külsint és alkalmat kell választaniuk a kártevő terjesztőknek. A **sok juser, sok letöltés, nagy merítés jegyében most például az Angry Birds játék Androidos újracsomagolt változata** kapott főszerepet a terveikben.



Már egy korábbi tanulmány is kimutatta, hogy a [kinai nem hivatalos mobilsoftveres piacokon](#) az esetek 11%-ában volt valamilyen rosszindulatú - legtöbbször kémprogrammal ellátott - [kóddal egybecsomagolva a letölteni kívánt szoftver](#). Nyilván szigorodniuk kell az elvárásoknak és az ellenőrzéseknek a hivatalos Market részéről, ám ilyen tényezők a nem hivatalos Marketeken nyilván nem is léteznek. Ezzel együtt úgy általában és platform függetlenül **a mobil alkalmazások fejlesztőinek is végre rá kell ébredniük arra, mit tehetnek meg és mit nem legálisan egy alkalmazáson belül** - a felhasználó személyes adatainak titokban való lekérése, az a fejlesztőknek és/vagy harmadik félnek - például hirdetőknél - való továbbítása biztosan nem megfelelő és elvárt módszer.



[Nem mindig indokolt a felhasználó GPS adatainak való lekérése](#) sem, igaz itt a **réveteg tekintettel végrehajtott és egyébiránt méltán világhírű Next-next-finish módszer is felelős** némiképp a kedvezőtlen végeredményért. A Lookout Mobile Security tanulmányára nyilván lehet azt mondani, hogy nem népitélet, a saját szekerüket tolják, és ez csak egy marketing fogás a részükről.



Ám valószínűleg [tényleg értenek hozzá, jól látják a folyamatokat](#), és ha most még esetleg nem is az általuk jelzett mértékben, de a **probléma egészen biztosan fennáll**, veszélyt jelent, és a helyzet a mobilplatformra egyre inkább rátaláló bűnözők miatt jelentősen romolhat is a jövőben. Nem hiszünk a mesékben, és nagyon valószínű egy olyan forgatókönyv is, hogy valamikor a jövőben [a kétes cégek nem csak a Firefox kiegészítők készítőit](#), hanem a mobil alkalmazások **fejlesztőit is felkeresik, megkörnyékezik majd "érdekes" ajánlataikkal**, és mindig van az a pénz, amiért valakit táncba lehet vinni.



[A jövő a mobilé](#) és ezt így látják a barikád mindkét oldalán. Tanulságnak mindebből azt vonhatjuk le, hogy **a fő trójai beszerzési forrás a bizonytalan eredetű letöltésekhez köthető**. Ám másik oldala is van a dolognak, az pedig a valódi, neves és megbízható gyártó terméke, amit azonban egyáltalán nem mindegy, hogy honnan is töltünk le.



Itt jön ki jól például az Apple Store erőssége, ami az esetek döntő többségében **jól szűri ki a megbízhatatlansági tényezőket, tiszta száraz érzést nyújt a felhasználóknak**. Ha pedig nem csak Macintosh rendszerről beszélünk, **Linux alatt a hivatalos tárolók, illetve Windows, de minden más esetben is az adott szoftvergyártó weboldala is rendre alkalmas arra, hogy onnan bátran töltsünk le**. A többi eset már mind sötét ló a biztonság szempontjából, [sosem lehessen tudni kérem szépen](#).



Mobil platformon [haszonlóan jól - persze nem 100%-osan, de majdnem :-\)](#) - szűr az [App Store](#), ám a mobil operációs rendszerek versenyének legvalószínűbb győztesének, [az Androidnak ezen a fronton még vannak teendői](#). Remélhetőleg, **mire befut a célba, addigra talán már az összes antivírus cég elkészíti az ideszánt komplett biztonsági csomagját**, és talán addigra az Android Market is összekapja majd magát. Addig is, lényeg a lényeg, [óvakodjunk a kínai Android Marketektől](#), ne igyunk mosatlan gyümölcslevet, illetve minden mobil és nem mobil letöltés, [telepítés ELŐTT jól jöhet egy kis extra odafigyelés, óvatosság, tájékozódás, etwas](#).



 3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2664667>

Kommentek:

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

Nincsenek hozzászólások.

Mary és a Lucky Number

2011.02.18. 12:30 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [a lottó](#) [csalás](#) [lelki szegények](#) [boldogok](#)

Úgynevezett "magyar" nyelven írt levelet kaptunk Marytól, aki **se nem Poppins, se nem Jane, hanem eléggé el nem ítéltető módon Wilbeirt - jelentsen ez bármit is.** És bár ő egy hangyányit még törni maccsar, meg lenni ottan bele oda neki, ám összességében felesleges pénzkidobásnak ítéltethetjük eddigi nyelvtanulási kurzusainak hatásfokát.



Úgy tűnik, **válságoktól, monetáris restriktióktól terhelt világunkban** már sosem fog **kihalni a kéretlen lottónyerés módj**. Próbálkozn **ezen szerint érdemes**, és józan ésszel valóban tök átlagosnak és **maximálisan hihetően hangzik az egymillió eurós nyeremény**, ők önzetlenül csak úgy adják, mi csak úgy kapjuk, és punctum, minek is feleslegesen kételkedni.



Jön az értesítés a szuper kompetens sorszámozott AOL-os címről, hogy "a The felhívja hivatalosan bejelentette, emellett pedig a győztes fizetik ki az A. kategóriájú winners". Az igazoló iraton aztán van itt [I] Hivatkozási szám, [ii] jegy száma, [iii] Batch szám, [iv] Sorozatszám, [v] Lucky Number.



Nem akarunk a kákán is csomót keresni, de azt meg kell állapítsuk a korrektség jegyében, hogy **a szakszerű alaposság valószínűleg némiképp csorbát szenvedhetett**, hiszen az igen jelentőségteljes és kiemelt fontosságú "[vi] A kutya oltási bizonyítványának száma" nevű kulcsadat nem is került bekérésre, ami ugye megbocsáthatatlan bűn egy A. kategóriájú Winners esetében, ez azért túlzott lazaságra, valamint magasfokú amatőrizmusra utal.



De ezen az apróságon nem érdemes csüggedni vagy fennakadni, hanem **máris szaladhatunk Mr.Frank Henrikhez "azonnal esedékes feldolgozása és utalványozása a pénzdíj"**, higgyünk hát el mindent, és siessünk nyomban megadni a nevünk, pontos címünk, valamint telefon- és bankszámlaszámunk.



Az [email lottó nyertesek](#) azért továbbra is kommenteljenek majd ide bátran, de ez csakis az egymillió euró kézhezvétele után ér!
Addig is a közelgő hétvége okán így hát marad akkor a hagyományos "Tesco gazdaságos" lottóban való reménykedés, már aki arra gerjed.
Igaz a fentiekkel ellentétben ahhoz már szelvényt is kell vásárolni.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2669855>

Kommentek:

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

Nincsenek hozzászólások.

Ingyen fejőstehén, csak most, csak nekünk

2011.02.21. 16:15 | [Csizmazia István \[Rambol\]](#) | [30 komment](#)

Címkék: [free scam](#) [facebook](#) [farmville](#) [cashcow](#)

Nagy az Isten állatkertje, és már az is egy érdekes filozófiai kérdés lehet, vajon egy ingyen kapható de egyben pénzt szaporító virtuális szarvasmarha, vagy az ezt a gáláns ajánlatot gondolkodás nélkül simán készpénznek vevő "Igen, yes, click, dunno, gimme" és adoptáló humanoid áll-e rendszertanilag magasabban a táplálkozási láncolatban.



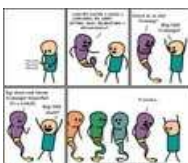
Meg sem lepődünk, hogy **újabb lehetséges csalási forma jelent meg**, már [csak húzunk egy új strigulát](#), valahogy [úgy a sokezervalahányszázadikat](#). Ezúttal az aranytojást tojó tyúk mintájára most egy **óránként 9 pénzegységet ajándékba adó csoda fejőstehén vár a kattintásunkra barátságos bőgéssel**. És annyi bizonyos, hogy ez vagy igaz, vagy nem ;-) Ne menjünk hát sehova, mert ez csak most, csak nekünk, limitált széria, hamarosan lejáró határidővel.



Emlékezzünk rá, [az adathalász csalásoknál is megszokott módszer a sürgetés](#), amellyel azt akarják elérni, hogy megijedjünk, és hibásan döntsünk. Ott például gyors adóvisszatérítési ígérettel kecsegtetnek vagy **számlánk azonnali zárolásával ijesztgetnek** minket, ha sürgősen nem kattintunk.



A helyes döntés érdekében **minden hasonló üzenetnél érdemes a küldőt, posztolót is megvizsgálni, és elgondolkodni, vajon ő vagy bárki más tényleg adna-e ilyet**, mikor egy Farmville-szerű játékban [a Market szolgál az igények kielégítésére](#), és mivel ott USD befizetéssel is juthatunk Farmville Cash-hez, akkor vajon miért adnának bárkinek bármit is ingyen? De persze hasonló esetekben [arra is figyelni kell, a valódi vagy csak egy hamis Farmville oldalra igyekezzünk-e jelszavunkat begépelve belépni](#), mert sajnos ez is egy gyakori forgatókönyv.



Úgy általánosságban is gyanakodjunk: ha valami túl szép ahhoz, hogy igaz legyen, az az esetek többségében valóban nem igaz.

Csak reménykedünk, hogy egyszer már nem csak az ilyen egyes konkrét esetek, hanem az összes eddigi csalás kapcsán egy kikristályosodott tanulság, egyfajta **univerzális tudatosság esszencia ad majd mindenkinek egy generális felvértezettséget** minden jövőbeli kísérlet ellen. Erre azonban **minden bizonnyal még várnunk kell egy keveset**.



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



0

Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- ["Szösölmédia" és nyaralás](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2676527>

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](#).

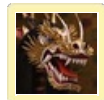


okostojgli 2011.02.22. 08:44:05

Nagy az Isten állatkertje.

Mondja ezt az, aki egyszerűen csak Antivírusnak nevezi el a blogját azt sugallva, hogy mindenki számára hasznos információkról tájékoztatja a nagyérdeműt miközben egy víruskereső programot értékesít.

Mert én, mint humanoid simán bedőlök a Víruskereső blog ajánlásának és megveszem a Nodot. És azzal, hogy megvettem igazolom, hogy tényleg nagy az isten állatkertje.



Jubari • <http://puceraj.blog.hu/> 2011.02.22. 09:48:21

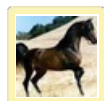
CoV-os tehén rulez! :)



Krajcs • <http://uralicowboy.blog.hu> 2011.02.22. 10:33:42

Most akkor mi volt ebből a cikkből az új infó?

Amúgy nekem anno Bill Gates simán adott a vagyonából.



ColT • <http://kilatagaleria.blog.hu/> 2011.02.22. 10:36:51

Hehh, aki bármilyen spamben található beetetésnek bedől... ..mindig csodálkozok, hogy vannak ilyen emberek, hiszen a TV és a net is tele van ilyen hírekkel, hogy több milliót fizettek valakinek...

...alapból nem fizetek semmiért, amit nem kértem, vagy nem látom, hogy mit kapok érte, és nem adják előbb a kezembe. :D



Nándusz 2011.02.22. 11:11:49

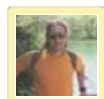
Én a mai napig várom Bill Gates beígért csekkjét. Igaz, hogy eurót írtak dollár helyett, de most hó vége felé az is jól jönne.

maxyore 2011.02.22. 11:12:20

Nincs Facebook accountom, így nem tudom megnézni, de ez a tehenes cucc nem véletlen ez a paródia:

www.bogost.com/blog/cow_clicker_1.shtml

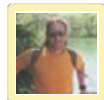
?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.02.22. 11:24:34

Szia Okostojgli!

Bár én személy szerint nem értékesítek neked víruskereső programot, a blogindító posztban világosan szerepelt, hogy hol dolgozom. Úgy vélem, ez nem csökkenti a közölt információk hasznosságát.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.02.22. 11:25:53

Csao Jubari!

Commodore Világ Évkönyv anno 1991, saját különbejáratú példány :-)



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2011.02.22. 11:31:05

Szia Krajcs!

A válogatott lényeg tulképpen az lett volna, hogy a konkrét infók helyett az óvhatna meg legjobban a csalásoktól, ha mindenki érezné az Erőt, és akár ismert esetről van szó, akár vadiújról, egy idő után meglátná benne a vörös fonalat és azt mondaná, hehe, átlátok rajta, ezt nem veszem be. És ez az a stáció, ahol egyelőre még nem tartunk, ha egyáltalán lesz ilyen (lásd egy újszülöttnék minden vicc új)



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2011.02.22. 11:32:20

@Nándusz:

Nekem 5 hetes email lottóm van, jokerrel :-)

Pzkipfw 2011.02.22. 12:45:05

CoV Evkonyv Ruez! :)

MetálFater (törölt) 2011.02.22. 13:38:05

@Csizmazia István [Rambo]:

Nem fikázni szeretném az Ön munkásságát - amely során antivírus programok vételére buzdít -, de személy szerint már évek óta megvagyok nélkülik.

Sőt! Külön bejáratú tűzfalprogramom sincs.

Ennek ellenére nincs semmilyen kártevő a rendszerben, 2009 nyara óta.

Természetesen van védelem, de - és ezt bárkinek, bármikor bizonyítom - ez megoldható a Registry, illetve a Szolgáltatások megfelelő beállításával, és 4 azaz négy program használatával.

maxyore 2011.02.22. 13:45:50

@MetálFater: 4 azaz négy program használatával...

Mármint az OpenBSD és három azon futó alkalmazás? :)

hiddenite (törölt) 2011.02.22. 13:53:53

@MetálFater: tipikus... ha nincs megfelelő vírusírtód, akkor honnan tudod hogy nincs rajta vírus? a mai vírusok már nem (csak) úgy működnek hogy kifüstölik a gépedet, és ha nem füstöl akkor nincs vírus... anélkül hogy tudnál róla, a gépedet használ(hat)ják több száz, ezer másik géppel együtt szerverek leterhelésére, információkat szerezhetnek meg hogy milyen weboldalakat milyen sűrűn látogatsz és ezeket eladják statisztika formájában, adatokat lophatnak a gépedről, jelszavakat szerezhetnek meg (pl netbankáros jelszó, számládnak annyi)

Nem mondom hogy mindenképpen telepíts vírusírtót, mert nekem aztán mindegy hogy te miben hiszel, de ne terjeszd már a fals ígét, hogy a vírusírtó fölösleges, mert nem.

egyébként ha vírusírtó, akkor csakis avast szvsz.



Benkovics Tomi 2011.02.22. 15:02:40

Én Mac-et használok, de én is megvettem a cybersecurityt. De csak azért, hogy ne továbbítsak másnak, a maradi win-es haveroknak semmit....

Persze amit István mond a legjobb módszer: "amiről nem tudod mi az, csak hagyd figyelmen kívül, Ne törődj vele". Ne kattints, ne olvasd és ne nyisd meg. Persze, hogy érdekes dolgok, és kinek nem kellene egy kis extra pénz, de meg kell értened, hogy senki sem ad neked semmit ingyen!



becketman • <http://putritours.blog.hu> 2011.02.22. 15:17:51

@MetálFater:

erről az a vicc jut eszembe, mikor kizuhan a faszi a tizedikről, és a másodikon megjegyzi: eddig minden rendben... ehhh....



cso zsi • <http://www.ingyen-jatekok.com/>
<http://www.demonoid.me/> 2011.02.22. 15:28:20

@becketman: Nálam van rajta ejtőernyő.

A tesztgépeimen nincs vírusirtó, és sok egyéb alkalmazást sem futtatok rajta. Neten járok vele, és drivereket töltök le a kezem alá kerülő gépekhez.

Időnként átvizsgálom vagy hálózaton keresztül, vagy a kiszedett vinyót a vírusirtóval, és reklámtakarítókkal felvértezett gépen. Mégsincs rajta semmi gonosztevő.

musi 2011.02.22. 15:48:34

Csak full dilettánsoknak lehet eladni vírusirtót. Pláne azért, mert a legjobb vírusirtó ingyenes: Avast. Aki egy kicsit utánanéz, az meg tudja hogyan kell törölni a vírust a géperől... Amikor legelőször csatlakoztam a netre, és full vírusos lett a gépem, na akkor jöttem rá hogyan kell ezeket törölni. Azóta tudom hogy lófászt sem érnek a vírusirtók...

MetálFater (törölt) 2011.02.22. 16:02:28

Okostojások.

Leírtam:

Fikázás helyett, BÁRKINEK? BÁRMIKOR megmutatom, hogyan lehet antivírus programok és tűzfalak nélkül olyan rendszer, amely TELJESEN mentes minden kártevőtől!

Tények:

2009 június 17-én telepítettem egy teljesen tiszta merevlemezre, egy eredeti WinfosXP op rendszert.

Azóta ISMÉTLEM, azóta nem volt, és manapság sincs semmilyen kártevő a gépen.

Ha lenne, nyilvánvalóan annak nyoma lenne (memória túlsordulás, leterhelt processzor, lassú internet, eltérített oldalak, stb.)

Természetesen időnként az Online Víruskeresők egyikével néha átnézem a gépet. SOHASEM talált egyetlen egyet sem.

Természetesen nincs a gépem védelem nélkül, de az említett 4 program egyike sem tartozik a gépet leterhelő antivírus programok közé.

Ehelyett használom a Sandboxie alkalmazást, amely segítségével a nevéből adódóan, teljesen különállóan böngészek a neten. Sőt! Torrentezem, pornót töltök le, és még warez oldalakra is lemegyek, ha szükséges.

A következő program egy monitorozó, amely segítségével minden pillanatban látom, milyen processzek futnak, hányas PID tartozik hozzá, és még további finomságok.

A Scotty WiPatrolja az egyetlen, ami (talán) tűzfalnak minősülne, bár nem az!

Viszont kiválóan jelez minden egyes registry módosítást, vagy bármilyen a kernelhez, illetve a rendszerhez tartozó program cseréjének próbálkozását.

Az utolsó program saját Microfos termék, mégpedig a Windows Steady State. Ez úgy van beállítva, hogy minden (engedély nélküli) változtatást a rendszeren hagyjon figyelmen kívül (telepítés, böngészés utáni sütik, egyebek), és állítsa vissza az alaprendszert!

És még néhány módosítást eszközöltem a Szolgáltatások között, illetve a registryben, amelyek felsorolása kissé hosszadalmas lenne itt.

Remélem világosan elmagyaráztam, miért nincs kártevő a gépen immár 1,5 éve.

Tehát mellőzzük a fikázást, és a hozzá nem értők kíméljenek.

Egyéb kérdésre privátban szívesen válaszolok.

Loading... 2011.02.22. 16:22:14

[@BenkovicsTomi](#): "a maradi win-es haveroknak" - lol, te ostoba mac fan. Megvetted, mert a buta osx is beszopja a vírusokat, csakúgy mint a maradi win.

Loading... 2011.02.22. 16:30:46

[@MetálFater](#), okostojás, registry betyár: LOL vagy fater!

Kedvencem: "Természetesen nincs a gépem védelem nélkül, de az említett 4 program egyike sem tartozik a gépet leterhelő antivírus programok közé." - MUHAHAHA

4 progit használsz, hogy ne terheld a gépedet?! LOL

Milyen vírusirtóra gondolsz itt? Melyik terheli úgy a géped, ahogy ez a 4 nem?

Lehet le kéne cserélned a pentium 1-es konfigodat a 256 mega rammal! :D

"Természetesen időnként az Online Víruskeresők egyikével néha átnézem a gépet." - Muhahaha, embeeer!

Ez a hsz felvillanyozta a napom!

Goompah 2011.02.22. 16:50:08

[@MetálFater](#): Az ugye nyilván tudod, hogy a Windows Steady State (vagy hasonló) mellett ugyanúgy beszophatsz vírust a következő rebootig? Jelszólopás stb. ellen sem véd. Persze attól még hasznos, nem tagadom.

Goompah 2011.02.22. 16:55:48

[@Loading...](#): "4 progit használsz, hogy ne terheld a gépedet?! LOL"

A WSS csak boot során fut. A Sandboxie valóban nem sok erőforrást igényel és egyébként is hasznos. Bár én a helyében a WSS helyett a Deep Freeze-t használnám, de ez magánügy.

Persze a WSS vagy Deep Freeze sem csodaeszköz. Ha egy beszopott vírus mondjuk letöröl egy rakás file-t, akkor azok nem állnak vissza, csak a rendszerfile-ok. Mint írtam, jelszólopás és hasonló ellen sem védenek. De az tény, hogy minden induláskor vírusmentes lesz a gépe. Ez is valami.



Van_mikrohullámú_sütőtök? 2011.02.22. 17:00:01

Jók a hozzászólások, köszi ! :)

Amúgy meg tökéletes védelem úgy sincsen, akkor meg minek, nem ? :)

Spam szűrő az nem antivírus.. de sok jó webmail is van, ha lusta az ember.
amúgy meg egy router amin freebsd/linux van tényleg hatékony tűzfalat képes biztosítani. Pláne ha frissített és kifelé csak biztonságos kapcsolattal kommunikál az ember (VPN, proxy, SSL..)

Trojaira, rootkitre azért tényleg elég szokott lenni a proc/reg watch.

Persze azért van az a csoport aki nem ér rá maszatolni a géppel, de a biztonság kell neki.



Van_mikrohullámú_sütőtök? 2011.02.22. 17:08:03

[@Goompah:](#)

WSS ingyenes volt amíg támogatták (tavaly óta nincs) DeepFreeze fizetős. Részemről valamilyen Virtual PC. mert lehet windowsos is akár, vagy solaris, vagy linux ugyanazon a vason.

Bármilyen fájlt törölhet, köv. restartnál ott lesz...

Jelszólopás meg csak elvileg léphet fel, feltéve, hogy a bankja biztonságos kapcsolatot használ az illetőnek meg virtuális billentyűzetet.

Persze fórumokra be lehet kártékony kódot csempészni, hogy jelszót lopjon de elég macerás, meg aztán sokra nem megy vele a hacker, nem éri meg... Akkor már trójait telepített, azt meg egy jó böngésző azért nem enged, vagy ha mégis ne a nap végén webbankoljon az ember koszos géppel...

Goompah 2011.02.22. 23:39:28

[@Van_mikrohullámú_sütőtök?:](#) "vagy ha mégis ne a nap végén webbankoljon az ember koszos géppel"

Én kb. negyedévente indítom újra a gépemet (XP SP3, szóval maradt az Avast és a router. :)



BenkovicsTomi 2011.02.23. 07:27:37

[@Loading...:](#)

Nem, mert ahol én élek ott mindegy mit veszel, bár nem mindedj mit kapsz.... Ezért váltottam mac-re, és nagyon szeretem. Hozzáteszem, hogy a véleményem nem változott... A Windows a legjobb OP rendszer, de a kapott programok silányak, vagy vagyont költhetsz jó progikra... és ne gyere nekem "torrentekkel"...



Van_mikrohullámú_sütőtök? 2011.02.23. 14:34:46

[@Goompah:](#)

Az szép uptime, a régi gépemen én is így voltam. Inkább hibernáltam, mint újraindítottam.

Aztán került a gépbe 4GB ram és a hibernálás lassabb lett, mint a restart.

A munkahelyi gépet meg GPO-val, WSUS-al és login script-el is patcheljük sűrűn, legalább 2naponta indítani kell.

Viszont a W2003 server változattal elégedett vagyok: azt minden páros hónapban indítjuk újra.

Régi Solaris 8 van sok vason Veritas clusterben, azt talán utoljára 2007-ben indítottuk újra ;-)

Goompah 2011.02.23. 19:21:59

[@Van_mikrohullámú_sütőtök?:](#)

Az enyém valóban megy éjjel-nappal, elsősorban a torrent miatt.

2007 óta... na az is szép uptime.



szikjáró 2011.07.02. 13:03:25

[@Goompah:](#) nekem a torrent miatt csak a router megy. azért bekapcsolva hagyni egy 4-500 W vagy nagyobb teljesítményű tápot....

józsibácsi meg nem győzi lapátolni az uránt pakson :)

alapesetben Linuxot használok, röhögök a vírusokon.

Iparúzés kicsit másképpen

2011.02.24. 10:50 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [anglia](#) [csalás](#) [hamis identity theft](#) [adóvisszatérítés](#) [személyiséglopás](#)

A [személyiséglopás - magyarul identity theft](#) - mára iparág lett, és bár az ellene való védekezés nem egyszerű, annyi szerepünk azért mégis van, hogy legalább nem adogatunk fel magas labdákat. Alaphangon jó, ha vigyázunk a gépünkre, és személyes adatainkra, illetve ezek széleskörű publikálásával is csinján bánunk.



A **lakcím, telefonszám mellett egy ilyen védendő adat lehet még akár a pontos születési dátum is**. Egy közösségi oldalon untig elég a semmi vagy csak egy csupasz évszám is. Akivel nem vagyunk mély barátságban, és például csak azért köszönt fel minket a születésnapunkon, mert felugrott neki egy Facebook vagy Skype értesítő ablak, az kedves gesztus ugyan, de mégis egészen más, mint amikor a családunk ünnepel velünk úgy, hogy **ezen dátum gyárilag a hippokampuszukban van, és nem egy virtuális postit-ról olvasva puskáznak**. (Egyik cimbora beírja ugyan, de paranoid android módra a születésnapja közeledtével már egy héttel előtte jól kitörli, és aztán csak az esemény elmúltával írja vissza, jól mondom? :-)))



A személyes adatok számítógépes környezetben történő [gondos kezelésének módjaiba most ne menjünk bele](#), ezeket már [ezerszer kitárgyaltuk](#). Ám van, amiről már nem is mi tehetünk, és védekezni sem igazán tudunk ellene: **ugyanis ott van az a lehetőség is, amikor a hivatal hanyag, vagy a csaló pont ott dolgozik, és legyünk mi bármilyen pedánsak, biztonságtudatosak, egy banki vagy hivatali alkalmazott sok mindenhez hozzáférhet, ellophat személyes adatokat** - nyilván persze ezt sem teheti nyakló nélkül, de azért többnyire időnként csak utólagos ellenőrzés - ha van ilyen egyáltalán - derül fény az egyes incifincidensekre.



Mostani történetünkben egy profi személyiségtolvaj pár ítélete született meg, ami nem kevesebb, mint nyolc esztendő börtönbüntetés. A 35 éves londoni biztonsági őr és női cinkosa **háromszáz feletti esetben lopott el személyes adatokat, és adott be ezek nevében éveken át hamis adóvisszérítési kérelmet**. A 42 éves nő pozíciójával visszaélve - a Jobcenter Plus nevű munkaközvetítő ügyintézőjeként **számos adathoz hozzáfért - olyan alacsony jövedelmű ügyfelek adatait lopták el, akikről úgy gondolták, az igények elbírálásakor feltűnésmentesen lehet a nevükben adóvisszatérést kérni**.



A kitöltött kérelmekben a számlaszámnak azonban ehhez természetesen már a sajátjaikat jelölték meg. A duó 2004 és 2008 között intézte ezeket a csalásokat, ám a letartóztatásukra csak 2010-ben került sor. [Az általuk okozott kár összegét a nyomozók 1.3 millió angol fontra \(nem kis összeg, durván 420 millió HUF\) becsülik](#), ám a letartóztatásuk után **beazonosított számláikon már csak mindössze 70 ezer fontot sikerült megtalálni és lefoglalni**. A nyolc és fél éves börtönbüntetéstől a hatóságok azt remélik, ennek mértéke megfelelő visszatartó erejű és elretentő hatású lesz.



Mi naiv ügyfelek, [ez ellen a változat ellen keveset tehetünk](#), de pár apróságot azért mégis igen. "A zsenialitás nem más, mint a józan paraszti ész ünneplő ruhában". Van egy csomó olyan regisztrációhoz kötött webes szolgáltatás, ahol nem tartanak pisztolyt a fejünkhöz,

nem kötelező valós adatokat beírni. Így megadhatunk bármit, ha éppen nincs meg a tökéletes bizalom: lehet a név Malyomváry Armandó, lakhelye Zomba, az emailcíme meg egy lejáró ideiglenes eldobható cím, és ráadásul ez még spammelés ellen is kiváló. Nyilván persze ez nem az ügyfélkapura, álláskeresőre vagy egy webáruházra vonatkozik, ahol ha nagy furmányosan a "Ló utca 23/B"-t írjuk be, akkor soha napján érkezik meg a rendelt árucikk.



Mindig erős egyedi jelszóval védjük a postafiókunkat, saját ügyeinket, ügyintézéseinket rendszeresen kísérjük figyelemmel, hivatalos leveleinket késelem nélkül vegyük át, és azokat olvassuk is el, legyen zárható a lakásunkhoz tartozó postaládánk, kérjünk SMS értesítést a Földhivaltól, ha ingatlanunk tulajdonviszonyaiban bármifajta változás állna be, banki egyenlegünket pedig rendszeresen ellenőrizzük, és járjunk utána minden gyanús tételnek, hiánynak - körülbelül ennyi. Meg persze titkon reménykedhetünk is, hogy pont velünk azért ilyesmi sohasem fog történni, mindig csak mással.



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- ["Szösölmédia" és nyaralás](#)
- [A jelszó érték, vigyázzunk rá](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés trackback címe:

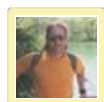
<http://antivirus.blog.hu/api/trackback/id/2686043>

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](#).

[zsigmond.judit1974](#) • <http://skypesuli.hu/hirek> **2011.02.27. 19:54:08**

ilyen vanb???



[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu> **2011.02.28. 11:47:14**

Szia Judit!

Sajna, igen, ez így működik.

Itt egy korábbi poszt, ami arról szól, hogy a briteknél már külön botnetet üzemeltetnek az adóvisszatérítéses bulira.
antivirus.blog.hu/2010/07/12/a_csaszarnak_ami_a_csaszare_1

Az Adobe Readerétől ments meg Uram minket!

2011.02.28. 16:30 | [Csizmazia István \[Rambo\]](#) | [18 komment](#)

Címkék: [social reader](#) [adobe malware pdf 2011 exploit engineering mikko rsa hyppönen](#)

Mikko Hyppönen is az RSA 2011 előadói között volt. A kártevők, kémprogramok kapcsán kiemelte, 2010-ben a veszélyes mellékletek közül leginkább a PDF dokumentumok okozták a legtöbb fertőzést.



A [február közepén az USA-ban tartott konferencián](#) az F-Secure antivírus-kutatási részlegének vezetője is előadást tartott, és arról beszélt, a mai korszak kártevőit **szinte kizárólag kémkedésre készítik fel**. A különféle trójai alkalmazások, célzott kémprogramok rengeteg egyedi, és változatlan formájában ritkán előforduló kódot jelentenek, amelyek **időben történő felismerése, blokkolása elképesztően nehéz** feladatot jelent a víruslaboratóriumok számára.



Jól megfigyelhető volt, hogy [minden híres ember, különleges vagy váratlan esemény, katasztrófa, díjátadás](#), sportesemény, politikai zavargás **remek alkalom a kártevőterjesztőknek**, akik mérgezett keresőtálalataiba, kéretlen üzeneteibe fertőzött weboldalakra mutató linkeket helyeznek el, illetve sebezhetőségeket kihasználó fájl mellékleteket csatolnak a leveleikhez. **A veszélyes dokumentum fájl típusok között az azt megelőző évhez hasonlóan 2010-ben is a PDF emelkedett ki leginkább, 61 százalékban tartalmazott valamilyen hibát kiaknázó exploitot.** És csak ezt követi aztán a többi, maradékon osztozó Office fájl típus: Excel, Word, PowerPoint, futottak még. Elmondása szerint [a létező legsilányabb szoftver az Adobe Reader](#), amit a szintén sűrűn támadott QuickTime követ a sorban.



Az ilyen incidensek után a támadók képesek hátsóajtót nyitni a sebezhető számítógépeken, és onnan adatokat tudnak ellopni, illetve a fertőzött gép **távról történő rejtett irányítása, valamint általában további támadásokban való felhasználása** a jellemző. A blogon is [beszámoltunk már a PDF támadások számának emelkedéséről](#), valamint [bátorítottuk](#) az olvasókat az [alternatív PDF megjelenítők használatára](#). A PDF olvasó **egyéb, megbízhatóbb és kevesebbet támadott thirdparty termékkel való kiváltása** a vállalatok számára is hasznos megoldás lehetne, különösen a gyakran támadott, célkeresztben álló stratégiai munkahelyeknek lenne érdemes ezt meglépni.



Persze azt Hyppönen is kiemelte, hogy **az alacsony észlelési küszöb miatt a felesleges, gyanús, kéretlen leveleket, levélmellékleteket legjobb azonnal olvasatlanul kitörölni**, esetleg indokolt esetben magától a feladótól megerősítést kérni, valóban ő küldte-e azt - persze mindezt szigorúan még a megnyitás előtt. Emellett a **felhasználók egyik lehetséges és igen hatékony védekezési módja az lehet, hogy folyamatosan pallérozzák elméjüket [az egyre újabb social engineering](#) (megtévesztésen alapuló) módszerekkel szemben.**



4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Akiknek a Captcha kinszenvedés](#)
- [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/2697362>

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](#).

Cirrus 2011.02.28. 20:00:47

Én eddig az Acrobaton kívül csak a standard Linuxos PDF readereket használtam, és elég fapadosak, hogy finoman fogalmazzak.

Cirrus 2011.02.28. 20:01:52

x



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.02.28. 20:23:46

Esetleg Evince? Az Linuxon kevésbé fapados, mint pl. Xpdf. Winre meg van Foxit, Sumatra, talán ezek a legismertebbek.

Amellett meg jól hátrakötném a sarkát és USB kulcsokra térdeltetném azt, aki kitalálta, hogy Javascript legyen egy PDF-ben :-)

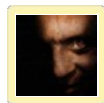
spontan • <http://erdekessegek.info> 2011.02.28. 21:37:45

Melyik Adobe alternatív a legjobb Windows-on? A Foxit-ról hallottam, hogy elég jó. Valaki próbálta már?

kafferbivalybalamber 2011.02.28. 21:45:52

[@spontan](#): Igen, elég sok gépen. Nincs rá panasz, működik.

Aki meg ilyen többszáz megás szörnyeket ír, ahhoz hogy egy nyamvadt pdf-et el lehessen olvasni, az eleve monnyon le.



Elstron 2011.02.28. 21:57:13

[@Csizmazia István \[Rambo\]](#): Nekem pl. most pont jól jött a munkámban, automatikus nyomtatást máshogy nem lehet csinálni PDF-ben.

Cirrus 2011.02.28. 22:21:14

[@Csizmazia István \[Rambo\]](#): Az Evince volt az egyik fapados. De azért a célnak megfelelt. Most nem Linuxozom.

Dr. Schwanzkopf Rudolf 2011.02.28. 22:22:05

[@spontan](#): Foxit, gyors, kényelmes, kicsi, használd bátran.

spontan • <http://erdekessegek.info> 2011.02.28. 22:24:28

[@Dr. Schwanzkopf Rudolf](#): feltettem, az adobe reader-t meg leszedtem

egyelőre jónak tűnik

énisfélek 2011.02.28. 22:51:16

Feltettem a Foxit-ot.

A tűzfalam szerint mindenáron fel akar csatlakozni valamilyen szerverre, ismeretlen célból. Emellett már a második pdf dokumentumot nem volt képes megjeleníteni (üres lap).

Van még más Adobe Reader helyettesítő?

Dr. Schwanzkopf Rudolf 2011.02.28. 23:18:57

@énisfélek: Frisíteni próbálja magát, lehet engedélyezni. PDF-megnyitás böngészőben: pipáld ki ezt: Tools-Preferences-Internet: Display PDF in browser.

Help-Check for updates now - a listáról érdemes a Firefox plugint feltenni (ha Firefoxot használsz)

énisfélek 2011.03.01. 00:57:08

@Dr. Schwanzkopf Rudolf:

Az installálás első pillanata: csatlakozási kísérlet a websearch.ask.com (66.235.120.94) szerverre. Ez tudtommal NEM a foxit szervere.

A telepítés végén egyből csatlakozni próbál a pis.foxitsoftware.com szerverre - na erről már elhiszem, hogy köze lehet a frissítéshez (habár nem kért rá engedélyt és nem is jelezte, hogy most frissíteni fog) ráadásul nem is találtam olyan opciót a beállításokban, ahol letilthatom az automatikus frissítéseket.

...egyébként jó a nicked :)

spontan • <http://erdekessegek.info> 2011.03.01. 09:41:17

A foxit-nál csak arra kell figyelni, hogy a Decline gombot válaszd installálásnál, hogy ne aktiválja az ask.com-os cuccokat.

Nem szimpatikus dolog, ha ilyet akarnak rám erőltetni, de ha az installálásnál kis odafigyeléssel elkerülhető, akkor ennyi még belefér.



bunkó • <http://bunko.blog.hu> 2011.03.02. 10:13:57

@spontan: Az ask.com-os trükközésen felül (kikapcsolásától függetlenül) a Foxit reader minden egyes pdf megnyitásakor két kedves kis adatsomagot küld a 218.240.24.199-es IP-jű szerverre, amelyek az én aktuális tevékenységem adatait tartalmazzák (URL/megnyitott file/stb).

Mi ez, ha nem kémkedés?

Vagy ez csak nekem tűnt fel egyedül?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.03.02. 11:27:41

Szia Bunkó!

Ha erre gondolsz, akkor ez az update szerver, és ha jól láttam, ki is kapcsolható.

forums.foxitsoftware.com/showthread.php?20783-connecting-internet-on-every-startup



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.03.02. 11:31:29

@Mindenki:

Linuxon a már említett Evince, Xpdf mellett az Okular is jó megoldás lehet, de természetesen rendelkezésre áll a linuxos Adobe is:

get.adobe.com/reader/?promoid=BUIGO

Ez még a színes, szagos, videós agyontrükközött pdf-eket is jól jeleníti meg.

Windowson pedig a Foxit és a Sumatra a legismertebb adobe pótló, ami nyilván nem tud mindent, csak sok mindent, Itt egy hosszú lista a készítő, editáló, megjelenítő programokról a különböző platformokon.

secure.wikimedia.org/wikipedia/en/wiki/List_of_PDF_software

Droli • <http://nivo.blog.hu> 2011.03.02. 15:11:53

A Windowson bátran ajánlom a Sumatrát, kicsi és gyors program .A Linuxon nálam az Okular vált be.

OFF: hasonló rémtörténet a szövegszerkesztők világa is, ahol sok ember lazán feltelepít egy többszáz megás monstrumot (pl. Microsoft Office), hogy aztán néha írjon rajta egy levelet. Pedig van egy rakat ingyenes programocska a neten, amely erre a célra alkalmas, pl. mostanában az Abiwordöt használom erre. És az egy dolog, hogy "nem a méret a lényeg", de az Office is előkelő helyen szerepel a "hogyan kapjunk könnyen vírust" listán. Az a bajom ezekkel a programokkal, hogy a sok, az átlagfelhasználók által soha nem használt funkciók mellett egy rakat biztonsági kiskaput is ad.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2013.01.10. 11:59:20

A Foxit és a Sumatra már volt korábban, de ezen felül is van még Windowsos alternatíva a Nitro Reader képében, hátha valakinek éppen ez jön be.

www.nitroreader.com/

Malware vadászat egy kicsit másképpen

2011.03.02. 16:10 | [Csizmazia István \[Rambol\]](#) | [8 komment](#)

Címkék: [microsoft](#) [malware](#) [mark](#) [rootkit](#) [segédprogramok](#) [hunting](#) [sysinternals](#) [russinovich](#)

Egy ritka színvonalas és tanulságos posztot olvashattunk a minap attól a Mark Russinovichtól, akinek segédprogramjait az egész világ víruslaboros elemzői használják, csatlakozása a Microsofthoz új időszámítást jelentett a Windows biztonság terén, és akinek azt a bizonyos 2005-ös [Sony BMG rootkit leleplezését](#) is köszönhetjük.



Írásában azt mutatja be, hogy **kártevő gyanús esetben hogyan lehet apró, de roppant hasznos rendszerdiagnosztikai segédprogramokkal sikeresen Sherlock Holmest és CSI-t játszani**. A történet azzal kezdődik, hogy egy amerikai kórházban a Mariofever nevű, hálózaton és hordozható eszközökön egyaránt terjedő kártevőt találnak. A trójai program kísérletet tesz az antivírus programok kikapcsolására is a megfelelő Registry bejegyzések törlésével, hátsó ajtót nyit a rendszerben, adatokat lop el és továbbít távoli szerverre - **magyarán egy manapság igencsak jellemző aktivitást vezet elő nekünk**.



A dolog a nagyközönségnek ott kezdhet érdekes lenni, hogy ezúttal nem a format C:\ vagy az "hívjunk össze konzíliumot, indítsunk el egy teljes keresést a frissített anti vírusunkkal aztán intubáljunk" módszert vetik be, hanem in medias res, **a homo ludens kíváncsian játszani kezd azzal, amije van neki, és az pedig nem más, mint a Sysinternals Listdlls**. Ezzel kerül látóterünkbe egy a Winlogon alatt betöltődő DLL, a nvrsm.dll.



Am egy másik Sysinternals programmal, az automatikusan induló dolgok listázására szolgáló Autoruns listájában ennek érdekes módon még sincs nyoma, így tovább kell ásni ezúttal a Process Monitorral. Nem löjük le teljesen a poént, **tényleg érdemes végigolvasni a lépésről lépésre részletesen bemutatott esetet, mi itt már csak spoilerезünk egy jóízűt**, elmondjuk **ki tette a nyomravezető lószórt a bárszékénybe**, és megmutatjuk a gyilkos Sysinternals Stringes képét :-)



Aki szeretne közelebbről is megismerkedni ezekkel a hasznos és remek eszközökkel, az [a Microsoft weboldaláról tudja ezeket a legbiztosabban letölteni](#), de emellett érdemes lehet néha [Mark blogját is felkeresni](#) a hasonló bejegyzések miatt.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2703360>

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](#).

Takoca 2011.03.03. 15:13:23

"az egész világ víruslaboros elemzői használják, "

ne menjünk ilyen messzire :)

szerintem minden informatikus használja őket: kb egy full-full extrás svájci biciskához tudnám hasonlítani a kis progikat!

Egyébként nagyon jó kis nyomozás ez, tényleg tiszta CSI!

fidesz = házmesterek pártja 2011.03.03. 15:44:58

@Takoca: minden IT-s Windows-t használ? ;-)

Takoca 2011.03.03. 15:49:44

@Atomot az indexre!: jogos.... na de másra meg nincs is vírus :)

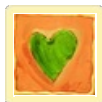
fidesz = házmesterek pártja 2011.03.03. 15:52:31

@Takoca: hááááát... biztosan én vagyok túl paranoid, de még a jogok nélküli linuxos userem alól sem mernék felmenni sok helyre. :-)

Nem beszélve a antivirus.blog.hu/2011/01/24/realitas_lehet_az_androidos_botnet cikkről. Mert ugye az android végeredményben egy linuxos mellékág...

Takoca 2011.03.03. 15:57:12

@Atomot az indexre!: én sem gondoltam komolyan



Kirándulás • <http://www.adventures.hu> 2011.03.03. 16:02:22

Istenem...

fidesz = házmesterek pártja 2011.03.03. 16:06:04

@Takoca: bocs, akkor félreértettem a smiley-t...



Van_mikrohullámú_sütőtök? 2011.03.03. 16:21:41

Nnna ez igen, ez kérem kártevő írtás! Így kell ezt csinálni kérem szépen.

Persze nem mindenki egy született helyszínelő: nos, nekik ott vannak az okos programok amik megcsinálják ugyanezt.

Azért a dologban benne van az is, hogy 2005 óta lám aki csak és kizárólag eredeti progit használ, nincs neten a gépe, lám az is kaphat rootkitet.

I like to like it like it

2011.03.04. 13:10 | [Csizmazia István \[Rambo\]](#) | [3 komment](#)

Címkék: [facebook](#) [kártevő](#)

Többféle csali üzenettel is terjednek új megtévesztések a Facebookon. Akik arra fogadtak, hogy az "**az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót**" nem a legutolsó Facebookos trükk volt, azok most mehetnek a kasszához: nyertek.



Az egész úgy kezdődik, hogy a felhasználó váratlanul kap egy üzenetet látszólag az egyik ismerősétől. Mivel ugye nem idegentől jön, ez már sokaknak ok lehet arra, hogy bátran rákattintsanak. Többféle üzenet verzió létezik, az egyik - már nem először - valamiféle sokkoló videót ígér - ezúttal Miley Cyrusról, egy másik Emma Watson nevével él vissza.



Felugrik, hogy oszd meg az adatlapodon...



Ide visznek a linkek...

Rákattintás után egy weboldalra érve mielőtt még meg tudnánk nézni a videót, előbb lájkolni kell, majd jön még ilyen felkérés is kérdőívkitöltésre (igazából elég csak lekattintani), akkor megnézhetjük a videót, hurrá! Ez utána aztán "természetesen" kikerül az üzenőfalunkra, és egy új oldal is bekerül a kedvenc Facebook oldalaink közé. De az ügymenet ezenkívül sokféle lehet még, az is sokszor előfordul, hogy egy ismeretlen alkalmazás telepítését kérik előbb tőlünk.



Ha a play gombra kattintasz, előbb lájkolnod kell...



Ezt kell kitöltened...

A folyamatok a kártevőterjesztők részéről már eléggé jól bejáratottak, és öngerjesztőek is, hiszen részint aki felelőtlenül kattint, az rászabadítja ismerőseire a komplett Szomodát és Gomorrát. Ha pedig megszabadulni akar egy jelentősebb Facebookos kártevőtől, és begépeli annak nevét a Google keresőbe, biztos számíthat arra is, hogy már 10-15 százaléka a megjelenő linkeknek vezet kártevővel fertőzött, jó előre elkészített weboldalakra.



Meg ezt is...



Meg még ezt is...



És ezt is...

A Facebook egyébként **valahol zseniálisan fedte le a platformfüggetlen kártevők kérdését: bármilyen OS alól kattinthat a kíváncsi juzer**, aztán operációs rendszertől függően vagy a számítógépe is megfertőződhet, de a profilja az ismerőseivel így is, úgy is mindenképpen kompromittálódik. Nem egyszerű a dolog mindenesetre, hiszen miközben az egész rendszer arra szolgál, hogy mindeféle laza logika mentén kifejezetten biztasson a megosztásra, lájkolásra, eközben **[a felhasználóktól nem várhatja el a szolgáltató, hogy biztonsági szakértők legyenek.](#)**



Feloldottuk a videót, mert lekattintottuk a hivatkozásokat...



Működik a videó. Nem Youtube, YouTubo...

Az egyik tanulság az, hogy **sajnos nem érdemes arra bázírozni, hogy majd gondos kezek Facebooknál gyorsan röptében kitakarítják a gyanús, kártékony linkeket, alkalmazásokat**, erre jó példa **[a mostani egyik trükk is, ami már 2010 október 7-én is biztosan terjedt](#)**, és még azóta is közöttünk van.



Jé, kikerült az adatlapodra ez itten kérem tisztelettel...



A kedvelt oldalaid közé is bekerült ez valahogy...

Arról a paradox sorrendi kérdésen lenne érdemes tűnődni: ha valamit csak azután nézhetek meg, hogy likeolom, akkor vajon ez kinek lehet az érdeke? Vett már valaki úgy autót, hogy először kifizette és csak aztán nézte meg?



Szóval ha egy másik tanulságfélét is le kellene vonni zárásként, az úgy szólna: ha valami tényleg tetszik, azt kellő megfontolás után bátran lehet lájkolni. **Ám ha valamiről csak és kizárólag a lájk után tudjuk meg, miről is van szó valójában, akkor az így látatlanban nagy ívben kerülendő.**



62 személy kedveli ezt **[Regisztrálj](#)**, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2708975>

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](#).



[MeriFast 2011.03.04. 14:19:46](#)

Itt van mégegy gyönyörűség
kephost.hu/share-9769_4D70E5FB.html



[atko 2011.03.07. 05:15:15](#)

Most akkor nyomjak egy tetszik gombot a cikk végén? :-)



[gothmog 2011.03.12. 21:31:56](#)

Lályk.

A hamis antivírusok újabb kalandjai

2011.03.08. 12:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [botnet](#) [antivirus](#) [leleplezés](#) [brian](#) [rogue](#) [krebs](#) [chronopay](#)

Mindent lehet egy picivel még jobbra tenni, még tovább fejleszteni, és az világosan látszik, hogy ezt a nemes küldetést csöppet sem veszik félvállról a hamis antivírus programok készítői, terjesztői.



Arról már korábban is beszámoltunk, hogy a folyamatos újítás jegyében **valóságos termékek nevére hajazó hamis programok is megjelentek** - például Smart Security, XP Smart Security, Windows Smart Security, WireShark Antivirus vagy SysInternals Antivirus - [lejárta ezzel az eredeti márkanevet, illetve a hatékonyabb megtevesztés jegyében](#) megzavarva a félinformációkkal rendelkezőket. Ezek a programok mind álvírusirtók, **amelyek nem létező fertőzéssel ijesztgetik a felhasználókat, majd a "mentesítést" elvégezni képes teljes értékű változatért 30-80 dollár körüli összeget kérnek**, amelyet Mastercard, Visa vagy PayPal utalással lehet teljesíteni.



Ezúttal a [ChronoPay cégről derültek ki további érdekességek Brian Krebs jóvoltából](#). Már az is vicces volt, amikor az elején még azzal védekeztek, rendszerüket - amely eredetileg hitelkártyás fizetési lehetőséget biztosított kiskereskedőknek - csupán megfertőzték, de nekik maguknak semmi közük nincs a hamis antivirus terjesztéshez, és más számítógépes bűncselekményekhez. Aki azonban folyamatosan figyelemmel kísérte az eseményeket, ennek pontosan az ellenkezőjét tapasztalta, vagyis hogy **igenis vastagon benne voltak és kihasználták, sőt irányították ezt a fajta bizniszt**. Erről számos szakmai cikk, többek közt a [Washington Post is beszámolt már évekkorábban](#). Ezúttal még újabb dokumentumok, bizonyítékok szivárogtak ki minderről, amelyek további érdekes részleteket fednek fel.



Emlékeztet, hogy 2009-ben a Microsoft és a Symantec tanulmánya már említette, hogy **a TrafficConverter.biz az egyik legnagyobb hamis védelmi szoftvert terjesztő hálózat volt**. A számos webhelyet felölelő kiskereskedői hálózatra emlékeztető modell **jutalékot fizetett a kártékony kódok terjesztéséért** és a modell sikerességére jellemző, hogy a TrafficConverter.Biz üzemeltetői **a legaktívabb hamis AV terjesztőnek versenyt írtak ki, melynek fődíja egy 36 ezer dolláros Lexus gépkocsi volt**. Meg is tehették mindezt, hiszen egy szintén 2009-es felmérés alapján [a cég tíz legnagyobb értékesítője akkoriban heti 23 ezer dollárt \(azaz 4.4 millió HUF\) keresett, ami úgy háromszorosa az Egyesült Államok elnöki fizetésének](#). (Nyilván ehhez a nagyságrendhez igyekezett igazítani az MS is a maga 250 ezer dolláros kitűzött vérdíját.) **A Trafficconverter.biz bezárása végül akkor következett be, amikor a Microsoft kérelmezte és hozzájutott a Conficker férget terjesztő domaineinek listájához.**



A ChronoPay az évek folyamán azonban szorgalmasan dolgozott tovább, és 2010. márciusában például az F-Secure kutatói figyeltek fel arra, hogy egy **újabb megtevesztési módszer indult be, amely látszólag RIAA szerzői jogi figyelmeztetéseket tartalmaz, és a kb. 400 USD befizetése ellenében mentesülünk az állítólagos torrentezés miatt várható állítólagos börtönbüntetés és a per alól**. A közös most is mindegyikben az, hogy itt is a semmiért a csalóknak fizetnek a becsapott emberek.



Az eredeti cikk végén található egyik PDF mellékletben 12 oldalon sorolják a [különböző, ChronoPayhez tartozó kártékony kódokat terjesztő domaineiket](#). Ebben többek közt az a hírhedt Shieldec.net is megtalálható, amelyet a [botneteket feltérképező Zeus Tracker is megjelölt korábban](#), mint az egyik jelentős hamis antivírus terjesztő oldalt. A kiszivárgott dokumentumokból többek közt az is kiderült, hogy **a hamis antivírus üzletág két általuk alapított ciprusi offshore cég, a Yoliand Holdings és a Flytech Classic Distribution Ltd. irányítása alatt működött**. Ugyancsak érdekes az a [75 oldalas bizonylat is, amely a fake programok megvásárlásáról szóló bankkártyás](#)

[tranzakciókat tartalmazza](#), és jól látható, hogy **mindössze egyetlen óra leforgása alatt akár 80-100 befizetés is történik**. Érdemes a teljes cikket végigraggni, amelyben az évek alatt alapított, megmozgatott cégekről, és 2008-2010 közötti időszakban elkövetett üzemeikről részletesen beszámolnak.



Arról már olvashattunk a blogban, hogy az ügyvédeknek újabban mekkora nagy szerep jut a kártékony kódok elleni harcban. Emlékezzünk csak arra, amikor **Eugene Kaspersky** cégét a **Zango** nevű online reklámcég **bepereelte az USA-ban arra hivatkozva, hogy a kártevőként való detektálás rontja az üzletmenetüket és a jó hírnevüket**. Az évekig tartó per végül a Zango (korábban 180Solutions) csődjével és az antivírus cég győzelmével zárult. De említhetjük azt is, amikor [az ESET a tájékoztatás alapján kopogtatta a hamis antivírus készítőket és követelőztek, hogy az adatbázisból 14 napon belül távolítsák el a WinAntiVirus Pro 2006 detektálását](#). A korábbi hosszadalmas Zango-per óvatossá tette az antivírus cégeket, és **kénytelenek minden egyes esetben alaposan utána nézni, ezer százalékig biztosra menni**. Pontosan ilyen jogi okok miatt nincs alapértelmezés, és kell a NOD32 telepítéskor minden egyes felhasználónak magának kézzel kiválasztania, akarja-e szűrni a kártékony alkalmazásokat is vagy sem.



Éppen ezért eléggé hihetetlen, és **inkább megtévesztési manővernek látszik egyelőre az is, hogy a ChronoPay jó útra térne, és mostantól Saulból Pál lesz: képeslapok és díszműárak terjesztésével fog foglalkozni a legális antivírus bizniszben teszi majd tiszteletét ChronoPay Antivírus néven**. Bár örömmel üdvözljük, hogy "olyan egyszerű és letisztult felületet szeretne, mint az ESET-é", Pavel Vrublevsky [ezen állítását majd igazából akkor hisszük el, ha a termék valóban meg is jelenik](#), és majd megvédi első VB100 díját.



Ha már a módszereknél tartunk, már korábban is láthatóak voltak olyan kezdeményezések, amikben a [Bejelentett Támadó Webhely ablakát utánóztatva igyekeztek megtévesztetni a nagyerőműt](#). Ezekre, a [legitim böngésző üzenetekre hasonlító, preparált, megtévesztő ablakok felbukkanásáról írt a Zscaler](#). Ám az **igazi újdonság ezúttal ebben az, hogy először bukkant fel a különböző böngészőkre szabott hamis antivírus**. Firefox alatt például nem csupán Firefox grafikai elemeket használnak fel benne, de közben manipulálják is a kártékony oldalakra történő figyelmeztető ablakokat is a jó öreg: fertőzés gyanú, kattints a Start Protection gombra a "mentéshez", fizess trükkel. Az a vicces az egészben, hogy **a használt böngészőkliens függvényében minden kliensen testreszabva jelenik meg, például Chrome alatt az ottani megszokott elemekből áll, de természetesen tudja ezt Iovon és trapéz is, így van Safaris változat is**.



Jó hír lehet, hogy a számtalan, folyamatosan bővülő How to Remove útmutatókon felül [számos antivírus cég kínál letöltésre ingyenes egyedi rogueremover segédprogramot](#), ugyanis a mentés sok esetben nehézkes, sok komponenst érintő fáradtságos és összetett folyamat. Emellett szemlátomást kialakult egy hamis vírusok eltávolítására specializálódott fejlesztői kör is, egyikük - a Frontline Rogue Remover - még a YouTube videóval is reklámozza magát. A [weboldaluk kinézete kissé hasonlít a hamis antivírus oldalakra](#), de állítólag valóban mentesít. Ha esetleg használta már valaki, bátran kommenteljen a tapasztalatairól.



Egy biztos, ez az "üzletág" egyre inkább virágzik, így mi csak annyit tehetünk, hogy egyfelől használunk valamilyen valódi megbízható, nem fake antivírust, másfelől pedig [még óvatosabbak, alaposabbak leszünk, és jobban vigyázunk](#) netezés közben.



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



• [1 trackback](#)



Ajánlott bejegyzések:

- [Majdnem mindenki átverhető adathalászzal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2719920>

Trackbackek, pingbackek:

[Trackback: Amikor azt hiszed, biztonságban vagy: hamis vírusirtók](#) 2011.03.12. 17:15:30

Gondtalanul szörfölsz a neten, nézelődsz, linkekre kattintasz, aztán egyszer csak az egyik ablakban felugrik a figyelmeztetés: "VÍRUSOS A GÉPED!" A gép helyett ilyenkor az átlag felhasználó fagy le, hogy jaj, mostmileyen??? Pe...

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 hirdetések titkos élete

2011.03.10. 13:35 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hirdetések](#) [fertőzött](#) [dasient](#)

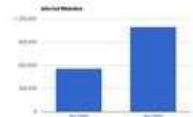
Kétszeresére nőtt egy év alatt a [kártékony weboldalak](#), valamint a fertőzött hirdetések száma egy friss vizsgálat szerint.



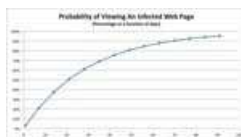
A Dasient 2010 negyedik negyedévét vette górcső alá, és úgy találta, a [kártékony kódot tartalmazó hirdetések](#) száma az előző negyedévhez képest **100 százalékkal**, másfél milliőről három millióra növekedett. Elképesztően nagy szám ez, **magyarul naponta ennyien kattintanak fertőzött hirdetésre**.



De nem szebb az arány sem, mely szerint **egy átlag internetező három hónap leforgása alatt 95 százalékos valószínűséggel fut bele** egy ilyenbe és [fertőzi meg a számítógépét](#). Azt pedig már mondani sem kell, hogy a bűnözők előszeretettel használják a szociális hálózatokat is ilyen [kártékony hirdetések](#) terjesztésére.



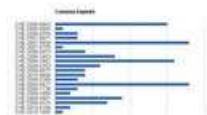
A Dasient [igyekezett alapos lenni és jól elvégezni a házi feladatát](#), ezért aztán **nagy furmányosan teszt kódokkal ellátott** (nem vírusos, nem fertőző, hanem exploitokat kihasználva például elindították a felhasználó gépén a calc.exe számológépet) hirdetésekkel helyezett el és figyelte, mennyi idő után távolítják el azt a rendszerből a rendellelenes és gyanús viselkedése miatt. Lehet tippelni, mennyi volt ez: volt eset, hogy kevés híján négy hét is eltelt, mire a hirdetést letiltották.



Maga a teszt hirdetés szövege úgy szólt, hogy "Kattints ide egy biztonsági ellenőrzéshez, ha a végén a számológép megjelenik a képernyődön, akkor sebezhető a rendszered, és haladéktalanul frissítsd a Java Virtual Machine-t". A hirdetés így is kapott 159 ezer megjelenést, és 103 kattintást. **Ha ugyanezen a helyen egy dekoratív hölgyemény mélyen alul öltözött fotóját, és a veszélytelen hackerhome.org helyett valami durvoid malwareterjesztő oldalra irányították volna**, akkor ezek a számok nagyságrendekkel nagyobbak is lehettek volna.



A kísérlet során az is kitűnt, hogy a bit.ly linkrövidítési szolgáltatás ellenőrzi a rövidítendő linkeket a Google SafeBrowsing List segítségével, valószínűleg ez lehet az oka annak is, hogy számos szociális hálózatban nem tartják azt veszélyforrásnak és engedélyezik a használatát. A Chrome és a Firefox böngésző kliens egyébként már régebb óta beépítve tartalmazza Google SafeBrowsing szolgáltatást, és 2010 március óta [a Twitter is ezzel ellenőrzi a közvetített linkeket](#).



A hirdetési ügynökségek tulajdonképpen legtöbbször semmilyen ellenőrzést nem végeznek az eladott hirdetésekben, hajtják a pénzt, és

minden eladatlan szabad helyet igyekeznek értékesíteni - eddig tart az ő figyelmük és kompetenciájuk.



Emiatt a szakértők a **2011-es évben a hirdetésekkel terjedő kártékony kódok mennyiségének meredek emelkedésére**, valamint a szociális hálózatokon jelentkező támadások számának hasonlóan erőteljes növededésére számítanak. Lehet beizzítani az AdBlock Plus-t és a NoScriptet...



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2727118>

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.

Óvakodj a görögöktől, még ha ajándékot hoznak is

2011.03.16. 18:10 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [skype csalás](#) [trójai](#) [antivirus](#) [hívás](#) [rogue](#)

Néhány trükkös csaló nem tud annyira elképesztően képtelen forgatókönyvet kitalálni, hogy az ne legyen mégis sikeres.



Egyedül nem megy, pamparam, egyedül nem megy. A csaláshoz is két résztvevő félre van szükség. Az egyik maga a csaló, a Homo Simliensis áll velünk szemben teljes életnagyságban, de a sikeres lebonyolításhoz ugye kell még maga az áldozat is, a Homo Naiviticus. **A naívság kiemelése itt most nem valamiféle frappáns szófordulat, hanem maga a szomorú rögvalóság.** Életkortól függetlenül ugyanis valóban kínzó kérdés: ki az, aki egy Skype rendszeren érkező kéretlen telefonhívásnál valóban elhiszi azt, hogy egy ismeretlen által küldött link igazi, hamisítatlan, abszolút megbízható Microsoft biztonsági javító frissítéshez vezető út, amely csak a javunkat szolgálja.



Annyit azért persze a csalók javára lehet írni, hogy egy, csak egy gomb van talpon a vidéken: "Erase all Threats" néven, **"kilépés", vagy "mégsem" egérutat naná hogy nem kínálnak fel.** A lefutó script pedig [akár egy Macen vagy egy Linuxon is mutatja](#) a 364 darab Windows fájl érintő igen súlyos "fertőzést" :-). Sőt az idők szele már az is jól mutatja, hogy [20 USD ellenében a rogue antivirus nevű semmit nem csak Windows, de már OS X alá is](#) megrendelhetjük, csak most, csak nekünk.



Az ötlet persze egyébként jó, mindig is bővül a paletta, csak úgy, mint az, hogy mostanában az igazi IRL csalók is úgy csöngetnek be az egyedülálló idősekhez, hogy visznek egy kiló krumplit és egy kiló hagymát: az önkormányzat küldi nagy tisztelettel felkiáltással. **Akik pedig nem ismerik a "timeo Danaos et dona ferentes" latin közmondás igazságát, azok sajnos ezzel fogják azt majd közelebbről megtapasztalni.** Szerencsétlen idők pedig esetleg csak napok múlva, a nyugdíjuk, spórolt pénzük eltűnése után döbbennek rá, csalókkal kerültek szembe, akiknek persze busásan megérte az "ajándékra" költött néhány forint, **mert annak segítségével bejutottak.** Ugyancsak divatos, hogy a szintén egyedülálló öregekhez azzal az ürüggyel csengetnek be, hogy régi iskolájuk szeretne az egykori tanulóiról tablóképet készíteni, és ehhez készítenének most a lakásban egy fotót. Ha pedig valaki az ismeretleneket egyszer már beengedte a lakásba, akkor az értékeknek megintcsak jó eséllyel lába kel.



Kicsit hasonló a helyzet a számítógépes betolakodók frontján: [ha éppen mi magunk tárjuk sarkig nagyfokú naivsággal az orcánkon az ajtót a trójaiaknak,](#) és egyéb kártevőknek, biztosan elszenvedünk valamifajta káreseményt: **hátsóajtót nyitnak rendszerünkben, ellopják a jelszavainkat, banki azonosítóinkat, vagy folyamatosan figyelik billentyűzet leütéseinket,** esetleg mindezeket együtt. A nagy kedvenc ebben a műfajban az a fertőzött szériaszám generátor, amely még tájékoztat is, hogy némely vírusirtó "tévesen" riasztana, ezért a futtatás előtt ugyan legyünk már olyan kedvesek, és kapcsoljuk ki addig a vírusvédelmünket. **Ez már az a szint, amikor az ablakunk alól még külön be is kopognak papírért.**



Jó lenne ha mindenkinek feltűnne már végre a La Fontaine mesék azon igazsága, miszerint "ne várjuk könnyörületet a könnyörtelentől". Magyarul [az egészséges túlélés érdekében](#) tudni kell, kitől mit várhatunk. Legalább **legyen valamiféle körvonalazott elképzelésünk, mit honnan illik, lehet, kell, érdemes, tilos beszerezni, letölteni,** és ettől a bevált ökölszabálytól semmilyen kéretlen levél, üzenet, Skype hívás ne térítsen le bennünket.



6 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2743784>

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](#).

[Advocatus Diaboli 2011.08.24. 17:53:04](#)

A legjobb vírusvédelmet Linuxnak hívják!!!

40 éves a számítógépes vírus

2011.03.18. 14:55 | [Csizmazia István \[Rambol\]](#) | [9 komment](#)

Címkék: [történelem](#) [vírus](#) [40 éves](#) [kárttevő](#) [creeper](#)

Hát felnőtt a kicsike. Bár a "Boldog születésnapot" kicsit durva lenne, azért csak megemlékezünk az első [computer vírus megjelenésének](#) időpontjáról, [nosztalgia](#)zunk egy jóízút a kártevők korai alacsony számát illetően, és felidézünk pár hősi emléket.



Soha se felejtjük el az elsőt - és ez nemcsak a randira áll, de hihetetlen módon nincs másként a számítógépes vírusokkal sem. [1971-ben a Creeper nevű vírus történelmet írt, és új fejezetet nyitott a programozás történetében.](#)



Idősebbek és katonaviseltek még emlékeznek a Turbo Pascalt idéző F-Protra

Egy [PDP gépen futva](#) (nem mond ez semmit azoknak, akik már abba születtek bele, hogy CD lejátszó nélküli gépet egyszerűen nem is láttak) majd a korai DOS-os PC világban az akkori vírusok még keresték a feltűnést, és **mindenfélét nagy látványosan kiírkáltak a képernyőre**, például: ["I'm the creeper, catch me if you can!"](#) vagy ["Your PC is now STONED!"](#). Manapság ez éppen pont fordítva van, némán rejtőzködnek, ehhez akár rootkitre is támaszkodnak, és igyekeznek titokban, hosszú ideig kémkedni, ügykődni a megfertőzött gépen.



A HTScan, amiben még szövegfájlban editálhattuk a szignatúrákat. Azóta már kriptográfiai aláírással, titkosítva és tömörítve illik az adatbázist készíteni

Az egyik "kedvenc" DOS-os a sok közül - ekkoriban volt divat a Yankee Doodle-t is különféle időpontokban a speakeren eljátszani - [az Ambulance volt, amely a karakteres képernyőn ASCII grafikával megrajzolt mentőautót mozgatott](#) át éktelen szirénázással, hát képzelhetjük az akkori sikító titkárnőket.



Álmomban két mentő autó voltam, és magammal játszottam ;-)

A nosztalgia egyébként terítéken van, nemrég [Mikko Hyppönen járt Pakisztánban, és felkereste a Brain vírust készítő testvérpárt](#), hogy interjút készítsen velük.



Szorgalmas emberek a hamburgi VTC-ben táblázatban vezették a makrovírusokról szóló összefoglaló táblázatot

Vegyük észre, hogy a 80-as években, 90-es évek elején az akkori letöltések hogy történtek: MS DOS rendszer, monokróm Hercules monitor, AUTOEXEC.BAT, CONFIG.SYS, jó kis VIRNET, 3600 baud modem, 8 adatbit 1 stop bit, betárcsázós BBS, vonalszakadás, foglalt, etwas.



Vírus a számítógépes magazin CD mellékletén. Még a Déli Krónikában is bementék, hogy mindenki vigyázzon

A szignatúra frissítések ekkoriban még csak kb. havonta jöttek. Azóta aztán a párszáz, pár ezres számról a ma már szinte hihetetlen számmillió értékhez értünk.



C programozóknak érdekes csemege lehet a vírus eredeti forráskódjának tanulmányozása. Ez volt azért a ritkább eset, többnyire izzadságosan magunknak kellett visszafejteni

És anno valóban lehetett a programozásnál csak és kizárólag a jó végeredményre, a működőképességre koncentrálni, azonban **ma már a biztonságos programozás elengedhetetlen eleme lett** a szakmának.



A HTScan, és egy a több magyar alkotás közül, itt most Nagy Ferenc László programja.

Manapság már értelmetlen egy adott időponttól félni, nem tartunk az egykor rettegett péntek 13-ától sem, hanem csak úgy ambloc lehet az egész jövőtől :-). Az egyik korábbi **A Vírusok Varázslatos Világa** cikkben már felidéztünk pár jelentős vírus alkotást Melissától CIH-ig, itt a 12-es epizódban lehet elolvasni ezt a cikket. Jómagam a szerencse fiának érezhetem magam, mert a PDP hőskora ugyan kimaradt, de munkám és hobbim során a lyukkártyától a lyukszalagon át XT-AT-386, 486, Pentiumok is, sőt olyan home computernek nevezett házi kedvencek, mint Spectrum, C64 is "megvoltak" egészen a mai korszerű gépekig. Így a PC-s vírusokat már az elejétől figyelemmel kísérhettem, nekem potyogtak le a karakterek az alsó sorba :-)



A táblázatban egy négyszáz gépes nagyvállalat kéthavi fertőzése 1997-ből. Ilyen kevés támadással manapság azért sokan cserélnének

Aki pedig szeretne egy kicsit a gyakorlatban szöszmötölve kipróbálgatva elrédetni a múltban, annak a **Slovak Antivirus Center** **AVMUSEUM** letöltési szekcióját és a **DOSBOX programot** ajánljuk jó szívvel.

 20 személy kedveli ezt [Regisztrálg](#), hogy megnézd, mi tetszik az ismerőseidnek.

  0 

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2749617>

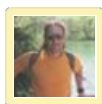
Kommentek:

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> 2011.03.18. 15:01:58

amblock: helyesen: en bloc
bocsika ;)



**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
2011.03.18. 15:32:07**

Szia Xaba99!

Köszí a szöveget, már javítottam. További Creeper mentes gépet kívánok :-)



[xaba99](#) • <http://landf.blog.hu> 2011.03.18. 15:47:44

Szia,

az sajnos azt hiszem pont nincs meg, pedig van egy néhány száz darabos gyűjteményem...

[kpityu2](#) 2011.03.18. 19:30:40

A régi szép idők, amikor az Enterprise-osok boldogok voltak hogy végre az ő gépekre is van vírus. :D Ami floppy-n terjed...

[szb9](#) 2011.03.18. 19:36:06

Floppys hardvervírus megvan? Sűrűlódásra gyúlékony/robbanékony anyagot tettek a floppyba, aztán az áldozat gépe bánta, ha betette a meghajtóba és olvasni próbálta...

[H Stahl](#) 2011.03.18. 19:45:44

Nekem meg még megvan a hivatkozott 98/9-es CIH vírusos PC Guru cd! Vitrinben tartom. Szerintetek mennyit adnának érte Vaterán? :D



[Nomante 2.0](#) 2011.03.18. 19:56:20

hú, én a OneHalf nevű vírustól /s annak variánsaitól/ fostam... nálam ő volt az ultimate vírus.

moshi (törölt) 2011.03.18. 20:52:21

Hőskor. Egyszer elővigyázatlaniságból megfertoztem egy novell szervert a michelangeloval. Ott meg ugye nem üres az első Cylinder nagy része, tehát nem várta meg a márciust, azonnal leállt az egész. Mehettem vissza a központba, assemblyben írni egy programot, ami a bentli novell szerverről lementi a hatodik (hetedik?) szektor, aztán megint ki a fiókba, ott meg fel. És működött! :) ez volt a világ legegyszerűbb virusirtása.

Exicom Kft. 2013.08.05. 15:05:57

Azok a régi szép idők.... ;)

Robog a trójai úthenger

2011.03.21. 16:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hamis trójai rendszerkarbantartó utility rogue defrag](#)

Fedélzetén persze nem Józsi vagy Odüsszeusz utazik. **Bár ez utóbbi azért felmutatta a mintát az utókornak, ezt mindenképpen a számlájára írhatjuk**, így ha esetleg csuklanának a felmenői, az korántsem a pusztán véletlen műve.



Egy ősi dakota közmondás szerint "A chiliszósz nem más, mint egy határozott fellépésű ketchup". Ennek analógiájára **a trójai biztonsági programoknak sem kell a szomszédba menniük egy kis határozott fellépésért**, vagy szimplán csak amiatt beiratkozni egy Szabó Ervin könyvtár nevű műintézménybe, hogy az ilyen jellegű fellépésről puhatolózva megtudjanak egymás alapidolgot.



A hamis antivírusok a maguk mellbevágó üzeneteikkel már befutottak egyfajta komoly karriert az utóbbi években, és mivel a terjesztőik részéről féltő, hogy sokan majd tanulnak a más vagy éppen a saját kárukra, veszthet a lendületéből a hamis fertőzésekre figyelmeztető, értéktelen, de pénzt zsaroló antivíruscsomag biznise. Ezért aztán **gőzerővel és folyamatosan dolgoznak a bűnözők is, mivel is lehetne még bővíteni az eszköztárat**. A korábbi kamu nevek mellett egy idő után [bepróballoztak a valódi alkalmazások neveivel való visszaéléssel is](#), ami kétségkívül már haladó csoportosan is mélyen szofisztikált megoldásnak számít. Persze nem állt meg itt az élet, és [akár a zseniálisnak is mondható hamis RIAA figyelmeztetést](#) nézzük, akár a körülbelül [tavalay januárja óta szórványosan megjelenő adatmentő, adatjavító](#) alkalmazásokra gondolunk, tény: **az ilyen egyéb "segédprogramok" egyre inkább keresik az új medreket, és lassan felzárkóztak az álvírusirtók mezőnyéhez**, sőt képletesen szólva lassan akár a csapatászlót is átvehetik rövidesen.



Egy igen jó kis összefoglaló jelent meg ezzel a jelenséggel kapcsolatban, ahol is csokorba szedve láthatjuk a [sokféle frappáns, de igazából hamis smart defragmenter, diskutility, hdd doctor, és hasonló nevet](#), de azt is megtudhatjuk, **milyen DLL trükkökkel ír ki a kártevő hamis Windows rendszerüzenetet, sőt hamisított Safe Mode képernyőt is kapunk háttérkép BMP-ben, ami látszólag újraindítást kér**, majd a program engedélyt kér, hogy "javítsa a felmerülő lemezproblémákat", de persze a vége már az ismerős forgatókönyv szerint zajlik: a nem létező bajok megmutatásán túl a **"javítást" is elvégezni képes "teljes verzió" már sajna fizetős**, ezért aztán lehet alfa szögben előkészíteni a bankkártyákat.



A trójai eltávolítását is igyekeznek minden eszközzel megnehezíteni, például ezúttal olyan részletekbe ereszkedő furmányoknak is tanúi lehetünk, mint a háttérkép cseréjének megakadályozása Registry bejegyzés segítségével.



Az új üzletág erősödésének fényében újabb figyelmeztetéssel bővíülhet a már korábban itt szajkózott, és memóriafogason tárolható repertoárunk: tartsuk naprakészen az operációs rendszerünket, használjunk megbízható antivírust, kémprogramirtót és tűzfalat, ne válasszunk ismeretlen, bizonytalan vírusvédelmi programot, sose telepítsünk olyan alkalmazást, amelynek [szinte minden említése a Google-ben "How to Remove"-val kezdődik](#). És akkor jöhet a legújabb: **a rendszerkarbantartás segédprogramjai ugyanolyan bizalmi kérdéskörbe tartozó alkalmazások, mint egy vírusirtó, akármire ne bólintson az, aki valódi biztonságra törekszik**. Borítékolhatóan tovább fog nőni a laikusokat zavarbahozó, hamis rendszerkarbantartónak látszó trójaiak száma, így mindenkinek érdemes lesz böngészés közben alaposan résen lenni.



5 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



0



Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2758304>

Kommentek:

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

Nincsenek hozzászólások.

E-set Antivirus 2011, ezmiez?

2011.03.23. 14:35 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [hamis 2011](#) [antivírus](#) [antivirus](#) [av](#) [rogue](#) [e set](#)

Igérjük, más témákkal is fogunk foglalkozni a hamis vírusokon kívül, de ez most egyfelől újdonság, másfelől ezt a hamis programot merő véletlenségből pont E-set Antivírus 2011-nek hívják a keresztségben.



Na szóval [már több menetben is tollhegyre tűztük az ismert](#) programok neveire hajazó hamis vírusok tematikáját, ám [most a korábbi Smart Security mellett feltűnt egy újabb rogue AV: az Eset Antivirus 2011](#). Vajon igazi lehet? Remélhetőleg ez a kérdés olvasóink fejében csak költői.

Aki csak életében egyszer is látott már valamilyen NOD32 programot, az tudhatja, hogy ez a [minden évben új verziós évszámos divat mizéria](#) hála Istennek **nem mótelyezte meg az ESET fejlesztőit**. Ha előfizetünk egy évre, akkor igen korrekten mindegy mikor vesszük, mindegy hogy 1.0 vagy 100.100 az aktuális termékverzió, **használhatjuk azt egészen a licenc érvényességének végső lejártáig**. A képernyőn látható vírusirtó cég nevének E-set, valamint a [NOD32-t fejlesztő valódi ESET](#) írásmódja közti különbség észrevétele már haladócsoporthoz Sherlock Holmes felismerés lehet, ennek beazonosítását ezért nem is várhatjuk el a hétköznapi átlagfelhasználóktól, sőt a következő hamisprogramban már lehet hogy antinemecsekként csupa nagybetűvel írják majd.



Szerencsére van szembeszökő különbség, ez itt a valódi

Ám ami a legfontosabb - és ezt érdemes is leszögezni, mielőtt megjelenik az E-SET Antivirus 2011, a NOD32 2011, E-SET Smart Security 2011 és hasonló vírusirtók: **minden korrekt és megbízható vírus program kínál egy teljesértékűen használható teszt időszakot - ez lehet 2 hét, 1 hónap - ami alatt FIZETÉS nélkül, mindenféle vagy jelentős korlátozás nélkül használhatjuk az adott terméket, és természetesen IRTANI is tudunk vele ingyen.**



Smart is, meg Security is, ám az igazihoz vajmi köze sincs

Egy korrekt és megbízható vírus program **nem jelenik meg váratlanul böngészés közben, hanem mi magunk telepítjük, mi választjuk ki, addig semmilyen üzenetet nem produkál.**

Egy korrekt és megbízható vírus program **nem ijesztget fertőzésekkel, és semmi esetre nem kapcsolja ezt össze azzal, hogy megzsaroljon minket**. Mindössze annyit tesz, hogy tájékoztat a licenc lejáratáról, és érdeklődés esetére ad egy linket a fejlesztőkhöz vagy a legközelebbi kereskedőhöz. A fizetés a vásárlási konstrukció fixálása előtt maximum tájékoztató jellegű ármegjelölésként jelenik meg.



A szakma annak idején elítélte, én **személy szerint viszont tökös húzásnak tartottam a tolvajok trükkös megleckéztetését**, akik hamisítással, lopással munka nélkül igyekeznek más hátán sikereket elérni, más fáradságos eredményét, jól csengő bevezetett márkanevét lejárta meg nem érdemelt sikereket elérni. Éppen ezért nekem tetszett, amikor [Kaspersky bácsi fogta magát, és a felismerési adatbázisba betett pár kamu detektálást, feltöltötte a VirusTotalra aztán figyelte, kik és hány nap után másolják az ő riasztásait hasonló vagy akár tök ugyanolyan névvel](#). El is vérzett az a pár AV cég, igazából sok logikus magyarázattal nem igazán szolgálhattak (csak pusztán véletlenségből lett mind a tíz mintának hajszálpontosan egyező a neve, egy öreg jósnő adta oda ezeket a szignatúra neveket egy mormota vérrel írt jegesmedve bőrére írt listán újhódkor a kiserdő mögött, a víruslaborosok három sör után egyszerűen megálmodták, vagy esetleg maga Uri Geller iderepült és transzbaesve segített a névadásban): az adatbázis lopás volt az egyetlen lehetséges ok. Nyilván az

emberi természet keveset változik, és bár a lopás az mindig lopás, azért "[a fű zöld, a másolók másolnak](#)", hamisítanak.



Vigyázó szemetek a logóra vessétek! Hol is láttam már ezt?

A csalók repertoárjában a nevek jönnek-mennek, ezért nehéz idők ezek az ismert márkák évtizedek alatt kivívott hírnevének megőrzése szempontjából is - és ne legyenek illúzióink, más antivírus gyártók is áldozatul esnek ennek, íme egy [AVG-s screenshot ennek demonstrálására, itt már a céges logót is lelopták hozzá](#). Élesszeműek pedig észrevehették az égbekiáltó anakronizmust is: az E-set programnál is az AVG embléma volt látható.



Mindig van lejjebb: itt már az AVG emblémát is pofátlanul lelopták

Végül de nem utolsó sorban szintén **erősítheti a biztonságunkat, ha vagy közvetlenül a magyar disztribútornál, vagy a már korábban bejáratott, ismert, megbízható, technikai támogatást is nyújtó viszonteladóknál** vásárlunk programot ismeretlen domainről domborító ismeretlen céget képviselő ismeretlen háttérű kártyás tranzakciók helyett.



Ám sebj. Ennyi ontópik poszt után lehet, hogy **lassan érdemes lenne egy megfelelő szimpatikus napot is kiválasztani a naptárból, hogy mikor tartsuk a hamis antivírusok elleni küzdelem világnapját.**

 4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

  0 

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2764254>

Kommentek:

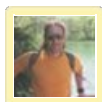
Verify 2011.03.23. 16:33:22

Sírtam ezen a stíluson. Nem kéne ennyire erőltetetten humorkodni.

cworm (törölt) 2011.03.24. 12:14:10

"vajmi köze sincs" helyesen: "vajmi köze van" :P

Hamarosan lehet, hogy minden "rendes" av szoftvert le fognak másolni, lásd avg?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.03.25. 07:13:03**

Szia Cworm!

Válaszolhatnám azt is, hogy most nemrég kezdték és még egyelőre csak a 3 és 4 betűsöknél tartanak :-)

Azért ennél sokkal jobb válasz szerintem az, hogy igyekeznek ők is minimalizálni a saját kockázataikat, és szerintem egyelőre nem fognak egy Kaspersky vagy F-Secure nevű sokkal rizikósabb cuccot felmutatni. Mert a pár betűs neveknel simán mondhatják azt, hogy milyen hamisítás? Hiszen ez nem, ez az AVG valójában, A Viziló Gereblyézik rövidítése. Mi kérem talpig becsületes emberek vagyunk. Szóval ez már része a homályzónás jogászkodásnak, ügyvédezésnek.

Lásd VVV29, mikor a hamis AV gyártó ügyvédi pofátlanul még felszólítást küld a Nodnak, per lesz, ha nem veszik ki a detektálást:

www.commodore64.hu/pdf/vvv29.pdf

Vagy a Chronopay viselt dolgai emitt:

antivirus.blog.hu/2011/03/08/a_hamis_antivirusok_ujabb_kalandjai?_ts=20110325070208

Népszerű a PDF állományokat támadni

2011.03.25. 10:00 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [magyar adatok](#) [nod32](#) [eset](#) [havi](#) [threatsense](#) [vírusstatisztika](#)

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



Kismértékű átrendeződés történt csak a mezőny második felében, míg az élboly maradt szinte változatlan. A Conficker féregről nem is ejtünk szót, amíg a "szokásos" első helyét őrzi. Ám egy vadonatúj szereplő is a porondra lépett: nevezetesen a JS/Exploit.Pdfka trójai személyében. Ez a kártevő úgy működik, hogy **a PDF állományban található JavaScript kód a dokumentum betöltésekor az Adobe Readerben automatikusan lefut és a felhasználó tudta nélkül titokban megkísérel távoli**, például hongkongi weboldalakhoz csatlakozni, ahonnan további kártékony kódokat próbál meg letölteni. Érdeemes lehet tehát jobban vigyázni a PDF kiterjesztésű állományokkal.

Összességében elmondhatjuk, a 2010-es évben a veszélyes mellékletek közül leginkább a PDF dokumentumok okozták a legtöbb fejfájást. Ezt a kétes értékű staféta botot a Microsoft szövegszerkesztői állományoktól ragadta el az Adobe még 2009-ben, amely nem csak a Flash állományok lejátszóját, de a Portable Document Format fájlok megjelenítésére alkalmas Adobe Readert is készíti.



Egy 2010-es évre vonatkozó összesítés szerint a veszélyes dokumentum fájltypusok között a PDF emelkedett ki leginkább, 61 százalékban tartalmazott valamilyen hibát kiaknázó exploitot. És csak ezt követte aztán a többi, maradékon osztozó Office fájltypus: Excel, Word, PowerPoint.

Érdeemes tehát alaposan megválogatni, kitől fogadunk el PDF dokumentumot, a felesleges, gyanús, kéretlen leveleket, levélmellékleteket pedig legjobb azonnal olvasatlanul kitörölni. Fontos ügyeknél esetleg érdemes magától a feladótól megerősítést kérni, valóban ő küldte-e azt - persze mindezt szigorúan még a megnyitás előtt. Ugyancsak **hasznos lehet gyanús esetben a VirusTotal oldalon is ellenőrizni a dokumentumot.**



Az okok között említhetjük, hogy egyfelől az Adobe elég lassan reagálva bocsát ki biztonsági frissítéseket, és az is valószínű, hogy maguk a felhasználók sem tartják mindig számítógépeiket minden alkalmazást érintően naprakészen, hiszen ez elég sziszifuszi munka. Ezenkívül PDF exploitot találni az interneten nem igazán okoz gondot a kártevőterjesztőknek, így könnyűszerrel terítik kártékony dokumentumaikat.

Megoldásképpen a JavaScriptek futtatását érdemes letiltani az Adobe Readerben, vagy akár másik megjelenítő program után is nézhetünk. Ezek az alternatívák a legtöbb esetben megfelelő minőségűek és cserébe nagyságrendekkel kevesebb támadási felületet nyújtanak.



Vírustoplista - 2011 február

Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2011 februárjában a következő 10 károkozó terjedt a legnagyobb számban, és volt együttesen felelős az összes fertőzés 20.96%-ért.



1. Win32/Conficker féreg

Elterjedtsége a februári fertőzések között: 6.07%

Előző havi helyezés: 1.

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 eljárshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárásán 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.



A számítógépre kerülés módja: 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>



2. INF/Autorun vírus

Elterjedtsége a februári fertőzések között: 3.42%

Előző havi helyezés: 2.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozónak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.



A számítógépre kerülés módja: Fertőzött adathordozókon (akár MP3-lejátszókon) terjed.

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



3. Win32/PSW.OnLineGames trójai

Elterjedtsége a februári fertőzések között: 2.23%

Előző havi helyezés: 4.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományaikat és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatokat titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



4. Win32/HackMS trójai

Elterjedtsége a februári fertőzések között: 1.69%

Előző havi helyezés: 3.

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítéskor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>



5. Win32/Tifaut trójai

Elterjedtsége a februári fertőzések között: 1.59%

Előző havi helyezés: 7.

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csrss.exe és autorun.inf néven. A kártékony EXE fájl automatikus lefutásához külön bejegyzést is készít a rendszerleíró-adatbázisban. Működése során több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21tifaut>



6. Win32/Shutdowner trójai

Elterjedtsége a februári fertőzések között: 1.47%

Előző havi helyezés: 6.

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>



7. Win32/VB féreg

Elterjedtsége a februári fertőzések között: 1.41%

Előző havi helyezés: 8.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefutásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



8. JS/Exploit.Pdfka trójai

Elterjedtsége a februári fertőzések között: 1.24%

Előző havi helyezés: -

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/exploit-pdfka-oph>



9. HTML/ScrInject trójai

Elterjedtsége a februári fertőzések között: 0.95%

Előző havi helyezés: 5.

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



10. Win32/RegistryBooster trójai

Elterjedtsége a februári fertőzések között: 0.89%

Előző havi helyezés: 10.

Működés: A Win32/RegistryBooster alkalmazás a hamis antivírus programokhoz hasonlóan hamis riasztásokkal igyekszik rábeszélni a felhasználókat a „program” fizetős változatának megvásárlására.



A számítógépre kerülés módja: Fertőzött weboldalról települ, vagy a felhasználó maga telepíti.

Bővebb információ:

<http://www.eset.hu/tamogatas/viruslabor/virusleirasok/registrybooster>



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



0



Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2767391>

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](#).

evat 2011.03.26. 03:08:27

Tudom, tudom.... Hülye vagyok, hogy megnyitottam egy felettébb gyanus levél pdfjét, de ha ilyen hülye vagyok, kénék egy kis segítséget, hogy hogyan hozhatnám helyre a hibámat?! Amúgy nod32m van és nem jelzett semmit!!!!Köszönöm



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2011.03.28. 11:53:29

Szia Evat!

Itt keress egy szimpatikus (cim, telefon, email, fax) eleresi modot - szerintem az email a legjobb, - es kuldj el minel reszletesebb infot, kepernyokepet, sysinspector logot, pontosan milyen weblapon, milyen fajlnal mit irt ki micsoda es segiteni fognak.
www.eset.hu/tamogatas/kapcsolat

Így szerezd az öszvéredet

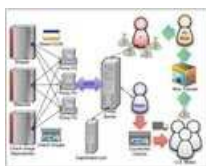
2011.03.28. 17:15 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [csalás](#) [pénzmosás](#) [álláshirdetés](#) [öszvér](#) [mule](#)

Bár a kezdőképen a régmúlt kellemes C64-es emléképeivel nyitunk, maga a téma azonban már nem lesz ennyire vicces, különösen, ha a munkanélküliek és munkát keresők jelentős számát tekintjük. Hova nem érdemes jelentkezni, az tüstént kiderül.



Hogy kik és honnan küldik a kéretlen álláshirdetéseket, azt már abban a korábbi jó kis posztunkban szabatosan leírtuk, [melyben az online bűnözés elképesztő mértékű erősödéséről szoltunk](#). Aki esetleg még nem olvasta volna, annak beidézzük a mostani írásunk pontosabb megértéséhez szükséges fölényeget:



*"Régebben, ha a kábítószerfutárok elvesztették az árut, bankot raboltak, hogy megtérítsék a kárt a főnökeik felé. **Ma már tudnak egyszerűbb, és lebukásmentesebb verziót: inkább bérlik vagy megvásárolják egy ukrán szerző kártékony programját, és ezek segítségével csapolják meg tömegesen hétköznapi felhasználók, vagy cégek számláit. A hamis álláshirdetéssel toborzott balekok (mule) pedig egy kevés jutalékért elvégzik a piszkos munkát, vagyis átutalják a pénzt a lopott számlákról a bűnözőknek. Ha nagy ritkán el is kapnak az öszvérek közül valakit, az semmit sem fog tudni a szervezet nagy egészéről.**"*



Ezek után nézzük az utóbbi pár nap friss termését a postafiókban. A leveleket nagy meglepetésünkre **látszólag mi magunk írtuk saját magunknak**, ám hogy az áhított munkaerőre milyen nagy szükség lehet, azt jól mutatja, **hogy annak beszerzését nem a HR osztály végzi a szokott módon, hanem kiadták azt a dolgozóknak gebinbe**. Kapunk ajánlatot a szabvány domainről Herscheltől, Perrytől, Kerrytől, sőt Dominiquetől is, Helenről nem is beszélve.



Sajnos [az ilyen levelek nem kecsegtetnek valódi állással](#), hanem vagy címgyűjtő csalások, vagy pedig a már [említett lopott bankkártya pénzek tisztára mosásában veszünk részt](#). Ha mégis alkalmaznának, a börtönbe is kerülhetünk a végén. Érdemi ajánlatokat ezért sokkal inkább az erre szakosodott jelentősebb [állásközvetítő oldalaknál érdemes keresni](#), akik biztosan nem ilyen kétes, törvénybeütköző munkákra toboroznak.



Hogy aztán ezen felül a magyarországi munkaerőhelyzetnek vajon mi használhatna még, annak eldöntése nem a mi asztalunk, de **pár remek ügyviteltechnikai ötletünk azért állampolgári jogon kikönyököl itt az asztal sarkán a valódi hirdetőknak is, amit a téma kapcsán nem tudunk visszatartani:**

- az álláshirdetések ne csak idegen nyelven, hanem ezzel párhuzamosan magyarul is kötelezően mindig jelenjenek meg. ha már egy itteni cégalapításkor csak magyar hangzású lehet az új név, egyébként is magyar a hivatalos nyelv, akkor simán beleférne ez is, a nyelvtudást majd úgyis letesztelik a cv-ben, meg az interjún is

- mivel a munkavállalók amúgy is szerfelett kiszolgáltatott helyzetben vannak, minden hirdetőnek legyen kötelező a munkakörhöz tartozó

nettó munkabér megjelölése is a hirdetésben a szokásos "fizetési igényének megjelölésével jelentkezzen" szófordulat helyett

- minden hirdető garantálja, hogy maximum 60 napon belül/60 naponként írásban visszajelez: felvettük, elutasítottuk, a hetvenharmadik kör várható hazugságvizsgáló műszerrel, vizeletmintával és önkéntes DNS teszttel - mondjuk legyen ez ingyenes email útján. fekete lyukba levelezni válaszok nélkül uncsi, modortalan és lélekromboló

Bármelyik elmulasztása esetén elsőre mondjuk lenne 1, másodikra 10, harmadikra 100 miller - tetszőleges alkalommal újra kiszabhatóan. **Na de most már térjünk is vissza a fantázia világából a saját technikai jellegű vizeinkre. Ha utána akarunk nézni - és minden esetben akarjunk is :) - pontosan ki áll a hirdetés mögött, a cégnevet, a feladó nevét, a levél tárgysorát lehet megguglizni, és ott nyugtalanító jeleket lehet keresgélgni.**



Vannak ilyen speciális [weboldalak is, ahol a hasonló szemetelöket, csalókat gyűjtik](#) szép csokorba. Ha pedig megpróbálunk levonni valamiféle gyakorlatban is jól hasznosítható amolyan Dr Bubó féle összesített univerzális záróokosságot, az valami ilyesmi lehetne:



"Ursula, kérem jegyezze fel: sose jelentkezünk olyan álláshirdetésre, amely [kéretlen emailben érkezett](#) és/vagy a levél feladója vezeti a Google találati tükrében az aktuális havi sztahanovista [spamkibocsátó versenyt](#)".

Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2778391>

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.

Reklámzabálók nappala

2011.03.30. 16:10 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [hirdetés](#) [banner](#) [antivirus](#) [exploit](#) [fertőző](#) [rogue](#) [spotify](#) [blackhole](#)

Ezúttal a Spotify zeneszolgáltatást felkeresők gépeit támadták a weboldalon megjelenő kártékony kódot tartalmazó hirdetések.



Már korábban is beszámoltunk fertőző hirdetésekkel kapcsolatos incidensekről, talán a legemlékezetesebb a [2007-es NHL League](#), és a [tavalyi DoubleClick-es](#) eset volt. Most a Spotify "volt soron", és itt még magára a reklámra kattintani sem volt szükséges ahhoz, hogy a különféle trójaiak települjenek.



A blogunk törzsolvasói már bizonyára meg sem lepődnek, hogy ezúttal is szerepel **egy hamis antivirus program, a Windows Recovery** nevű [megtévesztő és pénzt követelő alkalmazás települt fel](#) azoknak a számítógépére, akik nem frissítették rendszereiket idejében, illetve nem rendelkeztek naprakész vírusvédelemmel.



[A Websense szakértői szerint](#) az első támadást 2011. március 24-én 11:30-kor észlelték, arról a megfertőzött látogatók is folyamatosan beszámoltak fórumokban, Twitter bejegyzéseikben. Az utólagos elemzés szerint az ismeretlen elkövetők egy **Blackhole Exploit Kit** nevű készletet használtak a támadáshoz.



A Spotify azóta már elnézést kért, és mostanra minden káros kódot eltávolítottak már. Egyfelől azonban jól látszik, a reklámszolgáltatásban - különösen ha az szerteágazó alszolgáltatókra, ügynökségekre oszlik, egyre inkább egy nehezen ellenőrizhető, [egyre gyakrabban kihasznált gyengepont](#), illetve **módszer lett, amibe bárki beleütközhet netezéskor**.



Másfelől viszont megint adhatunk egy piros pontot az ilyenek ellen [kellemesen megvédő NoScriptnek](#), amit valljuk be: ha nem lenne, ki kéne találni.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászával](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Elégedetlenség vagyunk a Facebook biztonságával](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2784575

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.

Egyszerűsödtek a Facebook biztonsági beállítások

2011.04.01. 12:25 | [Csizmazia István \[Rambo\]](#) | [4 komment](#)

Címkék: [móka](#) [április elseje](#)

Úgy tűnik, végül mégis megérhettük, hogy **egyszerű, átlátható felületen, mindenki által érthető módon történjen a biztonság beállítása**. A korábbi, számos menüponton, és aloldalon áthúzódozó, félszázal is több opció helyett ezentúl az úgynevezett Easy Secure Settings segít a hatékony védelmi beállításokban.



Vagyis a biztonsági beállítások korábbi dzsungel helyett **immár egyetlen helyen egy szimpla Facebook Security ON és Facebook Security OFF között kell csupán választanunk**. Érdekesség, hogy az **ON állásban a rendszer letiltja minden korábbi botlásról, félrelépésről, részegeskedésről szóló üzenet, fotó megjelenítését abban az esetben, ha bármilyen leendő munkaadó, valóperes ügyvéd vagy bulvárújságíró szeretne ilyen témában rólunk tájékozódni**. Vagyis ezzel lehet mégis elkerülni azt a kényelmetlen helyzetet, amire **korábban azt gondoltuk, nincs rá megoldás**, mert ami felkerül az internetre, az örökre ott is marad.



Ez volt a korábbi helyzet. Ember legyen a talpán, aki ezek közt kiigazodik

További jó hír, sőt talán ez az összes közül a legnagyobb volumenű változás, hogy **a korábbi opt-out (mindent megosztok, amit le nem tiltok) helyett a jövőben az opt-in módon lesz beállítva minden felhasználó alapértelmezett megosztása, azaz csak azt osztjuk meg, amit a könnyen kezelhető és világos felületen engedélyeztünk**, és ezen kívül semmi mást. Ezt a kedvező elmozdulást - [melyet többek közt Graham Cluley is javasolt korábban](#) - az egész **antivírus szakma, valamint az IT biztonsági cégek is egyöntetűen kedvezően fogadták**, és üdvözölték.



Mostantól egy mozdulattal beállíthatjuk a biztonságos működést

Ezzel egyidőben szintén megoldódni látszik az utóbbi idők egyik legsúlyosabb, vagyis **a kártékony linkek és applikációk problémája is**. A jövőben ugyanis már nem fordulhat elő olyan eset, mint például az emlékeztetés **"Az emberek 98%-a nem tudja 17 másodpercnél továbbnézni ezt a vidót" típusú** csalásnál. Ehhez a korábban különféle **biztonsági audit, és antivírus cégeknek is fejlesztő LirpaSoft cég készített el egy 100%-os hatékonyságú szűrőt**, amely végül úgy kerülhetett a Facebook eszköztárába, hogy az eredetileg Hutt River Provinceben működő céget teljes egészében felvásárolták. A korábbi CEO, aki jelenleg a Facebook biztonsági osztály egyik **vezető szakmérnöke**, a koreai Loo Flir Pa szerint ezáltal **kizárt, hogy a jövőben kártékony linkeket lehessen küldeni becsapós üzenetekben**.



Valódi 100%-os hatékonysággal szűr az új védelmi kód

Emellett nem várt területeken is változások történtek, ugyanis Mark Zuckerberg azt is megígérte, hogy **ezentúl megelégszik azzal a profittal, amit a rendszer legálisan termel, és a jövőben soha többé nem adja el titokban a hirdetőknak a felhasználók személyes adatait**, a rendszeren belüli hálózati, kapcsolati és viselkedési információit.



Jócskán növelhetik a cégvezér népszerűségét a frissen bejelentett kedvező intézkedések

Meg nem erősített és nem hivatalos információk szerint egy **"Beast"** becenevű magyar származású barátja bírta végül rá arra, hogy korábbi nem túl korrekt bevételszerző gyakorlaton túllépve, valamint a kissé túlbonyolított biztonsági beállításokat sutba dobva **ebbe a várva várt, tisztább üzletmenetet és erőteljesebb biztonságot ígérő irányban tegyen végre határozott és konkrét lépéseket.**



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2789614>

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](#).



[atko 2011.04.01. 17:07:53](#)

Ez most az április 1. vagy esetleg elgurult a gyógyszere a arckönyembernek? :-)

Egyébként jót mulattam az íráson. ;-)



[atko 2011.04.01. 17:09:39](#)

Álomnak viszont szép volt!



[Vektorigo • http://iranylondonblog.hu 2011.04.02. 00:46:35](#)

kiváncsi leszek...





Csizmazia István [Rambo] • <http://antivirus.blog.hu>

2011.04.02. 09:37:42

Üdv mindenkinek!

Sajnálom hogy csalódást okozok, de úgy tűnik, maradnak a korábbi biztonsági beállítások, és az adataink eladása sem szűnik meg majd nagy valószínűséggel. Azért igyekeztem jó érzékkel vegyíteni a vágy villamosát a rögválóság morzsáival, és konkrét linkjeivel remélve, hátha lesz aki azt mondja majd: kavarja ez most vagy nem kavarja, vagy csak annyit: nice try :-)

Gyanakodni azért jócskán lehetett, legyen az a megelégszik a kevesebb profittal is (muhaha) vagy a 100%-os hatékonyságú szűrés a hozzá való Hello World kóddal is egy intő jel volt. Gondoltam, azért akad majd, aki visszafelé is elolvassa a koreai tudós vagy a szoftverfejlesztő cég nevét. A Beast egyébként Zucker mester pulikutyája, itt a végére már keményen tombolt az féktelen agymenés :-)

Nem várható a kártevők számának csökkenése

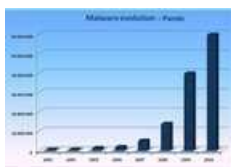
2011.04.04. 14:45 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [malware száma kártevők egyre kit olcsóbb emelkedik](#)

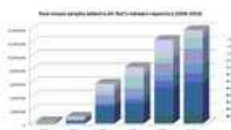
Nem tudni, akad-e egyáltalán valaki, aki éppen erre akart volna fogadni jelentős összegben, de biztosan kimondhatjuk: nem érdemes. Áttekintünk néhány számot, okot, trendet, hogy megtudjuk: miért, hogyan és egyáltalán.



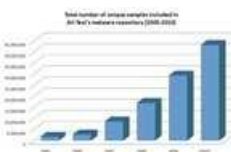
Annak idején talán a [Stockholmi Békekutató Intézet](#) egyik jelentéséből vált világhíressé, mi is volt az úgynevezett hidegháború egyik legfőbb célja. A másik fél gazdasági eszközökkel való térdre kényszerítése. Ugyanis míg az USA-nak a felfegyverkezés (amit meg aztán évekkel utána jól megsemmisítettek) a saját GDP-jének csupán - most csak hasból következnek körülbelüli számok - öt százaléka volt, addig a Szovjetunió megizzadt és erőforrásainak jó 30-40 százalékát is rákényszerült elkölteni, hogy tarthassa a lépést.



Az IBM kompatibilis PC-k hajnalán is volt egy olyan idilli időszak, amikor a programozók legfőbb gondja kizárólag még az lehetett, mennyi tizedesre kerekítsenek, lehet-e logaritmussal egyszerűsíteni az egyenlet két oldalát ;-) vagy hogy az Epson FX-1000-esen szépen tagolt legyen a nyomtatási kép, amit előtte jól fájlba küldtek, hogy a begyűrt leprello esetén könnyen újra lehessen printelni a hiányzó oldalt.



Ma már az erőfeszítések legalább 30-40 százalékát - ha nem még ennél is többet - a biztonsági kérdések veszik el, akár akarjuk, akár nem. Programozáskor hiába jön ki jó eredmény, ha közben kihasználható hibáktól hemzseg az alkalmazás. Üzemeltetéskor hiába működik látszólag minden, ha adatot szívárogtat weboldal, kompromittálható az adatbázis vagy zombiként bedolgoznak valami ismeretlen helyre a kliensek. [A kártevők száma elképesztő mértékben meredeken emelkedik](#), a variánsok száma az egekig nő. Ha csak a Moore törvény szerint történne mindez, még akár örülhetnénk is.



A vírusirtók fejlesztői folyamatosan küzdenek a memória méret, a keresési sebesség, a szignatúra állományok méretének ésszerű, kezelhető határok között tartása miatt, és mindenhol a generikus felismerés, valamint a heurisztika irányába tolják a szekerüket. Eközben a kártevő terjesztés lassan bárki számára elérhető közelségbe került.



Korábban csak bennfentesek, bűnözők által ismert, eldugott chatszobákban viszonylag jelentősebb - pár ezer dolláros, de persze megtérülő - összegért lehetett olyan kitekhez, készletekhez hozzájutni, amelynek segítségével érdemi számítógépes tudás hiányában is lehetett iparszerűen "dolgozni" és "pénzt keresni", mostanra már teljesen nyíltan zajlik mindez, és [ezen a fekete piacon is óriási árcsökkenés tapasztalható](#) a Trend Micro nyegyedéves jelentése szerint.



Biztos, hogy a válság is jelentősen hozzájárult ehhez, de nyilván [ezen a piacon is dúlnak](#) harcok. [Pár éve még ritkaságszámba ment, hogy a kártevő terjesztő készlet forráskódját közzétegyék az interneten.](#) Ám később már - [ahogy nálunk az őrző-védő cégek tagjai színleg belépnek a konkurenciához](#), és próbálják ily módon leleplezni az esetleges adózási szabálytalanságokat, feljelenteni a másikat - [a kártevő készletek fejlesztői is gyakran ellopkodják egymástól a forráskódokat](#), tovább értékesítik azt olcsóbban, így letörve az árakat küzdenek egymás ellen.



Mindez a felhasználók szempontjából azt jelenti, **nem szabad alábecsülni a védekezés fontosságát, és ebben a folyamatos képzés is igen lényeges.** Hiába fut korrekten a vírusirtó, [ha közben valaki bedől a social engineering trükkökhöz](#), és önként kattint, továbbküld, telepít, számlaszámot ad meg. Csak a megfelelően kiválasztott biztonsági program és a biztonságtudatos hozzáállás **együtt tudja megadni az elvárt eredményt.** [Kételkedem, tehát vagyok.](#)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

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](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2798098>

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.

Hát ha csak úgy nem

2011.04.06. 13:45 | [Csizmazia István \[Rambo\]](#) | 24 komment

Címkék: [felmérés](#) [riasztás](#) [nrc](#) [kikapcsolás](#) [virusirtó](#)

Hogyan mennek bele a számítógépbe a micimackók? - ez a kínzó kérdés motoszkálhat a fejünkben, amikor az NRC által végzett kutatás eredményeit olvasgatjuk. Az Eset megbízásából történt felmérés arra kereste a választ, **hogyan viselkedünk, ha riaszt a vírusirtó**. Riasztó adatok jönnek.



A 2011. februárjában végzett piackutatás **a magyar internetezők viselkedését vizsgálta** online kérdőíves felmérés segítségével, ahol a minta reprezentatív a 18-69 év közötti, legalább heti rendszerességgel internetezőkre nem, korcsoport, végzettség és lakóhelytípus szerint. A kutatás eredményeiből kiolvasható, hogy **a magyar internetezők egynegyede a vírusirtó szoftverének riasztása ellenére is végignéz egy fertőzött weboldalt, ha annak tartalma érdekli.**



A férfiak 15%-a ezenkívül ki is kapcsolja vírusirtóját, hogy **el tudjon indítani egy fájlt, amit a biztonsági szoftver fertőzöttnek jelzett**, míg a nőknek 6%-a tesz így. Különösen veszélyeztetettek a fiatalok. A 18-29 évesek **17%-a szokta kikapcsolni a vírusirtóját azért, hogy fertőzött fájlokat tudjon elindítani**, 12%-uk pedig azért, hogy fertőzött weboldalakat látogathasson.



"A vírusok készítői kihasználják az emberi kíváncsiságot és a monitor előtt ülő felhasználók téves biztonságérzetét. A felmérésünkéből az is kiderült, hogy a legnagyobb veszélynek pont a tapasztaltabb internetezők vannak kitéve. Ők azok, akik tévesen azt gondolják, hogy könnyedén tudják kezelni a veszélyeket, és azt is megengedhetik maguknak, hogy fertőzött weboldalakat látogassanak, vagy **kikapcsolják a vírusirtót annak érdekében, hogy meg tudjanak nyitni egy fertőzött fájlt**" - nyilatkozta minderről Kiss Zoltán Gergő, aki szerint **a megfelelő számítógépes védelem alkalmazása mellett a felhasználóknak a felelősségteljes internet használatra is törekednie kellene.**



A vírusirtó program jelzéseinek figyelmen kívül hagyása, vagy a biztonsági szoftver kikapcsolása jellemzőbb a férfiakra és a fiatalabb korosztályra (18-29 évesek), míg a legóvatosabb a legidősebb korcsoport (50-69 évesek). **"Egyetlen biztonsági szoftver sem védheti meg a felhasználókat, ha nem foglalkoznak annak riasztásaival"** - ezt lehetne kiemelni legfőbb tanulásként az egészből.



Bár a helyzet korántsem rózsás, semmiképpen nem sommásan elítélni kell azt, aki rosszul áll hozzá, hanem érdemes inkább megszívlelni a tanulságokat és a jövőben átértékelni, másképp csinálni. Ez csak **egy újabb, az élethosszig tanulásról szóló tégl a falban**.

 3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

f Megosztás



Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2803994>

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 2011.04.07. 09:52:17

Majd ha nem adnak totál kamu riasztásokat a vírusirtók, akkor talán nem fogom kikapcsolgatni. Ameddig legalább valamiféle sandbox módot nem találnak ki a károsnak minősített weboldalak előnézetéhez, hogy eldönthessem én a dolgot, addig azt is ki fogom kapcsolgatni.

Persze én Kaspersky-t használok, de más gépeken rendszeresen deaktiválgatom a sok hulladék vírusirtót, ami mindenre amit "nem ért" pofázik, de legtöbb esetben kérdezés nélkül töröl.

Mert például Igen Bmeg újratelepítés előtt vissza akarom fejteni a messenger/dialup/skype/akármilyen jelszót, mert a kedves tulaj már rég elfelejtette, értem, hogy sok ilyen program a "nem szép dolog" kategóriába esik egy vírusirtó szemében, de akkor is nyasgem az összes lusta tolvaj cégnek.

A kaspersky szerint miért nem vírusos? Talán mert ők utánanézték, mielőtt kamuriasztásokkal fárasztanák a kedves jüzert?

különvélemény 2011.04.07. 09:56:53

Persze a Kaspersky-nél is volt olyan, hogy talán egy keygen (tudom nem szép dolog) már nem emlékszem, rögtön került a karanténba, de 1-2 nappal később már szövegelt is, hogy az mégsem vírusos, kiszedjük onnan?

különvélemény 2011.04.07. 10:10:05

Természetesen aki nem ért ezekhez a dolgokhoz, az inkább hagyja bekapcsolva a vírusirtóját, vagy futtassa a dolgot www.sandboxie.com/-val, mert a kikapcsolás a lehető legrosszabb megoldás.

fidesz = házmesterek pártja 2011.04.07. 10:43:53

Hogyan viselkedjen a felhasználó, ha AVG9-t használ, lefuttatja az update-et, majd restart utána Spybot S&D közli, hogy valami baci van az AVGTray.exe-ben?

Csak ott, sehol máshol... de ott következetesen.

Spybotnak hagyom, hogy csináljon vele amit akar, AVG9 uninstall, reboot, újabb keresgélés, másik víruskereső telepítés, ellenőrzés azzal is, online keresőkkel is, sehol semmi...

Ilyenkor vajon mi van? Mondjuk az AVG-t már régóta utáltam az erőszakos önreklámja miatt, de akkor is...

aha, persze 2011.04.07. 10:59:40

Off:

OSX

On.

Dandie 2011.04.07. 11:14:29

[@aha, persze](#): miért írnának osx-re vírust? Mibe találsz több halat, egy pocsolóban vagy egy tengerben?

De tod mit?

Off:

Kenyérpíró

On.

[aha, persze 2011.04.07. 11:17:45](#)

[@Dandie](#): Miért ne?

Tudod mit?

Javaslom neked: Logika: ON.

(értsd: nem volt épp logikus az érvelésed - már ha ezt nevezhetjük annak. Mindegy is, szarozzatok csak a vírusírtóval, PC-n éveken át használtam olyan kis alkalmazást, aminek köszönhetően sose volt vírusom.)

[Dandie 2011.04.07. 11:21:56](#)

[@aha, persze](#): Hát oké, most jól megkaptuk - mi gonosz PC felhasználók -, lassan a logikai érzékem is kifejlődik, csak még vezess mester. Az nem derült ki, hol dobott kivételt az érvelésem, de ha megosztod velem, több ezer embernek adom át az ígét!

[aha, persze 2011.04.07. 11:25:09](#)

[@Dandie](#): Ugyan már, én nem az összes PC felhasználóról beszéltem, csak rólad. Te nem érvelsz, csak vagdalkozol.

(Meg, nem is akarok vitába szállni, ezért írtam OFF-ként, amit írtam.)

[Dandie 2011.04.07. 11:29:20](#)

[@aha, persze](#): Na de tényleg, már annyira kíváncsi vagyok, hol siklik ki az érvelésem?

[aha, persze 2011.04.07. 11:30:37](#)

[@Dandie](#):

Mondom: nem érvelsz. Mit nem értesz ezen?

Hagyjuk már az egészséget... Minden jól.

[Dandie 2011.04.07. 11:36:51](#)

[@aha, persze](#): : DDDDD

[Dandie 2011.04.07. 11:37:54](#)

[@aha, persze](#): "nem volt épp logikus az érvelésed" vs "Mondom: nem érvelsz."

Respect, peace!

(sorry a dupláért, hirtelen felindulás)



[nitro1 2011.04.07. 12:14:34](#)

[@Dandie](#): Ha tovább olvasnád, rájönnél:

"(értsd: nem volt épp logikus az érvelésed - már ha ezt nevezhetjük annak...)"

Egyébként veled értek egyet. :-)



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.04.07. 13:15:28**

Sziasztok!

Húha, ennyi kommentre őszintén szólva nem számítottam :-O

Az említett Sandboxiet ismerem, és én is jó ötletnek tartom a használatát. Emellett pedig aki tudja mit csinál, és maximálisan tisztában van a dolgokkal, az bátran kísérletezhet. Én is kikapcsolok mindent, ha épp Windowson akarok elcsípni, elemezni valami kártevőt, ilyenkor a kikapcsolás miatt nem érzem magam "idótának".

Még egy gondolat a keygen témához. Nehéz alapos analízálás (virustotal, debug, process monitor, process explorer) nélkül kimondani egy kulcsgenerátorról, hogy az most ok nélkül felkoppan pusztán a használt gyanús technika miatt a heurisztikán, adatbázison, vagy pedig tényleg van benne valami trükkös és káros dolog. Ezt minden egyes esetben ellenőrizni kell, addig nem mondhatjuk pavlovi reflexből, hogy ó ez csak egy szimpla keygen, csak megmosom a hajam, kikapcsolom a vírusirtót, és már indulok is.

Szóval úgy vélem, ezek a felismerések az ilyen helyzetek kerülése az átlagfelhasználói többségre vonatkoznak, és ez jól is van így.

különvélemény 2011.04.07. 14:11:26

[@Csizmazia István \[Rambo\]:](#)

Keygen téma:

Igazad van, és bocs, tudom NOD-os vagy (azzal nem nagyon volt eddig tapasztalatom), de arra van a heurisztikus/akármilyen ellenőrzés, és van olyan keygen, amit a Kasp. 20 sec alatt nyit meg, kikapcsolva azonnal indul, na az megnézi rendesen a dolgot.

De az, hogy a legtöbb keygenre, ami agyon van tömörítve/titkosítva, mivel nem szeretnék, ha visszafejtenéd, rögtön kiírja a legtöbb av, hogy "generic trojan", na az egy hatalmas BULLSHIT.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.04.07. 19:55:08**

Szia Különvélemény :-)

Ezzel a Kalap uras "a tömörített rossz, mert a tömített rossz, értem" dologgal messzemenően egyetértek. Lásd itt a calc.exe tömörítésére kapott mukinyulas fals riasztásokat:

pcworld.hu/a-virusok-varazslatos-vilaga-1-totalis-ellenorzes-20070831.html?p=2

De azt azért tudni kell, vannak kifejezetten olyan tömörítők is, amelyek polimorf kódja minden antidebug technikát tartalmaz, és jelenléte hagyományos, jóindulatú kereskedelmi forgalomban lévő termékek szinte sosem fordul elő, például Morphine packer, Armadillo, Yoda packer, meg hasonló. Ahol ha nem is riasztás kell, de egy warning kiköpése szerintem segítő információ, hogy hoho érdemes figyelni.

különvélemény 2011.04.08. 08:52:08

[@Csizmazia István \[Rambo\]:](#)

Igen, de mennyivel korrektebb lenne, ha ezt írná ki az av, felajánlva választási lehetőséget.

Ahelyett, hogy kamu riasztással letörli, csökkentve ezzel a bizalmat a felhasználóban az av szoftverek iránt.

Mi is történik?

Felmegy a jüzer pl. a piratebayre, látja a kommentekben folyamatosan, hogy nem vírusos, csak kamuzik a vírusirtó.

Elhiszi, felrakja, nem lett vírusos.

Így a következő warezolásánál már nem is nézi, hogy "generic trojan", vagy konkrét kórokozó, reflexből kapcsolja ki, mert megszokta, hogy az általa használt av kamuzik a warezzal kapcsolatban.

És szépen beszívja a legújabb vírust.

Ez kinek a felelőssége vajon?

Az átlagjüzernek, aki kikapcsolta az av-t, vagy az av gyártóknak, akik elaltatták a gyanúját a sok kamuriasztással?

különvélemény 2011.04.08. 09:04:57

Azt hagyjuk, hogy a warezolás jó, vagy sem, maradjunk annyiban, hogy szükséges.

Nélküle a kis szoftvercégeknek semmi esélyük nem lenne, de win7-et sem vett volna senki egy Vista után, ha nem tudja kipróbálni, amire a 14 nap édeskevése egy oprendszernél.

A legjobb szoftverdisztribúciós csatorna a világon, a warez scene.

Oda kell bejutni, ha benne vagy a 0-day-ben, akkor sokan ki fogják próbálni a programodat, és ha tetszik, sokan meg is veszik.

Ha én egy kis szoftvergyártó lennék, új termékkel, azzal kezdeném, hogy keygen algoritmust mellékelve elküldeném az egyik nagy groupnak, tolják már fel légy-szi saját nevük alatt a cuccot.

fidesz = házmesterek pártja 2011.04.08. 09:26:41

@különvélemény: na ne csináld már! Egy otthoni felhasználónak nem elég 14 nap??? Ez még viccnek is rossz. Vállalkozásnak meg... általában a szoftvercégekkel lehet tárgyalni, hogy biztosítsanak több időt a tesztelésre, ha valami komolyabb rendszerről van szó. Az meg egyenesen röhejes, hogy egy akármilyen kisvállalkozásnak ne legyen 30-40000Ft-ja gépenként egy windows-ra, ha ennyire ragaszkodnak a M\$ világához... (nem Ultimate Editiont kell venni, oszt jónapot!)

fidesz = házmesterek pártja 2011.04.08. 09:27:47

Bocs, hülyeséget írtam az előbb: Win7 Prof. OEM ha jól emlékszem, 25000 körül kapható...

különvélemény 2011.04.08. 10:01:56

@Álamfő álmás következik:

Oprendszere? Na te ne csináld már! :)

Mit gondolsz, mi a roszabért 180 napos a win2k8 r2 server evalja?

Pedig azt szakemberek tesztelik.

Egy laikus azt sem tudja mit teszteljen, egyszerűen csak használja és használat közben derülnek ki a dolgok.

Senki nem mondta, hogy egy cégnek nincs pénze egy windowsra, ne gyere ezzel a tucat faxszággal, nem ez a téma, ha nincs érved, maradj csendben.

fidesz = házmesterek pártja 2011.04.08. 10:21:49

@különvélemény: okos vagy, leülhecc!

Persze: a windows szerverre azért van hosszú tesztidő, mert olyan szar... még véletlenül sem azért, mert céges környezetben lényegesen aprólékosabb tesztekre van szükség, mint egy otthoni felhasználó esetében, ááááá...

Na jó, hagyjuk egymást békén! Itt is megy az ideológia gyártás, hogy miért szabad lopni a windows-t...

különvélemény 2011.04.08. 10:53:26

@Álamfő álmás következik:

Azt sem írtam, hogy szar, megint csak oda jutunk, hogy érvek nélkül inkább hallgass.

Azért van hosszú, hogy ezzel is elnyerjék a cégek bizalmát, legyen idő bőven tesztelni, ne foglaljon le külön munkaerőt, stb.

De ez már totál off.

"Itt is megy az ideológia gyártás, hogy miért szabad lopni a windows-t"

Ilyet senki sem írt, csak te a warez szót meglátva rögtön átmész keresztes lovagba, 1 bites aggyal, ami csak a feketét és a fehéret ismeri, nehéz ezt megérteni, elismerem.

Bill Gates is elismerte már nem egyszer, hogy warez nélkül nem ott tartana a windows ismertségben, mint most, de nyilván ő is egy idióta és arra buzdít, hogy lopjunk.

Ha továbbra is arra építed az érvelésed, hogy olyanokat cáfolsz/fikázol, amit én nem írtam, akkor inkább ne válaszolj.

DHL csomagunk érkezett

2011.04.08. 13:55 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [email csalás](#) [futárszolgálat](#) [trójai](#) [dhl](#)

Vízszintes három betű, és közben futárszolgálat küldött nekünk egy **emailt: megérkezett végre valahára a várva várt csomagunk**. Hurrá, illetve álljunk csak meg egy röpké pillanatra, hoppáré, hiszen mi nem is várunk senkitől semmit.



[Nehogy a korábbi UPS sztori](#), és a [legutóbbi Fedex incidens](#) után a DHL is ne kapjon az Úr színe előtt, a **kártevő terjesztők ezúttal őket pécézték ki**. Az alábbi angol nyelvű levélkét kaptuk unsolicited magyar címünkre:



"Tisztelt Ügyfelünk!

Egy csomagot küldtek az otthoni címére, melyet 10 munkanapon belül kézbesítünk Önnek.

További részletes információt és a nyomon követéshez szükséges azonosítószámot csatolva küldjük a mellékelt dokumentumban."

A melléklet pedig egy DHL.ZIP nevű fájl, ami valódi ZIP, benne egy csatolt "document private.exe" nevű tálrggyal. Zippel, vagy zip nélkül is jól látszik, egy jólfejlett Win32/Injector.FOZ nevű [egzotikus állatfajta röfög a belsejében](#).



Csak a kontraszt kedvéért egy futárszolgálattal kapcsolatos valódi, életszerű email. Nem egy semmit mondó levél, hanem **már a levéltestben jól láthatóan szerepel az azonosító**. Továbbá **a tárgysorban is ott szerepel már egy azonosítószám**, ez is inkább így szokott lenni. Ahol viszont [csak és kizárólag a mellékletből derül ki minden](#) hón áhított részlet, az már egy **komoly intő jel**.



Persze, **érdeemes ezeket a futáros leveleket _IS_ óvatosabban kezelni**, de igazából ez csak egy ürügy, egy apropó arra, hogy a *.* többi kéretlen üzenetnek, hasonló trükknek se dőlünk be a jövőben, jöjjön az látszólag akárhonnán.



20 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



0



Ajánlott bejegyzések:

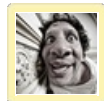
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Ez történik a weben egy perc alatt](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2809318>

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](#).



pazzo • <http://pazzo.hu> **2011.04.10. 16:41:42**

Én is megkaptam a "DHL"-től ezt a levelet, de ott lett gyanús a dolog, hogy FedEx.exe volt a zip-es tartalomban. ÷)

SMS küldős hamis antivírus

2011.04.11. 14:10 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [sms](#) [csalás](#) [hamis](#) [antivírus](#) [avast](#)

Durvul a helyzet az álantivírus fronton, egyre **újabb piszkos trükkök kerülnek bevetésre**, és sajnos már egyre gyakrabban sározzák be valódi vírusirtó cégek renoméját. Márkanévét kegyelettel lejáratjuk part III.



Az [ismert és elismert nevekkel való visszaélés](#), trükközés nem most kezdődött, már több ízben volt terítéken, legutóbb példának okáért [az úgynevezett "E-set Antivirus 2011" nevű program](#) szolgáltatta az apropót ehhez. Ezúttal az Avast! hírneve kerül néminemű rongálásra egy kártékony kódokat terjesztő érdekes weboldal kapcsán, ám az **alkalmazott furmányos technika merőben újszerű és vélhetően sajnos divatba fog jönni.**



From The, From The: megugrott a tű a lemezen, illetve visszhangzik a kopipaszta...

[Nem kell Sherlock Holmesnak lenni ahhoz](#), hogy az illető weboldalon ab ovo feltűnjenek bizonyos dolgok és [ezekből hadrafogható következtéseket tudjunk](#) levonni. Első lehet a **név egyezés (hasonlóság) ellenére észlelhető logo különbség** az eredetihez képest. Bár ezek inkább csak a biztonságos azonosításhoz szükséges apró nüanszok, ezek adják aztán a megnyugvás összképét vagy keltik fel bennünk a gyanút. Mindjárt ilyen egy weboldal favicon.ico ikonja, amelyik a böngésző sorban - mint egy megbízható ismerős - erősíti az érzést: a helyes weboldalon járunk. **Nem azonos az eredetivel, de azért ha egymás mellé tesszük, látszik rajta, kétségkívül sokat reszelgettek rajta, hogy erősen hasonlítson.**



Egy másik a **megnyugvást sugárzó 24/7 technikai támogatás felirat**, ám a **kapcsolat szövegre kattintva mindössze egy info@ emailcím bukkan elő**. Amelyik cégnek nincs publikus telephelye, címe, telefonszáma, az hiába ír ki 25/8, 35/9 és hasonló **elmésségeket**, valójában vagy el akar bűjni a megkeresések elől, vagy takargatnivalója van. Ha saját házuk táján söprögetünk, [íme ott mindez így néz](#) ki, és [itt a hazai is](#), de a többi valódi versenytársé is hasonló, csak úgy próbaképpen most reggel a McAfee lapját csekkoltuk ehhez.



Nem megyünk most itt végig a trükkös weboldal minden egyes elemén, [akit érdekel, itt nézheti meg a domain bejegyzésüket](#), hanem menten belecsapunk a lecsóba: ehhez pedig a weboldal legalsó sora adja a megfelelő kulcsot és muníciót: **"*ONLY FOR ADULT OVER 18 YEARS OLD AND SHALL REQUIRE SENDING ONE SMS FOR INSTALLATION, AND YOU WILL RECEIVE ONE CODE. THE PRICE OF EACH SMS IS 3€. TOTAL COST OF SERVICE 3€ + PRICE OF A REGULAR SMS . IF YOU WANT TO DOWNLOAD FROM THE FROM THE SOFTWARE'S OWNER CLICK HERE. THIS SITE IS NOT A AFFILADED TO THE SOFTWARE'S ONWER AND ONLY OFFER A VERIFIEDED LINK FREE OF VIRUS AND SPYWARES. THANKS FOR YOU VISIT us. Contact"**. Magyarul **nincs 2 hétig, vagy egy hónapig használható ingyenes próbaváltozat, ellenben van megrendelői emeltdíjas SMS 3 EUR-ért** - ez mai középárfolyamon darabonként kábé 800 HUF, egy a küldéshez, plusz egy a "kód" fogadásához.



Hogy [a jogi csúrcsavar se maradjon ki a zavarosban halászási dologból](#), a hamisítók gondosan megtervezik, mivel védekezhetnek, ha esetleg netalántán egyszer megszorongatják őket. Hiszen **az ő programjuk nem "Avast!" hanem csak "Avast"**, ők nem hamisítottak semmit se nem ;-). Ám ha az átlagnetezőket vizsgálunk, hányan vesznek észre ilyen különbségeket, azt kapnánk, jó részük a valódi programot vélte felismerni. Azt is **észrevehetjük, hogy a [valódi Avast.com oldalra is mutat egy link az alsó sorban](#)** (*IF YOU WANT TO DOWNLOAD FROM THE FROM THE SOFTWARE'S OWNER CLICK HERE*), talán ez is már egy olyan trükk, amivel úgy gondolják, eredményes védekezhetnek majd a bíróságon.



Mindenesetre **[amit ők terjesztenek, az nem valódi vírusirtó, erről egy VirusTotal is könnyen meggyőzhet minket](#)**, és erről árulkodnak [a témáról folyamatosan megjelenő How To Remove](#) intrukciók is.



Érdekes, hogy a riportban az Avast! is riaszt erre a kódra, nevesíti, de **a weboldalt [még nem sikerült neki bezáratnia](#)**, talán a fenti dolgok is sikerrel kuszálják össze a különben teljesen egyértelmű helyzetet és annak bizonyítását.



Mi következik mindebből? Egyfelől gyanakodjunk, ha váratlanul egy kasperkyfrance.com vagy nod32england.com weboldalt látunk - lehet hogy nincs ezzel semmi gond, **de ez feltétlenül ellenőrizendő**. Másfelől a "cipőt a cipőboltból" szlogen alapján a megbízható **letöltést kizárólag a gyártó-hivatalos viszonteladó weblapjáról/apple storeból/hivatalos tárolóból** elv lehet az, amit még alaposabban érdemes lehet megszívlelni.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kényszerű](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonsággal](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2816304>

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>

2011.04.12. 10:07:21

Fájt a szívem, hogy ennyire nem érdekelt ez a tegnapi téma senkit. Pedig nem is akartam, hogy ilyen gyorsan igazam legyen, de itt egy mai cikk, és benne már egy "McAfee VirusScanPlus" screenshot.

news.cnet.com/8301-27080_3-20052203-245.html

A beszámoló szerint: "The company has seen five versions of the rogue security programs masquerading as software from Avast, Norton, McAfee, BitDefender, and RootKitBuster, and they, as usual, target Windows systems."

Welcome to the Activation System

2011.04.13. 13:55 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [windows csalás](#) [aktiválás](#) [kártévő](#) [mikko](#) [ransomware](#) [hyppönen](#)

Üdv a Matrixban! Vagy csalás áldozata lettél, vagy rendszer hiba lépett fel. Szerinted? Ha mégis szeretnéd tovább használni a Windows-odat, előbb be kell fejezni egy telefonos aktivációs procedúrát. SMS lehetőség kizárva.



A [zsaroló kártevőkről](#) többször [is megemlékeztünk](#) már, [változatos, új utat](#) kereső helyre [kis trükkjeiknek számos posztot](#), sőt egy ízben [egy egész PC World cikket is szenteltünk az izgalmas témának](#). S hogy a készítők nem pihennek a babérjaikon, azt mi sem bizonyítja jobban, hogy meg tudnak még lepni bennünket: "az önök Magilla barátja új oldaláról mutatkozik be", ezúttal Microsoft Windows váltságdíj témában jeleskedtek.



Az egyik legremekebb szakmabeli fickó, **Mikko Hyppönen** vette a fáradságot és járt utána annak a kártevőnek, amely a **Windows** aktiválással kapcsolatban vet be egy agyafúrt social engineering trükköt. Ide a rozsdás bökött, hogy a számlájukon máris van egy tetetemes összeg a naív áldozatoktól.



A trójai a fenti szöveget még kiegészíti azzal, hogy **az aktiválási procedúra természetesen ingyenes (na persze)** és amíg azt el nem végeztük, addig **"biztonsági okokból"** az állományaink zárolásra kerültek (köszönjük Emese). Ehhez mindössze egy ismeretlen telefonszámot kell hívni, van ebből több is: például dán (45), madagaszkári (261) vagy egy Globalstar Mobile Satellite Service nevű szolgáltató előhívószáma (8819). [Mikkoék természetesen végigjárták a játékot, és felhívták a számot](#), ahol a klasszikus emeldíjas szivatás sötét bugyraiba csöppentek.



Várni kell: "Hello. Welcome to the activation system. Please wait! Please hold the line 3 minutes :-)", addig fülbemászó zene szól, majd **uszkve 3 perc 40 másodperc után a géphang bediktálja a mi aktiváló kódunkat**, ami nem más, mint: 1351236. Ám később kiderült, ez a szám egyáltalán **nem egy egyedi, hanem minden egyes hívásnál - természetesen a hosszas pénzketyegtető várakoztatás után - ugyanezt a kódot olvassa be** a szőke női hang ékes angol nyelven. Az MP3 formátumban elmentett teljes "beszélgetés" meghallgatása egy élmény :-)



Természetesen csalásról van szó, és a valódi Microsoft aktiváláshoz semmi köze. Aki már végzett telefonos aktiválást, tudja, legtöbbször lokalizált számot (saját anyanyelvén, nálunk például magyarul, nem emeldíjas, hanem helyi hívásként) és ott az azonosításhoz be is kell diktálni a saját egyedi kódunkat, aminél a hús-vér kezelő az adatbázisból látja, hogy már hányszor éltünk a telefonos lehetőséggel, majd segít, és bediktál egy valóban egyedi kódsort. Természetesen **a trójai valamelyik jövőbeni új verziója is kérhet majd be ílyet, ha addigra a csalók elegendő mule-t toboroznak** egy otthonról végezhető, jól fizető, szaktudást nem igénylő telefonos távmunka kategóriájú álláshirdetésre. A témához kapcsolódó, [a zsaroló kártevőkkel kapcsolatos áttekintést](#) itt lehet megnézni a YouTube-on.



A lényeg, **nem érdemes hívni a számokat, [ez egy csaló kártevő](#)**. A becsapott felhasználók között még akár olyan is lehet, aki ha nem olvassa ezt a cikket, fel sem vetődik benne, hogy becsapták - ez nagyjából egészen a telefonszámla kézhezvételének idejéig lehet igaz, ott már aztán jön a fejbekölintő meglepi és a felejtethetetlen "aha" élmény.



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2822295>

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](#).



[reconka](#) • <http://www.reconka.info> 2011.04.21. 17:43:24

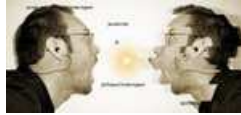
eszméletlen

JavaScriptke és a hét elgyötört trójai

2011.04.15. 12:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [magyar adatok](#) [nod32](#) [eset](#) [havi](#) [threatsense](#) [vírusstatisztika](#)

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



Ezúttal **hét trójait is találunk a toplistában**, amely fontos figyelmeztetés lehet arra, hogy a böngészés illetve telepítés mennyire fontos és kritikus területe a számítógépes biztonságunknak. A Conficker "bérelt" első helyén, és egy minimális sorrend cserén kívül csupán egy újonc kártevő felbukkanása bontotta meg a szokásos képet. **A JS/TrojanClicker.Agent trójai egy olyan kártékony JavaScript**, amely lefutva kártékony kódokat helyez el a Windows kulcsfontosságú (Windows, Windows/System32) mappáiba, és az ott el található fertőző komponensek automatikus lefutását biztosító Registry bejegyzéseket készít, amelyek a számítógép minden újraindítása után lefutnak. Ezen felül **hátsóajtót nyit a rendszerben, és további kártékony komponenseket próbál meg letölteni** különféle távoli weboldalakról.



Összességében elmondhatjuk, az internetes böngészés közben - de ahogy [a múlt heti statisztikában láthattuk](#), akár egy PDF megnyitásnál is - **komoly esély van rá, hogy különféle, kártékony kódokkal vagy adatlopással kapcsolatos JavaScriptek próbáljanak meg automatikusan lefutni számítógépünkben**. A már szokásos naprakész vírus- és kémprogramirtó használata, valamint az operációs rendszer és programjaink rendszeres biztonsági frissítésein felül így az is nagyon **fontos, hogy a böngésző kliensük megfelelően legyen beállítva biztonsági szempontból**. Ez természetesen okoz némi plusz feladatot, odafigyelni valót, viszont kezünkbe adhatja a hatékony védekezés további lehetőségét.



Az alapértelmezett böngészőkliens állapothoz képesti sebezhetőségünkön például **akár már egy olyan egyszerű beállítás is sokat segíthet, mint amilyen a "Harmadik féltől származó süti elfogadása: megerősítés minden alkalommal"** opció. Természetesen emellett számos opció és **külön telepíthető Plugin is segíthet nekünk ebben**, például a megfelelően beállított NoScript kiegészítő szinte minden káros Facebook kód vagy fertőzött bannerhirdetés kiszűrését el tudja végezni, így érdemes lehet vele megismerkednie annak, aki esetleg még nem használja.



Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2011 márciusában a következő 10 károkozó terjedt a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 18.76%-ért.



1. Win32/Conficker féreg

Elterjedtsége a márciusi fertőzések között: **5.84%**

Előző havi helyezés: **1.**

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 eljárashívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárason 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.



A számítógépre kerülés módja: 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>



2. INF/Autorun vírus

Elterjedtsége a márciusi fertőzések között: 2.98%

Előző havi helyezés: 2.

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozónak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.



A számítógépre kerülés módja: Fertőzött adathordozókon (akár MP3-lejátszókon) terjed.

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



3. Win32/PSW.OnLineGames trójai

Elterjedtsége a márciusi fertőzések között: 1.92%

Előző havi helyezés: 3.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományaikat és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatokat titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



4. JS/TrojanClicker.Agent trójai

Elterjedtsége a márciusi fertőzések között: 1.51%

Előző havi helyezés: -

Működés: A JS/TrojanClicker.Agent trójai egy olyan kártékony JavaScript, amely lefutva kártékony kódokat helyez el a Windows kulcsfontosságú (Windows, Windows/System32) mappáiba, és az ott el található fertőző komponensek automatikus lefutását biztosító Registry bejegyzéseket készít, amely a számítógép minden újraindítása után lefut. Ezen felül hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok!/trojanclicker-agent>



5. Win32/HackMS trójai

Elterjedtsége a márciusi fertőzések között: 1.34%

Előző havi helyezés: 4.

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítéskor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>



6. Win32/VB féreg

Elterjedtsége a márciusi fertőzések között: 1.28%

Előző havi helyezés: 7.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Áruklódó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



7. Win32/Shutdowner trójai

Elterjedtsége a márciusi fertőzések között: 1.23%

Előző havi helyezés: 6.

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>



8. Win32/Tifaut trójai

Elterjedtsége a márciusi fertőzések között: 1.15%

Előző havi helyezés: 5.

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csrcs.exe és autorun.inf néven. A kártékony EXE fájl automatikus lefuttatásához külön bejegyzést is készít a rendszerleíró-adatbázisban. Működése során több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21tifaut>



9. Win32/RegistryBooster trójai

Elterjedtsége a márciusi fertőzések között: 0.77%

Előző havi helyezés: 10.

Működés: A Win32/RegistryBooster alkalmazás a hamis antivírus programokhoz hasonlóan hamis riasztásokkal igyekszik rábeszélni a felhasználókat a „program” fizetős változatának megvásárlására.



A számítógépre kerülés módja: Fertőzött weboldalról települ, vagy a felhasználó maga telepíti.

Bővebb információ:

<http://www.eset.hu/tamogatas/viruslabor/virusleirasok/registrybooster>



10. HTML/ScrInject trójai

Elterjedtsége a márciusi fertőzések között: 0.74%

Előző havi helyezés: 9.

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2826824>

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.

Nyílt levél a Facebook biztonságról

2011.04.18. 15:50 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [biztonság](#) [facebook](#) [sophos](#) [graham](#) [clueley](#)

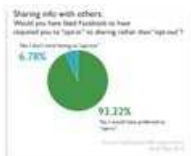
Kedves Facebook! Így kezdődik Graham Clueley levele, és bár lehet sokaknak az [április elsejei posztunk ugrik be](#), ám ezúttal valóban komoly dologról van szó.



Az első és legjobb bemelegítő logikai probléma legyen az, hogy ugye [mint az közismert](#), vannak ezek az [átverős, trójai applikációk, csalárd alkalmazások](#), ahol sokszor és sokan tanácsolják az egyszeri juzernek, hogy használj naprakész vírusvédelmet, használj fekete és fehérlistákat kezelő böngésző kiegészítőket: NetCraft Toolbar, Finjan Secure Browsing, McAfee, PhishTank, stb.), használj NoScript kiegészítőt, aztán meg [ne kattintgassunk ész nélkül](#). Rendben, ez eddig oké, segíts magadon, és Isten is megsegít. De mit csinál közben a Facebook? Ők miért nem tesznek valamit? Sőt még jobban átfogalmazva, miért nem tesznek már valamit ők - is? Nem utolsósorban pedig vajon csökken-e világszerte a kártékony Facebook alkalmazások száma, ha valódi, a megfelelő helyen elvégzett megoldás helyett mindenki csak a kliens végpontokon úzi az ördögöt magának kinyájában? Megszentségtelenítjük a költői kérdést, és válaszolunk rá: nem, nem csökken. Majd az utókor eltöprenghet a történelemórán, hogy miért nem tisztítjuk ki egyszer, egy helyen a nagy közös kutat, helyette inkább mind a 600 millió felhasználó szív, vagy beleszor 600 milliószor egy marék Katadyn tisztítótablettát a 600 millió vizespohárba. Bravó!



Hát igazából itt van a kutya elásva, és a továbbiakban nézzük is meg ezt a bizonyos levelet. Petőfivel ellentétben itt nem tizenkettő, mindössze három fontos pont szerepel, ezek közül is az első mindjárt a privátszféra védelmét erősítő, már korábban is, meg többször is falrahányt borsóként javasolt [optin rendszerű megosztás, azaz ne menjen minden azonnal automatikusan](#) (S. éppen fehér színű, XXXL méretű óvszert választ az online shopban), hanem csak az, amit a felhasználó önként, saját döntése alapján engedélyez. Hehe, végülis merjünk nagyot álmodni, nem? Gyáva népnek nincs hazája.



Második pontként következik a Facebook fejlesztők alaposabb ellenőrzése. Ma bárkiből lehet ilyen, számuk meghaladja már az egymilliót, és sokan közülük ontják a kártékony, becsapós, adathalászós, és egyéb kéretlen no meg nemkívánatos holmikat. Emlékezhetünk, hogy a Symbian esetében is hozott pozitív eredményt a [9.0 aka S60R3 verzióval bevezetett szigorító szabály, amiben a digitálisan aláírt, jóváhagyáson alapuló](#) módszert vezették be. Sosem lesz vége a Fancheck típusú hamis alkalmazásoknak, ha nem ott ragadják meg a lényeket, ahol azt kellene. (ám debár lett volna ide más, kevésbe elegánsan szalonképes hasonlat is :-).



Végül a harmadik pont arról szól, szép ez a HTTPS "everywhere is it possible", de ennek inkább defaultnak kellene lennie és mindig. Vagy ahogy Jack Bauer mondaná, "this is not an option, this is an order". Akkor működhetne ez igazán hatékonyan.



Szóval összegezve a válogatott lényeket, kíváncsian várjuk (na jó, sejtjük az eredményt, de azért hátha, mégis, netalántán, esetleg vajha, reménykedni már csak szabad, vagy nem) a választ a levélre: ["Why wait until regulators force your hand on privacy? Act now for the](#)

greater good of all. Your users tell us that these are issues they want resolved. So our question is simple: when do you plan to act?"

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [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/2836492>

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](#).

stvn • <http://blogok.info> 2011.04.18. 16:12:42

Valószínű, hogy a https-ből lesz valami hamarosan, legalábbis a fejlesztőket "szekírozzák", hogy az iframe appoknak legyen ssl változata is...



buherator • <http://buhera.blog.hu> 2011.04.18. 17:43:29

"Majd az utókor eltöprenghet a történelemórán, hogy miért nem tisztítjuk ki egyszer, egy helyen a nagy közös kutat, helyette inkább mind a 600 millió felhasználó szív, vagy beleszor 600 milliószor egy marék Katadyn tisztítótablettát a 600 millió vizespohárba." - Ez azért nem működik, mert a FB alkalmazások nem a FB-nál futnak, így nem lehet őket központilag ellenőrizni. A HTTPS pedig nem ér semmit, ha az egységjűzer minden alkalmazást ész nélkül telepít.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2011.04.18. 20:24:49

Hali!

Ebben igazad van, de ettől függetlenül ha lenne azért egy ellenőrzés, szűrés már az elején, ez jótékonyan jelentkezne a kártékony appok darabszámában, Meg nyilván teljesen sosem szűnne meg, és akkor mindenki a frissítésekbe pakolná a görénységet, de ha meg nem tesznek semmit se, azért az se jó.

A jűzer ellen nincs orvosság tételben is van igazság, de vegyük azt, hogy GC minden tanácsát megfogadják (1%). Csökkenne úgy a véletlen megosztásos adatszivárgás, a kecsége appok egy nap alatti sokezes ámokfutásos tarolása, az account lopási ráta? Én úgy vélem, hogy igen.

Murphy szerint azt mindenki briliánsanl meg tudja magyarázni, miért nem csinál meg valamit :-) Van valami olyan dakota okosság: többet használsz azzal, ha gyűjtasz egyetlen gyertyát, mintha álló nap az Edison társaságot szidalmazod. Úgy tippelem, Zuckkerék pénzüknél vannak így is, ezért amíg nincs igazi versenyhelyzet, magasról tesznek rá, csak pörögjön a forgalom, legyen az aztán bármitől.

Doktor Spamhaus, ROKSO és fivérei

2011.04.20. 15:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam levélszemét kéretlen spamhaus rokso](#)

Hivatkoztunk már rá többször a ROKSO lista kapcsán, de bővebben talán egyszer sem beszéltünk róla. Pedig [a Spamhaus projekt](#) már több, mint tíz éve harcol a kéretlen levélszemetelők ellen, sőt még hasonló kalandokba is keveredett, [mint anno Kaspersky a Zango/180 Solutions ellenében](#).



A szervezet rendszeresen közzéteszi, illetve karbantartja azokat a nyilvános listákat, amelyekben a spamterjesztők személyek, szervezetek IP címei, vagy tartományai kerülnek összegyűjtésre. A Spamhaus Block List (SBL) egy IP-címeket tartalmazó fekete lista, ahonnan a South Park szóhasználatával élve semmilyen korosztály számára nem ajánlott leveleket fogadni.



A már hivatkozott ROKSO (Registry of Known Spam Operators) lista a leggaládabb spammerek szégyen toplistája, és amikor [az állítólagos Alexey Tolstokozhev állítólagos fejbőlövéséről kaptuk az állítólagos híreket](#), többek között ott is az lett gyanús, senki nem hallott róla, a Google megnémt, és a hírhedt toplistában nem hogy előkelő helyen, de sehol nem szerepelt. Az aktuális havi [ROKSO Top10 listán](#) a volt szocialista utódországok adják a helyezettkek krémjét, az első három helyet is ők uralják: 3 ukrán, 3 orosz és 1 észt mellett éppen csak befér 1 indiai, egy hongkongi és egy USA-beli résztvevő. Ha pedig a [nagy százas listát nézzük, ott már érvényesül az amerikai fölény, 54 személy illetve szervezet képviseli az USA-t](#), míg a második helyezett Orosz föderáció "mindössze" 9 résztvevőt vonultatott itt fel, megelőzve a harmadik helyen osztozó 4 pontos Kínát, Indiát, Kanadát és Ukrajnát.



Az emlegett atrocitások között olyan kalandok szerepeltek, mint [összezördülés a Spamhausot bíráló Paul Grahammal, majd weblapjának felvétele a blokkolandók listájára](#), de a legjelentősebb kétségkívül [az évekig húzódó per az E360insight cég ellen](#). Bár a végeredmény [az ugyancsak évekig húzódó Kaspersky perrel](#) szemben nem az igazság diadala lett - [hihetetlen módon a Spamhaus vesztett és kártérítésre kötelezték](#) - szakmai hitele ennek ellenére nem kérdőjeleződött meg.



Nyilván rengeteg olyan spam is beesik a postaládánkba, [amiről első látásra kinderspiel eldönteni, hogy éppen az, aminek látszik - vagyis szemétlevele](#). Ám néha az ügyesebbje meglepi a közönséget formában és/vagy tartalomban is olyan szofisztikáltabb levéllel, aminél a kételkedés, utánanézés adhatja meg a választ annak, akinek a kéretlenség korábban nem volt elegendően erős érv a delete gombra való rákönyöklésre. Ekkor a Google találatok, vagy a [spam levelek gyűjtőhelyei](#) adhatnak [támpontot arra nézvést](#), miért is nem kell [elhinni az üzenetben foglaltakat](#).

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2842377>

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 Húsvét

2011.04.22. 21:00 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [húsvét ünnep](#) [kaspersky ivan](#)

Semmi komoly mélyenszántó nem következik, egy gyors örömhír valamint egy nyúlfarknyi köszöntő lesz a mai napra rendelt program.



Komoly aggodalomra adott okot, mikor pár napja hírt vettük, hogy [Moszkvában elrabolták Eugene Kaspersky húsz éves fiát, és 3 millió euró váltságdíjat](#) kértek érte. Bár semmilyen hivatalos információ nem látott napvilágot az elrablók kilétéről, a félsz azért ott bújkált mindenki belsejében, mert még egy esetleges fizetés sem ad garanciát hasonló esetekben arra, hogy biztosan élve viszontlássák a túszot.



Annál nagyobb volt a megkönnyebbülés, mikor három nap elteltével kiszabadult, és az ismeretlen összegű [váltságdíj kifizetése után újra családjához csatlakozhatott Ivan Kaspersky](#). **A szakma minden képviselője nevében ezúton is gratulálunk a szerencsés kimenetelű végkifejletéhez.**



Ezek után már nem is szaporítjuk tovább a szót, hanem **minden Kedves Olvasónknak Boldog Húsvéti Ünneket Kívánunk!**



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2848382>

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.

Elkerülhetők-e teljesen a trójaiak, kémprogramok?

2011.04.26. 16:00 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [apple](#) [gps](#) [iphone](#) [android](#) [consolidated.db](#)

És ha igen, akkor miért nem. A rövid válasz erre a kérdésre az, hogy: nem. A bővebb válasz pedig, hogy sajnos nem mindig.



Mire alapozzuk ezt? Ehhez részint utalunk egy korábbi írásunkra, melyben párhuzamot vontunk a Firefox pluginek - [nevezetesen a NoScript egyik vitatható frissítése](#) - és az okostelefonok alkalmazás áruházai, letöltési portáljai között. Magyarán **hiába van még egy kezdeti benyújtáskori szigorúság is, ha aztán később bármelyik frissítés hozhatja magával a késes viselkedést, kémkedést, adatlopást.** Hogy csak két apró mobilos példát hozzunk, egyfelől az Androidos telefonok már idén februárban felhívták magukra a figyelmet azzal, hogy **[az alkalmazások 11%-ban volt valamilyen kártékony funkció, vagy éppenséggel a felhasználók GPS adatainak illegális kikémlelése](#)**, továbbítása. De említhetjük azt a még 2007-ben kipattant esetet is, amikor **[felmerült annak a gyanúja, hogy az iPhone "hazatelefonál"](#)** és továbbítja az Apple szervereire a látogatott weboldalak, emailcímek, hívások adatait, amit persze cáfoltak.



Emellett nem is olyan régen mindkét platform látványosan demonstrálta a gyakorlatban azt is, hogyan működik [az alkalmazások távoli letiltása módszer](#). Ebben hónapban pedig végképp hegyomlásszerűen jöttek a dolgok: előbb **[az iPhone esetében bizonyosodott be, hogy már egy éve gyűjti egy consolidated.db nevű fájlba a felhasználó által érintett összes GPS adatot](#)**.



Természetesen **forensic szakemberek már ezt régóta tudták, megírták, [sőt könyveket is publikáltak a témáról](#)**. "A felhasználónak még mindig jóvá kell hagynia, hogy egy-egy alkalmazás hozzáférjen a tartózkodási helyek adataihoz, és azonnal ki is kapcsolhatjuk az alkalmazások helymeghatározó szolgáltatásait a Beállításoknál. - mutat rá Levinson. A színpalak mögött azonban az adatok loggolása tovább folyik, hiába tiltjuk azt le az adott alkalmazásnál."



Az igaz, hogy annak **[semmi nyoma, bizonyítéka nincs, hogy ezeket az adatokat az Apple szerverei távolról le próbálnák tölteni](#)**, de mindazonáltal egy átlagos felhasználó joggal jöhet zavarba egy ilyen ellentmondásos helyzetben. **[Az okostelefonokkal kapcsolatban kialakult gyakorlat](#)** sokak számára lehet ijesztő. Ezen pedig éppenséggel csak ront, hogy sajnos **az incidensek kiderülésekor rendre [csak a szokásos nagy kummantás, hallgatásba burkolózás](#) van, megnyugtató, tisztázó világos magyarázatok helyett.**



És akkor **[ezek csak a nagyágyúk, a neves gyártók körüli kételyek](#)**, a kisebb hardverfejlesztők, ismeretlen szoftverek, új alkalmazások készítői még ennél is kevésbé ellenőrizhetőek, illetve számonkérhetőek. Nyilvánvalóan a megbízható programok, szolgáltatók, letöltések tudatos és körültekintő kiválasztásával gyengíthetjük némileg kitétségségünket, ám minden ellen nincs orvosság, csak a tőlünk elvárható legnagyobb gondossággal járhatunk el. Ami sok esetben még így sem lenne kevés, sőt.



Bár félfő, az új divattal ismét itt lehet egy magas labda: most a bűnözőknek a consolidated.db látványos térképmegjelenítőjébe vagy az ilyenekre mutató Google találatokba lesz érdemes kártevőt vagy trójait csomagolni.



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2856196>

Kommentek:

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

Nincsenek hozzászólások.

Többször lesz neten kutyavásár

2011.04.28. 13:45 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [hirdetés](#) [kutya](#) [scam](#) [csalás](#) [átverés](#) [419](#) [kameruni](#)

Nem lehet csak a banki, [adóvisszatérítési](#), vagy árverési portálokon való vásárlásokra szűkíteni a [számítógépes visszaélések körét](#). Akár egy ajándék kutyakölyök befogadással kapcsolatban is simán belefuthatunk érdekességekbe.



Egy kedves olvasónk hívta fel a figyelmet egy hirdetésre, ami inkább egy jól fejlett csalástípus, és korántsem egyedi, no meg korántsem csak magyar. Időközben ezt a hirdetést már törölték, de nyilván megjelenik majd újra, másik kutyafajtával, látszólag másik városból adresszálv. Szóval ajándék kutya hirdetés az Express-ben, amire aztán a jó öreg 419-es gépezet fogaskerekei indulnak be fűlsüketítő csikordulással.



Érdeklődésünkre ez az első levél még úgynevezett "magyar" nyelven jön:

"Szia,

Csak olvastam, hogy érdeklődik a Jim. Akartam, hogy felajánlotta, hogy nővérem, de ő nem túl kényelmes a gondolattal, hogy növelése a kölyök most így, szerencsés is, ő továbbra is elérhető az elfogadásra.

Ő egy 14 hetes, 3 nap kan, fajtiszta, és ő kapott naprakész papírokat. Ő volt minden a lövések, és már dewormed. Is, ő még nem desexed. Remélem nem bánod, hogy megkértem egy-két kérdések:

Ön házas?

Van gyereke?

Van egy saját otthon saját, vagy ha bérbe?

Mennyi idő lesz már elérhető tölteni vele?

Volt valaha egy kiskutya előtt? vagy bármely más, Pet?

Van jelenleg bármilyen háziállat (ok) veled?

Ha valóban megvan a kölyköt, vajon egy "zárt" vagy "a szabadban" pet?

Attached alábbiakban néhány képet a baby Jim, szeretted őt?

Bocs, ha én kérek egy kicsit túl sok kérdést. Csak azt akarom, hogy biztosan ő is jó lesz veled. Csak annyit kell neki most, egy szerető család, amely kezeli őt, mint a jogdíj.

Nem vagyunk eladási neki. Adunk neki, hogy olyan szerető család, amely A vevő jó vigyázni rá. Ha készen áll erre, hadd tudjam meg a saját címét és telefonszámát (ok), hogy én is gondoskodik

A házhozszállítás az Ön számára. Fizet közlekedési és szállítási díj (9500HUF), közvetlenül a szállítmányozási vállalat. Ha a bírságot, engedjétek tudja, milyen hamar lesz szükség rám, hogy kezdjen tárgyalásokat az áruszállító.

Ha tényleg komolyan kezd neki, akkor kap vissza rám a lehető leghamarabb a választ a fenti kérdésekre, és nyugodtan kérni minden olyan kérdés (ek), hogy van. Kérjük repply angolul, ha lehet.

Köszönöm

Clement"



A mellékelt képekből jó érzékkel kiszedtek minden érdemi exif infót

Am később pedig **már nem is bíbelődnek holmi gugli transzlétekkel**, hanem bele is csapnak a lecsóba a kameruni fiúkák. Itt már [nincs is nagy különbség az emailtő nyeremény, vagy az afrikai örökség kimentésének](#) végjáték fázisai között: **fizessünk, utaljunk - ez itt a válogatott főlényeg.**



Csak pár ecsetvonás, és voila: hamis diploma, email lottó nyeremény, vagy kutya szállítás? Gond egy szál se!



Egy lehetséges névdonor Clement Shey a sok közül, ő sem kameruni

Összefoglalva: **aprócska intő jel lehet már az is, ha az eredetileg távoli Debrecenbe címzett levélre a közeli Kamerunból válaszolnak;-)** Ha pedig valaki bármilyen témájú - Facebook, Express, Addel, Viddel, Veddel, Mardel - hirdetéssel kapcsolatban belefut az ilyen [Fülig Jimmyvel ékesített Tuskó Hopkins stílusba](#); és/vagy **túl sok kíváncsi és abszolút nem releváns kérdést tesznek fel neki** hirtelen felindulásból; és/vagy látatlanban ismeretlenül megbízva kellene számlaadatokat megadni, esetleg **előre kellene pénzt küldeni, akkor érdemes előtte alaposan végiggondolni a dolgokat [egy White Russiannal kettesben](#)**. Vagy például előbb elszámolni végtelenig, akár mindjárt kétszer is.



Nyelvterületek jönnek, nyelvterületek mennek. Am a Debrecen-Kamerun tengelyt uraló Clement Shey roppantmód kitarító...

Ha valaki valóban ingyen akar örökbefogadni gazdi nélküli kutyát, [arra már megvannak a megbízható hazai csatornák](#), kameruni vargabetű nélkül.

 Tetszik  15 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Android kémprogram persze csak a mi érdekünkben](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [25-ször több a mobilos kártevő](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2861313>

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](#).

stevie-w 2011.04.28. 19:06:22

Nekem nagy tanulság, hogy a Google Translate milyen vacakul bánik a magyar nyelvvel. A bolgár szöveg csak kicsit természetellenes, olyan mintha valaki kapkodva vagy figyelmetlenül és egy kicsit óvodás stílusban írta volna, de teljes egészében érthető -- a magyarral ellentétben.

stevie-w 2011.04.28. 19:09:09

Amúgy én a minap egy tök egyszerű, 20 ezer forintos mobiltelefont hirdettem a neten, amire pont egy Kanadában élő ifjú hölgynek lett volna égető szüksége :-)



halál megdöglessz kinyírunk ® • <http://href.hu/x/73ug> **2011.04.28. 23:11:28**

de most komolyan. aki ilyen hirdetésnek felül, az meg is érdemli.

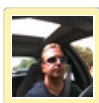


Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.04.29. 17:12:52**

Szia kedves halál megdöglessz kinyírunk!

Az igaz, hogy az első levél az valójában csak az én játszadozásomat és screenshotomat szolgálta, de akármilyen hihetetlen, ki kell, hogy ábrándítsalak.

A kitakart második levél igazi volt, a tippadó hús-vér ismerőséé, és már a valódi adatait feketítettem ki benne, lakcímmel, telefonszámmal. Hát sajna ez van.



BenkovicsTomi 2011.04.30. 14:31:07

Sajnos a magyar nyelvvel sok gondja van a fordító programoknak. (szerencsére a következő OS X beszél magyarul. :)) Bár ezek a hirdetések és vásárlási lehetőségek nagyon elképesztőek. Tényleg butának kell lenni ahhoz, hogy felüljél nekik. Azért csak képzeld el, ha nagyon szeretnél valamit... Nem keresgetnéd a net-en a legolcsóbb forrást?

Esküvőszagra gyűl az éji vad

2011.05.02. 11:40 | [Csizmazia István \[Rambo\]](#) | [2 komment](#)

Címkék: [google](#) [kereső](#) [hamis](#) [kate](#) [herceg](#) [antivírus](#) [mérgezés](#) [kártévő](#) [találat](#) [esküvő](#) [vilmos](#) [m Middleton](#)

Újabb neves esemény zajlott, amelynek hírverését felhasználva tarolhattak a kártékony kódok terjesztői. Ezúttal Vilmos herceg és párja, Kate Middleton esküvője jelentette az új apropót. A ceremóniát [csak Amerikából 22 millióan követték a televízió képernyőinél](#). A menyasszony nevére, ruhájára pedig az internetezők az elmúlt hónapban több mint 1.2 millió alkalommal kerestek rá a Google-ben.



Ezt a felhajtást használják ki rendre az internetbűnözők is, akik **fertőzött honlapokat optimalizáltak az eseménnyel kapcsolatos kulcsszavakra**. A nagy érdeklődést kiváltó események mindig alkalmat adnak az internetbűnözők számára arra, hogy megmérgezzék a keresők találatait. Ennek során először honlapokat készítenek, melyeket teljesen szokványos keresőmarketing technikákkal optimalizálnak az adott kulcsszavakra. Majd, **amikor a keresések száma hirtelen megugrik, az oldalakat vírusokkal fertőzik meg**.



Pontosan ezt tapasztalták az ESET víruslaboratóriumának szakértői is, miszerint április második felében a **Win32/Adware.XPAntiSpyware.AB** elnevezésű kártévő előfordulásának száma négyszeresére nőtt az Egyesült Királyságban. A trójai program egyébként az emberi hiszékenységet is kihasználja a terjedéséhez, mivel ál-antivírusnak adja ki magát.



Így, amikor az internetező rákeres a királyi esküvővel kapcsolatos kulcsszóra, majd a találati listából pont egy fertőzött linket kattint le, egy olyan weboldalra kerül, ami „arról tájékoztatja”, hogy megfertőződött a számítógépe, és felajánlja, hogy a gép megtisztítása érdekében töltsön le egy programot, ami valójában maga a kártévő.



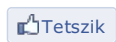
A nagy médiavisszhangot kiváltó eseményekkel kapcsolatos **internetes kereséseink kapcsán az alábbi szabályokat tartsuk be:**

- Óvakodjunk az olyan linkektől, melyek „sokkoló” híreket, videókat vagy képeket ígérnek.
- A megbízható, jó hírű portálokon keressünk információkat, és óvakodjunk az olyan „hírportáloktól”, melyekről még nem is hallottunk.
- Ne küldjünk pénzt vagy adományt olyan segélyszervezetnek, amelyről még nem is hallottunk (például a fukushimai katasztrófa kapcsán).

- Ha egy weboldalon olyan üzenettel találkozunk, amely szerint a számítógépünk vírussal fertőződött meg, ezt semmiképpen ne vegyük készpénznek, mivel a legvalószínűbb, hogy egy ál-antivírus próbál meg feltelepülni a gépünkre. A számítógépünket ilyenkor ismert forrásból beszerzett, jó nevű vírusprogrammal tudjuk ellenőrizni.



És bár ennek a mostani esküvőnek már vége, nem kell "búsulni", **a jövőben sem maradunk kártevővel mérgezett keresőtalálatok nélkül, hiszen Osama Bin Laden állítólagos halála és ezek videói** máris új apropót szolgáltatnak a következő hasonló akcióhoz.



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

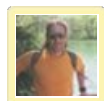
- [A PRISM szeme mindent lát](#)
- [Informatikai biztonság az egészségügyben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Ez történik a weben egy perc alatt](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2871280>

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>
2011.05.02. 20:24:28**

Na ez a Bin Ladenes dolog nem is váratott magára sokáig:
blog.eset.com/2011/05/02/osama-bin-laden-video-malware



**[pixmac3Cmanager](#) • <http://www.pixmac.hu> 2011.05.03.
08:35:45**

Elhiszem hogy kihasználják és igen, nagyon veszélyes és könnyen elhiszi az ember hogy a mutatott kép a böngészőben a saját computer képernyője, ami éppen vírus problémát mutat, és akkor meg elkezdünk klikkenni.

Béták reggelire II.

2011.05.05. 15:05 | [Csizmazia István \[Rambo\]](#) | [2 komment](#)

Címkék: [mobile security](#) [android](#) [eset](#)

Igaz [a korábbiakkal ellentétben](#) ezúttal csak egy adag reggeliről van szó, de az annál érdekesebb. Az Android várhatóan [a legsikeresebb mobil platform](#) lesz, illetve talán máris az. Most **megjelent és letölthető az ESET Mobile Security erre a rendszerre szánt nyilvános béta tesztverziója**.



Telepítése a szokásos: letöltés, futtatás, indítás, nem volt vele semmi gond, problémamentesen és gyorsan felkúszott mind az igazi HTC Desire HD vasa, mind pedig a Linux alatt futó Android SDK emulátorra. A beállítások már érdekesebbek, itt a mobil security csomagokra jellemző menüpontokkal találkozhatunk: **antivírus, spamszűrő, lopásgátló funkciók, adatbázis frissítés, jelszavas védelem, security audit** - ez utóbbira még később visszatérünk.



A program **minden fájlt, mappát, alkalmazást és memóriakártyát folyamatosan ellenőrzését végzi**. A telefonhívásokra vonatkozó szűrés kellemes régi Symbianos időköt idéz fel: **fekete és fehérlistázni lehet a bejövő hívásokat, és persze blokkolni a tiltott vagy ismeretlen számokat**. Nyilván a minden ismeretlen szám blokkolásának van egyfajta bizonytalansági tényezője is, magyarázom ha ezt választjuk, úgy egy fehérlistás ember lemerült mobilja után hiába kéri kölcsön a barátját, nem ér el minket, de a Posta, Eon, UPC, futárszolgálat stb. hivatalos ügyeinkben eljáró ügyintézők is felkoppánhatnak e korlátozásra. Ez **a ki- és bejövő hívásokat egyaránt érintő kontroll hasznos lehet például akkor, amikor a szülő állítja be mindezt a gyerek telefonja esetén**.



Persze érdemes a beállításokat teljeskörűen jelszóval védeni - ha bárki kikapcsolhatja a korlátozásokat, szabadon megváltoztathatja beállításokat, akkor nem sok értelme lenne az egésznek. A lopásgátlás beállításainál megadhatjuk a megbízható SIM kártyákat, míg az alertnél pedig egy incidens esetén használható telefonszámot tudunk beállítani, ebből is megadhatunk többet. Ha esetleg **ellopják a telefonunkat, SIM kártya csere esetén lezár a készülék, és a korábban bepötyögött számokra titokban riasztást küld SMS-ben**, de a korábban megismert [Remote Wipe](#), [azaz távoli törlési lehetőség is](#) a repertoár része.

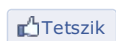




A **Security Audit** menüpont segít feltérképezni az "adatvagyon", ezek a tárolt adatok, számok, telepített applikációk és a kritikus beállítások állapota: szabad memória mérete, bekapcsolt Bluetooth, GPS és GSM beállítások, csatlakoztatott memóriakártya, USB eszköz, és hasonló. De **mindenféle incidens nélkül is hasznos lehet ez, például a nem használt Bluetooth kikapcsolása hasznos nem csak a biztonságunk miatt, hanem az akkumulátor idővel való takarékos gazdálkodáshoz is.**



A várhatóan még az idén megjelenő [Android program publikus bétaverzióját az ESET honlapjáról](#) lehet letölteni, próbálgatni, nézegetni; míg a hozzátartozó [PDF dokumentációt az alábbi linken](#) találjuk.



6 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

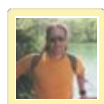
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Majdnem mindenki átverhető adathalászárral](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/2879473>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói tartalomnak minősülnek, értük a [szolgáltatás technikái](#) 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>
[2011.05.05. 14:21:24](#)

Android becomes most favorite platform for Trojans and malware in April:

mannasuurimo taikinakokkare keitto 2011.05.05. 15:35:15

én csak az ESET számítógépre írt vírusirtóját használom, és az tényleg nagyon expert, kár hogy csak harminc napig lehet próbálgatni :S

Béták reggelire III.

2011.05.09. 11:55 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [beta](#) [5](#) [security](#) [smart](#) [publikus](#) [nod32](#) [eset](#)

Vigyázni kell az egyoldalú táplálkozással, ezért ígérjük, egy ideig most nem lesz több bétareggeli, vagy ha lesz is, legalább egy gamma vagy delta virít majd a tányéron. Ami miatt azonban most mégis itt ülünk piritósunkkal a reggeliző asztalnál, **annak a [NOD32 és az ESET Smart Security vadonatúj, 5.0-s bétájának nyilvános megjelenése az oka.](#)**



Mi most az ESS-t választottuk ki a nézegetéshez, a letöltött csomag egyaránt használható aktív érvényes licenckulccsal, vagy pedig a mellékelt beépített időkorlátos bétateszt kulcsot is igénybevehetjük. Telepítés a szokásos, **figyelmeztet, hogy ne fusson másik valósidejű antivírus vele egyediőben**, ha mégis lenne ilyen, azt előtte okvetlenül uninstalláljuk.



Dönthetünk a felhőalapú **ESET ThreatSense.Net engedélyezéséről**, ezt bepipálva **a gyanús állományok gépünkről anonim elüldésre kerülnek további alaposabb elemzésre**, statisztikára, és innen értesülhetünk mi is, ha egy olyan vadonatúj kártevő jelentkezik, amely még az adatbázisban esetleg nem szerepel, de itt már születtek róla bejelentések.



A másik szintén **telepítési procedúra alatti szokásos választási opció a kérértlen alkalmazások blokkolása/engedélyezése** kérdés, amit szintén a felhasználónak kell eldöntenie. Ennek okát már többször is kiveséztük, ezért most erről röviden annyit: [jogi megfontolások miatt](#) történik ez ilyen módon.



A program [következő verziójának feature listájában](#) a **Gamer mód**, az észlelési teljesítmény és sebesség növelését, **felhő technikát**, és **szülői felügyelet menüpontot** látunk kitűzött célként a korábbi funkciók, például a spamszűrési hatékonyság, illetve a tűzfalas védelem továbbberősítése mellett. Ez utóbbinál a **HIPS megjelenése jelenthet további érdekes fejleményt** a részletekbe szívesen belemerülő, haladó felhasználók számára.



Az emlegetett gamer módnál pedig nem csak a játékokra kell okvetlenül gondolni, hiszen **lehet ez éppenséggel egy Powerpoint prezentáció is, ahol ilyenkor semmilyen üzenetet nem szeretnénk látni a teljes képernyős üzemmódban.** A szülői felügyelettel pedig egyszer később még hosszasan is el fogunk még játszani, kísérletezni.



Az 5.0 verzióban külön figyelmet szenteltek a fejlesztők a [hordozható médiakon egyre rafináltabb és kifinomultabb módszerekkel terjedő Autorunok](#) kártevők hatékonyabb ellenőrzésére is, ezért **a cserélhető USB eszközök, CD illetve DVD lemezek vizsgálata még részletesebben beállítható, illetve blokkolható lesz.** Kellemes további újdonság, hogy a programcsomag frissítés menüpontja alól is ellenőrizhető mostantól, van-e a programnak frissebb, letölthető változata.



Aki szeretné próbálgatni az 5-öst, az [az ESET.EU weboldaláról tudja letölteni](#) a 32, vagy 64 bites csomagot azzal a kiegészítéssel, hogy **ez egy előzetes béta kiadás, használata kizárólag fejlesztőknek és tesztelőknek ajánlott!**

 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](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2889151>

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 piszkos tizenkettő

2011.05.11. 16:20 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [spam statisztika](#) [malware terjesztés](#) [kártévő](#)

A [spam üzenetekkel kapcsolatos probléma sokrétű](#), nehezen kezelhető és nem igazán remélhető, hogy egyszer csak váratlanul elillan vagy magától megszűnik. És mióta ártatlan Rolex üzleti ajánlatok mellett, helyett már **rendre kártékony tartalmakat, vagy linkeket is hordoznak**, komolyan kiveszik a részüket a számítógépes kártevők terjesztéséből.



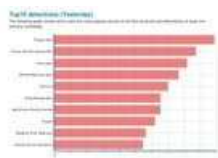
A Sophos tett közzé nemrég [egy statisztikát arról, hogy szerintük melyek a legjelentősebb spam kibocsátó nemzetek](#). Az élboly: **USA, India és Oroszország** után jól láthatóan a vén Európának nincs mit szégyenkeznie, hiszen számos közép-európai, köztük több volt szocialista ország, illetve utódállam képviselteti magát ebben az összeállításban. A statisztika annyira friss, hogy még meleg: azt **229 országot és 2011 első negyedét vizsgálva készítették a kutatók**.



Valószínűleg arról lehet szó, a felhasználók jelentős hányada nincs tisztában a kockázatokkal, nem ismeri azokat, ezért nem is fél tőle, és **ehhez volt jó adalék az a korábbi felmérés is**, amely arra hívta fel a figyelmet, [akár ki is kapcsolják a vírusvédelmet, ha az akadályozza a hőn áhított tartalom, program vagy weboldal megnyitását](#), használatát, futtatását.



Aki szívesen nézeget statisztikákat, az akár [az ESET VirusRadariján](#), vagy a VirusTotalon is tud pillanatnyi helyzetet, elemzett mintákat, gyakori kártevőket figyelemmel kísérni. Például **nem kicsi szám szerepel a tegnapi kedd mellett, amikor is 173 ezer mintát töltöttek fel VT vizsgálatra**, és ugyancsak meglepő, hogy ebből három változat is a közel tíz esztendő Nimda féreg volt.



Mindenesetre lényeg a lényeg: **a kéretlen tartalmak elutasítása nem könnyed részletkérdés**, hanem **fontos momentum a biztonság tudatos hozzáállás eszköztárában**, része és kiegészítője a gép fizikai és biztonsági programokkal való védelmének, valamint a biztonsági frissítések naprakész alkalmazásának.



Aki pedig dacolva az ésszerűséggel mégis megnyitogatja ezeket, [az nem csak a saját vagy munkaideje egy részét pocsékolja el](#), hanem emellett [számítógépének biztonságát is kockára teszi](#).

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)

- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2895654>

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](#).

[kultikula 2011.05.13. 07:49:54](#)

én találkoztam már olyan expert spamekkel, hogy észre se vettem és vihettem a gépet szerelőhöz...

A legjobb dolog a héten

2011.05.13. 12:15 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [konferencia](#) [hacking 2011](#) [ethical](#)

Lezajlott az idei [Ethical Hacking 2011 konferencia](#). Az évről évre emelkedő színvonal mellett az egy négyzetméterre eső etikus hackerek fajlagos száma is gigantikus, de van itt minden: zeroday, Android, felhő, RFID útlel és teltház.



A szokásos Aréna Plázás helyszínen zajlott le tegnap a **4. Ethical Hacking nap, ahol a jól összeválogatott témák, és a felkészült előadók** egy jó napot szereztek a téma iránt érdeklődőknek.



A főszervező Fóti Marcell (NetAcademia) bevezetőjében többek közt arról a jó hírről is beszámolt, hogy az [EC-Council CEH tananyag 7-es verziójába hivatalosan is bekerült a Barta Csaba által kifejlesztett](#), Windows rendszerek kompromittálására [alkalmas rootkites technika](#).

Az első előadást Veres-Szentkirályi Andrásról (Silent Signal) hallhattuk, aki a múltán népszerű Android platform érdekes gyengeségeire világított rá, és az általa kiemelt támadható részek hallatán az embernek az az érzése támadt, az Android lehet az új vadnyugat.



Mindenesetre újra kell gondolnunk az alkalmazásokkal kapcsolatos bizalmi helyzetet (például egy már feltelepített alkalmazás ajánl egy másikat), de emellett nem árt tisztában lenni azzal sem, hogy **a Google távoli program visszahívási lehetősége nem csak azt jelenti**, hogy [kártévő esetén ők ezt meg tudják tenni](#), hanem technikailag akár telepíteni is tudnának a telefonokra távolról bármit.



Barta Csaba (Deloitte) a jelszótárolással és megszerzéssel kapcsolatban tartott előadást, melyben újszerű megközelítéssel a Volume Shadow Copy segítségével készített olyan másolatot, amiben aztán offline már kényelmesen tudott vizsgálni.



Barátjával, John the Ripperrel ;-)) nem csak hashekből volt képes jelszavakat visszafejteni, hanem a teljes jelszótörténet segítségével a jelszóválasztási mintákat, szokásokat is eredményesen fel tudta térképezni, így **ezzel a módszerrel akár egy későbbi jelszó is megjósolható**.



A következő előadásban az **elosztott szivárványtáblás törést** mutatta be **Dávid Zoltán (BME)**, aki olyan megoldást igyekezett felvázolni, ahol a már kiszámolt eredményeket nem kell mindig fáradtságosan újra generálni, hanem az ilyen korábbi adatokra támaszkodva növelhető lehet a hatékonyság, illetve radikálisan csökkenthető az LM és MD5 hashek visszafejtésére fordított idő.



A szivárványtáblás törés lényege, hogy **nem okvetlenül az eredeti jelszót kapjuk vissza a segítségével**, hanem egy az adott hash értékhez társított egyenértű jelszóhoz jutunk, **amit mindenképpen tudunk használni** - magyarul egy adott hashhez több ekvivalens jelszó is tartozhat.



Buherátor és Pánczél Zoltán (Silent Signal) az etikus hackerek munkás hétköznapijaiba engedtek bepillantást, amelyből az derült ki, élesre fent nulladik napi exploit is egy szükséges kellék lehet az eszköztárban.



De emellett gyakran **tapasztalják azt is, hogy a rosszul konfigurált eszközök** (például root jogokkal futó Apache webszerver) is megkönnyítik az eredményes behatolást. Előadásuk végén meg is lett a hön áhított rendszerszintű jogosultság, valamint az ügyvezető igazgató laptopjáról megszerzendő tetszőleges állomány is sikeresen az ölükbe pottyant.



Aki az assembler kódokat hiányolta, az fellélegezhetett **Klock László és Spala Ferenc (kancellár.hu)** előadásán, akik a **virtuális környezetek biztonságáról beszéltek**. A megfelelő helyekre beszúrt NOP utasítások meg is hozták a kívánt látványos eredményt: lehetett jelszó nélkül utalgatni az összegeket a demo felhasználó számára.



Kihangsúlyozták ugyanakkor, hogy a "mindenható" vAdmin mozgástere és az azokkal való manipulációs lehetőségek valódi veszélyeket rejtene, de **ezt nem úgy kell felfogni, mint hibát ezekben a programokban, hanem sokkal inkább minden virtualizációs környezet sajátosságaként kell ezzel tisztában lenni**, és persze az ilyen jellegű kockázatok feltérképezésére is szükség van.



Az ebédszünet után egy könnyedebb téma következett, a [tavalyi Hacktivityn](#) debütált **Tomcsányi Domonkos** mutatta meg az **RFID-es e-útlevelek gyenge pontjait**. Mint kiderült, sajnos nagyon sok az Achilles sarok, nincs például brute force elleni védelem, és a meglévő útlevelek megdöbbenően könnyen másolhatóak, klónozhatóak percek alatt filléres, 50 dolláros eszközökkel.



Emellett látványosan demonstrálta, hogy **ahol nem külső forrásból ellenőrzik az egyes országok publikus kulcsait (PKD), hanem a saját magunk által aláírtat is elfogadják**, ott könnyedén lehet az előírásoknak és az ellenőrzésnek megfelelő hivatalos útlevele Elvis Prestley-nek vagy Keleti Tazannak Burkina Fasoból.



Második előadásában **Barta Csaba (Deloitte)** a **FireWire porton keresztüli támadásról** beszélt. A szakember a már ismert megoldást olyan módon alakította át, hogy **minden Windows verzió, sőt Linux alatt is működő képes lett, így segítségével megszerezhetővé vált a hőn áhított rendszerszintű jogosultság**.



További érdekesség, hogy a módszer segítségével nem csak a root jelszó, hanem a BitLocker recovery kulcs is elérhető lett a megtámadott számítógépből. Mivel ez csak bekapcsolt gépnél volt lehetséges, védekezőként a FireWire korlátozása, illetve a gépek távollétünkben való készenléti várakoztatása helyett a **biztonságosabb hibernálást vagy teljes kikapcsolást érdemesebb alkalmazni**, hiszen ekkor fizikai hozzáférés esetén nem lehetséges a fenti jelszólopási módszer. Érdekes volt az is, hogy akinek a gépén nincs IEEE1394 interfész, vagy kiöntötte azt műgyantával, az sem érezheti magát biztonságban, hiszen **elég egy PCMCIA foglalat és az abba dugható FireWire adapter**, máris reprodukálható a kísérlet.



Poén szinten már sokszor elhangzott a korábbi konferenciákon, hogy Amerikához képest mi milyen fejlettek vagyunk, lám nálunk "nulla" darab biztonsági incidens történik, mert hogy ennyiről számolnak be a cégek. Ezt az állóvizet próbálta most kicsit felkavarni **Keleti Artúr (KFKI)**. **Az etikus hackelési (természetesen fiktív, nem nevesített) tapasztalatok eddigi összképe alapján vázolt fel egy eléggé elkészerítő képet.**



A pentestek eredményeinek semmibevétele, admin/admin típusú jelszó, nagyfokú naívság a social engineering trükkökkel szemben, az ezt is kipipáltuk kérem a plecsnit hozzáálláson át igen gyakran előfordul, hogy **a jelzett gyenge pont kijavítása nem történik meg soha, vagy csak óriási időbeli késéssel**, de az is jellemző, hogy a javítás minőségben csak annyiban különbözik a korábbitól, hogy 15 perc helyett 20 perc kell a töréséhez. Nyilván nem várja el senki, hogy a megrendelők, a megbízó cégek atombiztos dolgokat vásároljanak, fejlesszenek ki csillagászati összegekért, de a tapasztalat szerint az elvárható gondoskodás mértéke sírnivalóan alulmarad az elvárhatótól. Nem is az új eszközökre szánt pénz hiányzik, hanem **sokkal inkább a meglévő dolgok helyes és szakszerű konfigurálása, beállítása vagy erős kívánnivalókat a cégek részéről.**



A szünet után az **Oracle biztonságról hallhattuk Tóth László (Deloitte) előadását**. Az Oracle fejlődése az évek folyamán egyre hatalmasabb programot eredményezett - ez a legfrissebb változatnál például már százezer feletti függvényt és 17 ezer globális változót jelent.



Egy általa felfedezett Remote Job Scheduling-ban talált sebezhetőséget demonstrált, amit a fehér kalap jegyében már a hivatalos hibajavítás elkészülte után mutatott csak be. Arról is hallhattunk, hogy az adatállományokban található **egyre értékeőbb vállalati adatvagyon miatt a sötét oldal egyre erőteljesebb érdeklődést mutat az úgynevezett adatbázis rootkit technika iránt**, ami az egyszer már sikeresen feltört adatbázisban való olyan manipulációt jelent, amely hosszútávon és rejtve biztosítja a támadóknak a folyamatos kikémlelési, hozzáférési lehetőséget.



A felhőkben való tárolásról, az abban kezelt adatok biztonságos voltáról hallhattuk **Lám Istvánt (ELTE)**, aki a **kriptográfiai fájlrendszereket hívta segítségül** annak demonstrálására, hogy ebben az irányban lehetséges kidolgozni olyan hatékony és rugalmas módszert, ami hosszú távon, **a felhasználók változása mellett is biztonságos csoportjogosultságokat képes biztosítani** harmadik fél bevonása nélkül.



Az általuk **Tresoriumnak nevezett eljárás kidolgozása és befejezése lehet a kulcs** mindehhez.



A mozi film (Tron:örökség 3D) előtt az ajándékok kisorsolása következett - ahol sajnos szomorúan konstatáltuk, sajnos mégsem mi nyertük meg a [mysec-es Androidos mobilt](#) ;-)





Zárásképpen a feszültség megfelelő levezetésről a már **szintén szokásosnak mondható helyszínen tartott [Buhera afterparty sörözés gondoskodott](#)**, ahol természetesen rendelkezésre állt minden szükséges kellék: alkoholos befolyásoltágú elágazó italkeverékek, zene, tánc, kitűnő széklábak :-)



8 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2900000>

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 antivírus már Mac-re is

2011.05.16. 11:05 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [macintosh](#) [osx](#) [hamis](#) [antivirus](#) [macdefender](#) [macprotector](#)

Ami késik, nem múlik - mormolták magukban a kártevőterjesztők, és mertek nagyot álmodni. És igen: a naiv jüzer már OS X alatt is kattinthat ilyenre.



Réges régen, mikor a hülyét még pontos jé-vel írták, csak [videokodeknek látszó trójai csomagok](#) csörgették láncukat **nagy néha Macintoshon**, később aztán a letöltések közé is korpa keveredett, és az **iWork, Photoshop telepítőcsomagok** is [résztvállaltak a kártevő terjesztésben, fertőzésben, sőt botnet hálózat építésben](#). Az igen ritka kártevős esetek közül olyan is volt, ahol viccesen vagy sem, de éppen **a figyelmetlen jüzer fogadja el a licenct**, hogy [az általa telepített játék random kockadobással letörölget néhány fájlt](#) a géperől.



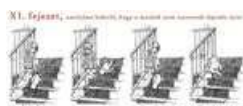
Régen jót mulattunk, mikor [az egy bites JavaScript mozi Linux vagy Mac alatt Windows DLL-ekben talált "veszélyes" fertőzéseket](#), de most úgy tűnik, végre valahára ;-) **külön OS X alá is készül ilyen hamis antivírus állatfajta**, testhezálló "Trojan.OSX.RSPug.C" és hasonló találatokkal.



Elméletileg bármilyen Google keresésből van esély, hogy ilyen találatokhoz jussunk, ahol aztán egy fertőzött oldara irányítva már egy testreszabott kis animáció jelenik meg, ó jaj, gépünk "fertőzött", de majd a jószágos MAC Defender, MAC Protector, MAC Ungabunga, stb. megvéd, kérjük a bankkártya számot.



Ha valaki valóban kíváncsi arra, **bújkál-e ismert rootkit a gépében**, [annak a chkroot](#) és az [rkhunter programot](#) ajánjuk, míg [ha valaki esetleg valódi antivirusban gondolkodik](#), annak is már egy széles palettáról van lehetősége választani: [ESET](#), Kasperky, Sophos, iAntivirus és társai.



Látható, hogy lassan, de [biztosan itt is próbálkoznak](#), érdemes tehát **figyelni, és itt is ésszel kattintgatni, telepítgetni**. Bár [klasszikus vírus veszély valóban nincs](#), azért a trójaiak egyre gyarapodó sisere hada [megkeserítheti majd a hétköznapijainkat](#).



6 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2907395>

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](#).



reconka • <http://www.reconka.info> 2011.05.16. 11:05:00

a leggyengébb láncszem a user..

Windows frissítés - ugyan kit érdekel?

2011.05.18. 11:11 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [windows statisztika](#) [frissítés](#) [biztonság](#) [felmérés](#) [sebezhetőség](#)

A magyar internetező nők 34%-a, a férfiaknak pedig 21%-a nem frissíti a Windows-t, mert nem ért hozzá, nem érdekli, vagy saját a bevallása szerint nincs rá lehetősége. Ők azok, akik hiába használnak vírusirtót, előbb-utóbb megfertőzik számítógépüket.



[Az ESET megbízásából készült piackutatás](#) az operációs rendszerek frissítését vizsgálta a magyar internetezők körében. Az eredmények szerint a felhasználók 27%-a, azaz **körülbelül 1.2 millió magyar internetező nem szokta frissíteni a Windows-át**. A nők 20%-a nyilatkozott úgy, hogy azért nem törődik a frissítésekkel, mert nem ért a kérdéshez, míg a férfiak közül a legtöbben (8%) azért nem telepítik a javításokat, **mert nem érdekli őket a dolog**.



"A válaszadók közül a legtöbben nincsenek tisztában azzal, hogy az operációs rendszerekben előfordulhatnak olyan lyukak, sérülékenységek, melyek segítségével a kártevők készítői kijátszhatják a biztonsági programok védelmét" - emelte ki Kiss Zoltán Gergő vírusvédelmi tanácsadó. A **vírusirtók akkor nyújtanak megfelelő védelmet, ha a felhasználók az operációs rendszerek frissítéseit is telepítik**.



A Windows **biztonsági hibáját** kihasználó kártevőkre példa [a magyarországi vírus toplistát régóta vezető Conficker féreg](#). A kártevő egy olyan sérülékenységen keresztül fertőz meg ma is havonta több tízezer számítógépet az országban, **melyre 2008 októberében létezik javítás**. A felhasználóknak meg kell érteniük, hogy a védelem hatékonyságát csökkenti, ha az operációs rendszer és az egyéb gyakran használt szoftverek biztonsági frissítései nincsenek telepítve.



A szoftvergyártók az elmúlt években rengeteget tettek azért, hogy a szükséges frissítések automatikusan települjenek a számítógépekre, de **ez sajnos csak akkor igaz, ha a felhasználó nem akadályozza meg a frissítés folyamatát**. Sokszor éppen azok az internetezők kapcsolják ki a frissítéseket, akik még mindig a Windows egy régebbi, feltört verzióját használják.



Persze közben nem árt észben tartani azt is, hogy a [Windows frissítés sosem érkezik kéretlen e-mail mellékleteként](#).



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2911610>

Kommentek:

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

[tsimike 2011.05.18. 12:45:26](#)

Nem tudom nekem automatikus letöltésre van állítva manuális telepítéssel. Mit kell ehhez érteni? Letölti és szól ha frissítés van. Rákattintok a Telepítésre és minden további beavatkozás nélkül megy minden.

Könnyed előzés az élvezőnyben

2011.05.20. 10:10 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [magyar adatok nod32 eset havi threatsense vírusstatisztika](#)

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



Megtört a 2009. októbere óta tartó folyamatos uralom, és **tizennyolc hónap után átadta trónját a Conficker féreg**. Ebben a hónapban ugyanis **az Autorun vírus törte a legtöbb borsot a felhasználók orra alá**. Bár a trójaiak magas aránya továbbra sem csökkent - még mindig heten vannak a tízes listában - a Conficker féreg azonban mégis búcsút inthetett korábbi "bérelt" első helyének, és cserélt a régóta örök második Autorun vírussal. A bűnözők előszeretettel építenek arra, hogy **a legtöbb felhasználó kényelemből nem tiltja le az automatikus futtatást** a Windows operációs rendszerek alatt. Emellett persze az sem elhanyagolható szempont, hogy **a Conficker féreg egyik fertőzési módszere is éppen az Autorun**.

A hordozható médiákon egyre rafináltabban és kifinomultabb módszerekkel terjedő Autorunos kártevők igen sok kárt képesek okozni, ezért [a NOD32, illetve ESET Smart Security következő, 5-ös verziójában](#) kiemelt figyelmet szentelnek majd a fejlesztők e terület hatékonyabb ellenőrzésére is, így a cserélhető USB eszközök, CD illetve DVD lemezek vizsgálata még **a korábbiaknál is részletesebben beállítható, illetve blokkolható lesz**.



A fenti sorrend cserén kívül **egyetlen újonc kártevőt köszönhetünk a toplistában, ez pedig a JS/Redirector trójai**. Ez egy olyan kártékony JavaScript, amely lefutva kéréslen böngésző ablakokat jelenít meg, emellett hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról. Előző havi statisztikánkban is utaltunk már arra, hogy internetböngészőnk biztonsági beállításait érdemes időnként felülvizsgálni, valamint a weblapok látogatása alkalmával automatikusan lefutó, és esetlegesen [kártékony JavaScript kódok ellen megfelelő külön beépülővel](#) (pluginnek) is érdemes kiegészíteni webes védelmünket.

Összességében elmondhatjuk, **a trójai programok túlsúlya egy komoly figyelmeztetés, hogy a böngészés és az új programok telepítése mennyire fontos és kritikus** területe a számítógépes biztonságunknak. Ezenkívül a hordozható meghajtók is kiemelt veszélyforrást jelenthetnek, így a naprakész antivírus mellett a naprakész Windows javító foltok megléte is kiemelt jelentőségű, valamint a külső adathordozók automatikus indulását is érdemes letiltani saját biztonságunk érdekében. Természetesen gyanakvásunkat továbbra se dobjuk sutba, és ne hagyjuk magunkat megtéveszteni, kecsgetessen a [kéretlen levélmelléklet vagy kéretlen link akár Vilmos herceg és Kate Middleton esküvőjével](#), vagy akár Osama Bin Laden halálának állítólagos videójával.



Az ESET több százezer magyarországi felhasználó visszajelzése alapján statisztikai rendszere szerint **2011 áprilisában a következő 10 károkozó terjedt a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 21.08%-ért.



1. INF/Autorun vírus

Elterjedtsége az áprilisi fertőzések között: **5.08%**

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.



A számítógépre kerülés módja: Fertőzött adathordozókon (akár MP3-lejátszókon) terjed.

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



2. Win32/Conficker féreg

Elterjedtsége az áprilisi fertőzések között: 4.68%

Előző havi helyezés: 1.

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 eljárshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárson 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.



A számítógépre kerülés módja: 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. JS/Redirector trójai

Elterjedtsége az áprilisi fertőzések között: 2.48%

Előző havi helyezés: -

Működés: A JS/Redirector trójai egy olyan kártékony JavaScript, amely lefutva kényszeríti a böngésző ablakokat jelenít meg, emellett hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21redirector>



4. Win32/PSW.OnLineGames trójai

Elterjedtsége az áprilisi fertőzések között: 1.99%

Előző havi helyezés: 3.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományait és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatokat titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



5. Win32/HackMS trójai

Elterjedtsége az áprilisi fertőzések között: 1.86%

Előző havi helyezés: 5.

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program

telepítésekor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>



6. Win32/VB féreg

Elterjedtsége az áprilisi fertőzések között: 1.32%

Előző havi helyezés: 6.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



7. Win32/Shutdowner trójai

Elterjedtsége az áprilisi fertőzések között: 1.27%

Előző havi helyezés: 7.

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>



8. Win32/Tifaut trójai

Elterjedtsége az áprilisi fertőzések között: 0.96%

Előző havi helyezés: 8.

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csrsc.exe és autorun.inf néven. A kártékony EXE fájl automatikus lefuttatásához külön bejegyzést is készít a rendszerleíró-adatbázisban. Működése során több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21tifaut>



9. Win32/RegistryBooster trójai

Elterjedtsége az áprilisi fertőzések között: 0.75%

Előző havi helyezés: 9.

Működés: A Win32/RegistryBooster alkalmazás a hamis antivírus programokhoz hasonlóan hamis riasztásokkal igyekszik rábeszélni a felhasználókat a „program” fizetős változatának megvásárlására.



A számítógépre kerülés módja: Fertőzött weboldalról települ, vagy a felhasználó maga telepíti.

Bővebb információ:

<http://www.eset.hu/tamogatas/viruslabor/virusleirasok/registrybooster>



10. HTML/ScrInject trójai

Elterjedtsége az áprilisi fertőzések között: 0.69%

Előző havi helyezés: 10.

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

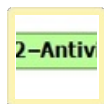
- [Majdnem mindenki átverhető adathalászzal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Safe mód a Mechagodzilla ellen](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2914957>

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](#).



www.nod32-antivirus.hu • <http://www.nod32-antivirus.hu>
2011.06.01. 10:04:07

Nagyon tetszik az oldal, csak Így tovább. Ha ingyenes demó vírusírtó, antivírus kellene, olcsó, akciós áron, akkor nézzétek meg a weboldalamat. www.nod32-antivirus.hu

Chello UPC karbantartás

2011.05.23. 15:10 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [spam upc chello](#) [adathalászat](#) [malájzia](#)

"Miután karbantartás folyik a szerverek, mi jelenleg korszerűsítés adatbázisunkban", ezért most kérjük a nevedet, jelszavadat és a születési adataidat, hehe.



Csak reménykedünk, hogy egy ennyire szimplán fatengelyes, átlátszó trükknek már senki nem dőlhet be. Ismerősünk jelezte, kapott ilyet, és **mivel valóban UPC Chello ügyfél, meglepődött nem kicsit**, vajon honnan tudhatták a címét. Azért a szanaszét **szórt cirill karakterek** jócskán elvesznek a levél sportértékéből, így csak másfél Michelin csillagot érdemelhet a szőrös szívű zsűritől maximum ;-)



Ezúttal valószínűleg maga **Szandokan, a maláji tigris állhat a háttérben**, neki mondhatta tollba a szöveget Fülíg Jimmy és Arkagyij Rajkin, legalábbis az email cím fejlécében talált adatok tanúsága alapján. **Íme a roppant hiteles levél:**



"Kedves e-mail előfizetők

Miután karbantartás folyik a szerverek, mi jelenleg korszerűsítés adatbázisunkban. Ahhoz, hogy elérhető legyen szoros az e-mail fiókot, kérjük, frissítse az alábbiakban.

Megerősítette az e-mail fiókot

Felhasználónév :.....

Jelszó :.....

Születésnap :.....

Ország :.....

Köszönjük chello.hu!

Biztonságos szolgáltatás"

Netes keresésünk eredménye **nem csak azt mutatta meg, ezt a trükköt már máshol is elsütötték egy holland (UPC székhelye) levélta tanúsága szerint**, hanem az is kiderült, a korábbi verziók közül a 2010-es spameresztés levele sokkal furmányosabb volt, **ott egyenesen vírus fertőzésre hivatkozva kérték be az ügyfelektől az adataikat, jelszavaikat**.



Ott még az is vicces, hogy megnyugtadják a naív ügyfelet, adja meg bátran jelszavát, az majd úgyis **1024 bites RSA kulccsal lesz kódolva**. Közben meg **clear textben utazik** a levélben, a csalóknak címezve :-)



Fel kellene tűnnie alaphangon mindenki számára, hogy hát **milyen szolgáltató az ilyen, aki még ezeket az adatokat is tőlünk kéri be, normális ez, hihető ez?** Remélhetőleg ma már senki számára nem igazán.



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Tízből öt kártevő hátsóajtót nyit](#)
- ["Szösölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2925735>

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](#).



[upc on-line](#) • <http://www.upc.hu> 2011.05.23. 15:15:24

Kedves István,

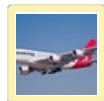
szeretnénk kivizsgálni a blog bejegyzésedben bemutatott visszaélési kísérletet, ehhez azonban szükségünk lenne az eredeti adathalász levélre, melyet csatolva elküldhetsz nekünk a abuse@upcmail.hu email címünkre. Segítséged előre is köszönjük!



[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu> 2011.05.23. 16:43:21

Udv!

Elküldtem akkor a jelzett címre.



[thepret](#) • <http://teneriferepulojegys.hu/> 2011.05.23. 23:55:48

Ezeket még kajolja vki?

Apple frissítés Mac Defender ellen

2011.05.25. 14:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [mac](#) [apple](#) [frissítés](#) [malware](#) [hamis](#) [trójai](#) [antivírus](#) [defender](#)

Ezt is megértük, biztonsági frissítést ad ki az Apple hamis vírus trójaiak ellen. A [Mac Defender](#), [Mac Protector](#), [Mac Security](#) nevű programok miatt a support is több segítségkérést kap, és ezek eltávolításával kapcsolatban egy knowledgebase bejegyzés is született már a weboldalukon.



Ami [remélhetőleg](#) sokáig ott marad a 2008-as vírus program használatával kapcsolatos emlékeztető bejegyzéssel szemben ;-). A bejegyzés lépésről lépésre részletesen leírja, hogyan lehet eltávolítani a rendszerből a megtévesztő trójait.



A tervezett [frissítés pedig eltávolítja a számítógépen jelenlevő esetleges kártevőt](#), illetve állítólag arra is képes lesz, hogy a jövőben felugró ablakban [figyelmeztessen majd az incidensnél](#).



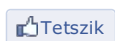
Nyilvánvalóan a megtévesztéses social engineering az egyik legkomolyabb támadási forma, és a felhasználóknak a legkülönbözőbb ténykedéseknél kell "ésszerű lenni", legyen az [állítólagosan hiányzó video kodek](#), kétes iWork trójai csomag letöltése, kéretlen email nyitogatás, megmondom ki törölt a Facebookon App telepítése, mérgezett Google Image találatok böngészése, [szimpla tárgyú figyelmeztetés](#) vagy bármi egyéb korszerű brejzli. Ma már szerencsére [szinte mindegyik vírus cég megjelent a Macs megoldásával](#), és jelen van vele az Apple Store-ban, így aki akar, tud miből választani.



Összefoglalva: [változni látszik a helyzet](#), már [vannak apró szurkák](#), szervezetnek tűnő próbálkozások az alternatív platformok területén is. Figyelni és [őrt állítani platformfüggetlenül](#) sosem értelmetlen, [amíg mindannyian ugyanazt a netet nézzük](#). Lehet, hogy az egyre sikeresebb és mind szélesebb körben elterjedtebb Mac lassan közeledik ahhoz a kritikus méretű tortaszelethez, ami héba-hóba [bekapcsolja](#) majd őket ebbe a "vérkeringésbe".



Természetesen nem riogatás vagy főcímvadászat akar ez lenni, hanem inkább csak figyelemfelhívás. [Az egyáltalán nem sebezhetetlen OS X](#) és a Linux pedig [még mindig egy idális mennyi hely](#) a Windowshoz és az ő százmillió kártevő mennyiségéhez képest. A [biztonság elhanyagolása vagy gőgös lekicsinylése](#) azonban mindig képes fájón megbosszulni magát.



4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:



- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2931035>

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.

Belül Chrome, kívül nikkel...

2011.05.27. 13:30 | [Csizmazia István \[Rambo\]](#) | [48 komment](#)

Címkék: [google játék böngésző telepítés felhasználói chrome adatszivárgás jogsértő](#)

Vigyázni kell! Ezzel az elpuskázott, [napi borzasztó szöviccet](#) megszegeyentő fűzfapoétás kétsorossal indítjuk ezt a posztot, amely a Chrome böngészőben futó egyes alkalmazások napvilágot látott "érdekességeiről" fog szólni.



Egy [David Roger](#) nevezetű úriember adta közre azt a [felfedezését](#), miszerint kipróbálta a **Chrome böngészője alatt a Chrome Web Storeból letölthető Super Marioworld Flash 2** nevű ingyenes játékot - amit már mellesleg tizenháromezren letöltöttek - és a nagy meglepetéstől egy orbitális méretű WTF tolt az ajkára a képernyő jobb alsó sarkában található **"this app needs to open a tab so we're going to allow it to access your entire browsing history."** felirat láttán. **"Ez vajon minek is kell, hozzáférés egy kutya-közönséges flash játék számára? Persze, jól tudjuk, bizonyára csak a mi érdekünkben, mindössze a ["felhasználói élmény fokozása"](#) céljából;-)**



Az biztos, hogy mind egy **"Access all data on your computer..." kezdetű mondat**, mind a vele települni szándékozó NPAPI is kevésbé tetszetős számunkra. Az mindenesetre érdekes lehet, amint egy mukinyulus flashjáték **nem csak hogy olvassa, hanem mondjuk meg is organizálja az eddig pályafutásunk során begyűjtött összes könyvjelzőnket :-)** A bejegyzésből az is kiderül, az ilyen Chrome webstore appholmik eltávolítása **sem mindig pofonegyszerű, ha az átlag felhasználóra gondolunk**, bár természetesen azért megoldható a lépés a settings->tools->extensions segítségével.



Emlékeztet, vagy mondhatjuk Safranek nevében, hogy "mint az közismert", a Chrome böngésző indulása is egy érdekes sztori volt a maga nemében, ugyanis a licencében az szerepelt, hogy **"minden adatunk, ami a böngészőn áthalad, a cég tulajdonába kerül, és a Google-nek joga van felhasználni, publikálni, lefordítani, módosítani, és nagyjából bármit megtenni vele, amit a kedve tart"**. Volt is belőle felháborodás, ami után szerencsére igen rövid időn belül az inkriminált passzus eltűnődött a felhasználói szerződésből.



Azt is érdemes lesz figyelemmel kísérni, hogy a böngészőháborúban [ki mit lép majd a biztonságot nagyon is érintő címsor link alapértelmezés szerinti eltüntetéses divatmajmolásban](#). Aki visszatérő olvasó, az emlékezhet, amikor az okostelefonok korlátozott méretű kijelzőjének URL rövidítési, elrejtési problémájáról írtunk, ott és akkor azt láthattuk, a biztonsági szakértő [sikeresen megmanipulálta a weboldalt, ami látszólag a Bank of America volt, a valóságban meg akármilyen](#). Persze az asztali PC-n ennél azért még mindig jobb a helyzet a vírusvédelem, tűzfal, meg a biztonságot szolgáló rendes browserpluginek miatt, de azért [a teljesen biztonságos böngészés így is csak illúzió](#).



[Visszatérve az alaptémánkra](#) mindenesetre jó kérdés, hogy biztonsági megfontolásból minek szavazunk majd bizalmat: a [böngészőben futó ismeretlen mellékhatású "ingyenes" játékoknak](#), vagy inkább az [atombiztos, Windows, Linux és Mac alatt egyaránt elkettyegő DOSBox](#) alatt futó régi játékoknak. Emellett legyen szó PC-ről, vagy okostelefonról, [érdemes jól átgondolni, pontosan mire is adunk vagy nem adunk engedélyt](#) egy alkalmazás telepítésekor. Dnet fogalmazott valahogy úgy: **"Ha például egy Android app telepítésekor jóváhagyjuk, hogy az SMS-eket küldjön, akkor nem túl praktikus dolog meglepődni azon, amikor az aztán tényleg SMS-eket fog küldeni."**



[Az említett jogsértő alkalmazást](#) mindenesetre már tegnap sem találtuk meg az interneten, **azóta szemlátomást eltávolították**, emiatt a webstore képernyőképet is már csak a Google cache-be történt időutazás segítségével tudtuk elkészíteni.



12 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

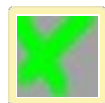
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2936226>

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/> **2011.05.28. 10:27:28**

Pont ezért KELL elolvasni a telepítés közben felbukkano szöveget, hogy ne erjen meglepetes minket később.

[Kuruttya 2011.05.28. 10:32:35](#)

"címsor link alapértelmezés szerinti eltüntetési divatmajmolásban"

Egyelőre kizárólag a Chrome dev csatornájában megjelenő, ott is a "rejtett" beállításokban csak kézzel bekapcsolható dologról van szó. Ezt talán még egy kicsit korai divatnak nevezni. A Google már mondta párszor, hogy a Chrome dev csatorna azért van, hogy játszanak vele, próbálgassák a dolgokat, aztán hogy mi kerül be onnan a stabilba, az még egyáltalán nem egyértelmű. Elég valószínű, hogy a Google alkalmazottai sem hülyék, ha lesz is valaha alapértelmezésben elrejtett URL bar a stabil Chrome-ban, bizonyára kitalálnak valamit, hogy a biztonságot ne befolyásolja.

Egyébként hasonló lépés volt annak idején a "http://" eltüntetése a címek előtt. Eleinte emiatt is károgtak páran, aztán kiderült hogy nem származik belőle semmi probléma.

[tyberius 2011.05.28. 10:57:24](#)

@Álmos: Azt azért ne feledd, hogy erősen konvergálnak a böngészők, amit az egyik kitalál, azt rövid időn belül az összes többi is lemásolja. Nem lepődnék meg, ha egy főverzió múlva az összes népszerű böngészőben benne lenne ez az opció, egyesekben alapbeállításként.

Én mondjuk nem szeretem, ha hülyének néz a böngésző, amint eltüntették a hőtötöpöt, az első dolgom volt, hogy visszakapcsoljam, és akkor is így fogok tenni, ha az egész URL mezőt akarják elrejtetni előlem.

[Kuruttya 2011.05.28. 11:03:42](#)

[@tyberius](#): ha jól tudom a Firefox fejlesztői azt nyilatkozták, hogy ők nem szándékoznak ilyesmit csinálni. Mondjuk ha bejön a Chrome-nak, akkor valószínűleg fognak. No és? Meg lehet ezt úgy oldani, hogy ne legyenek biztonsági implikációi.

A http eltüntetése miért hülyének nézés? Ezt abszolút nem tudom értelmezni. Nekem tetszik, hogy nincs ott feleslegesen, semmilyen plusz információt nem ad.

passaran 2011.05.28. 11:14:26

Nekem egyáltalán nem tetszik ez a pár hetente új főverzió kiadási irány. Lényegében sima parasztvakítás csak és nekem úgy tűnik arra megy a játék, hogy az IE-t beelőzzék és elhitelessék az userekkel, hogy pl. az IE9 elavult mert can már Chrome 12 is. Év végére lesz FF10 is simán.

Ráadásul a "tüntessünk el minden kiegészítő infót a képernyőről" is elég vakvágánynak tűnik az átlag usernek több problémát fog okozni hosszú távon, mint előnyt. Az adathalászok meg már bontják a pezsgőt örömlükben :(

Kuruttya 2011.05.28. 11:20:07

[@exonka](#): "Lényegében sima parasztvakítás"

Nézd meg a changelogot. Történnék ott fejlesztések. :)

"arra megy a játék, hogy az IE-t beelőzzék"

Akit egy icipicit is érdekel, hogy milyen böngészőt használ, az már régesrég hozzá sem nyúl az IE-hez. Aki meg a főverziószám nagysága alapján dönti el, hogy egy böngésző mennyire jó... :D

chabusch 2011.05.28. 11:47:59

Ami még érdekes, az az Android Marketen található alkalmazások engedélyezése. Van pl. a Multiling keyboard, minden engedélye elfogadható. A keyboard mellé le kell tölteni a nyelvi pluginokat, azok nem kérnek engedélyt.

Települ a keyboard és a plugin, majd kiderül, hogy a plugin mégis kap engedélyt, read phone state-t és modify sd card content-t. Így pedig már a keyboard és a plugin együtt hozzáfér a személyes adatokhoz.

atila68 (törölt) 2011.05.28. 12:24:10

Az milyen mikor a google (gmail, picassa) profilomban turkálva, egyszer csak elémtáru a teljes böngészési előzmények lista (függetlenül attól, hogy valaha töröltem e avagy sem), mióta feltelepítettem az aktuális böngészőm (Firefox 3.6. - a 4 feszt összeomlik nálam), és udvariasan érdeklődik a google, hogy kívánom e ignorálni ezt a 'szolgáltatást'?

No nálam itt ugrott ki egy "Mikurvanyád!" a számon.

Bambano 2011.05.28. 12:25:25

aki krómot használ, sikeres nem lehet...

- Rendi - 2011.05.28. 12:31:47

[@Bambano](#): Valamivel meg is tudod indokolni, vagy csak idebőfögtél valamit?

sztatty 2011.05.28. 12:34:44

[@Bambano](#): Aki nem krómot használ sikeres nem lehet...

+ egy katica is megverne egy iq teszten, neki legalább lenne 7 pontja.

dozen 2011.05.28. 12:47:52

ne keverjük a szezon a fazonnal.

chromium = nyílt forráskódú böngésző

chrome = google saját képére formát chromium böngészője

egy összehasonlítás:

www.srware.net/en/software_srware_iron_chrome_vs_iron.php

Bambano 2011.05.28. 12:48:35

@- Rendi -: chrome=google. a google adatkezelési szabályai hajmeresztőek. azok a szabályok, amiket meg elsőre be akartak vezetni, még inkább rosszak voltak, szerencsére elsöpörte őket a népharag.

Az ilyen adatrabló cégektől kiráz a hideg. De nem csak engem, jónéhány hivatalos embert is. Hogy csak a streetview autók körüli disznóságokra célozzak.

@sztatty: a katica jó. a katica nem él át adatvédelmi problémákat.

Kuruttya 2011.05.28. 12:50:57

@chabusch: minden app, ami 1.6 előtti API támogatást jelöl meg a menifestben automatikusan megkapja a rendszertől a "read phone state" és a "modify sd card content" jogosultságokat. Ez azért van, mert egészen az 1.5-os verzióig ezek nem voltak külön kezelhető jogosultságok, automatikusan járt minden appnak. Ahhoz, hogy a legújabb Android is visszafelé kompatibilis legyen muszáj volt a régi API-t használó alkalmazásoknak továbbra is automatikusan biztosítani ezeket.

Abban igazad van, hogy jobb lenne ha a market is tudna erről, és ezeket is kiírná neked, hogy ne legyenek félreértések.

arch 2011.05.28. 13:06:46

Nem használok Chrome-ot, de néha kíváncsi voltam hol tartanak a fejlesztésben. Ekkor jött szembe az Iron:

www.srware.net/en/software_srware_iron_chrome_vs_iron.php

Van win/mac/linux kiadás is. Próbálta valaki az Iron-t?

arch 2011.05.28. 13:14:29

@dozen:

Iron vonatkozásban megelőztél :)

Ne keverjük: a chromium, a chrome és az iron az három dolog, valójában csak kettő. Csak az iron mentes a google kedves adatrabló szolgáltatásaitól.



Epokit Drive 2011.05.28. 13:53:42

Egy tipp, nem tudom, tud-e vki többet róla: SRWare Iron 10.x.x portable böngésző. Ezt használok e percben is, teljesen mint a Chrome, csak nem települ, és állítólag nem küldözget semmit a Guglinak, lévén NEM a Guglié, ellentétben a Chrome-mal, ami ugyan szintén OpenSource-alapú, de mégiscsak hozzátesznek ezt-azt.

Vélemény?



Epokit Drive 2011.05.28. 13:54:21

A "böngésző" természetesen brózer lett volna, bocs.



Epokit Drive 2011.05.28. 13:59:39

Az Iron most itt tart: 11.0.700.2

(Ha már ajánlottam, frissítettem is, május 6-i a legfrissebb. Ez is portable, természetesen.)

Kuruttya 2011.05.28. 14:29:59

@Epokit Drive: az én véleményem az, hogy az adatvédelem úgy általában egy túllihegett álprobléma, és ha szerinted a Chrome mint böngésző jó, akkor leginkább a Google féle verziót érdemes használni, felesleges ilyen Iron-okkal pöcsölni.

(Gy.k. a Google belőlünk él, tehát elemi érdeke hogy a rólunk gyűjtött adatokat olyan dolgokra használja fel, ami végeredményben nekünk lesz jó. Lásd suggest, UI optimalizálások, stb. Ha megtagadod az adatok megadását, vagy mégrosszabb meghamisítod őket, azzal a felhasználóknak ártasz végsősoron.)

powerage 2011.05.28. 14:49:43

[@Álmos](#):

"az én véleményem az, hogy az adatvédelem úgy általában egy túllihegett álprobléma"

"Ha megtagadod az adatok megadását, vagy mégrosszabb meghamisítod őket, azzal a felhasználóknak ártasz végsősoron."

Wow. Csak én találok ijesztően elbaszottnak ezt a hozzáállást?

Kuruttya 2011.05.28. 14:51:10

[@powerage](#): nem, van egy hangos kisebbség aki szereti hisztizni emiatt :) De ha gondold leírhatnád, hogy mi a bajod vele.

powerage 2011.05.28. 15:50:09

[@Álmos](#):

"De ha gondold leírhatnád, hogy mi a bajod vele. "

Felesleges.

Inkább arra kémelek, írd már meg ide a személyes adataidat. (Név, cím, mailcím, telefonszám, útlevekszám, adóazonosító jel, bankkártyaszám stb)

Ha ezzel nincs gondod, akkor elhiszem, hogy komolyan gondold az adatvédelem túllihegettségét.

Kuruttya 2011.05.28. 15:52:56

[@powerage](#): nyilvánvalóan te is tisztában vagy vele, hogy nem erről van szó :) De ha nincsenek érvek, hát nincsenek.

Bambano 2011.05.28. 16:04:52

[@powerage](#): nem.

Kuruttya 2011.05.28. 16:31:19

[@Bambano](#): te is csak vagdalkozol itt az adatrablással, de hogy ez pontosan kinek rossz és miért, arról nem sikerült még nyilatkozni.

Bambano 2011.05.28. 16:50:38

[@Álmos](#): alapvetően evidenciákat, axiómákat nem szoktak magyarázni.

Miért nem jó az, hogy mindenféle hivatalok és magánszervezetek kotorásznak az adataimban?

Miért nem jó az, hogy gyakorlatilag bárki összegereblyézhet egy csomó terhelő adatokat azokról, akik erre nem figyelnek oda?

Miért nem jó adathörcsögök pofájába tolni a bankkártya adataimat?

Miért nem jó, ha pártok, kormányon és ellenzékben, ideológiai harcok megvívására alkalmas adatbázisokat építenek?

Miért nem jó, hogy a streetview autók email részleteket, esetleg komplett emaileket is összegereblyéztek?

Miért nem jó, hogy azt a mocskok fészbukot akkor sem tudod kikerülni, ha nem vagy rá regisztrálva?

Miért nem jó, hogy hivatalos célból megadott email címedet bankok spammelik?

Miért nem jó, hogy a bíróságnak kell szétpofoznia a microsoftot, hogy ugyan árulja már el, hogy milyen adatokat lopkodott össze a jüzereikről?

Az ég kék, a fű zöld, a windows lerohad. Evidenciákat nem magyarázunk. Sosem tudhatod előre, mikor ki milyen módon fordítja ellened, amit rólad talál a neten. Akár a gugli, akár a cia, akár egy pszichopata. Na nem mintha olyan élesek lennének ezen halmazok között a határok...

Bambano 2011.05.28. 16:51:37

[@Álmos](#): arról, hogy pontosan kinek rossz, szerintem sikerült már nyilatkozni, lehet, hogy túl burkoltan. NEKEM rossz.

Egyébként is: ha valaki pénzt csinál abból, ami az én tulajdonom, akkor jutalékot akarok.

mughuzu565 • <http://kerdesek.hu> 2011.05.28. 17:16:11

jaja no comment...

Kuruttya 2011.05.28. 17:17:19

[@Bambano](#): az élet sok nagy felfedezése származott az axiómának gondolt dolgok megkérdőjelezéséből :)

Néhány apróság:

-Ami adatot "bárki" összegerebléyzhet valakiról, arról nem a Google tehet, ők nem tesznek közzé gyűjtött adatokat. Ha te beposztolod Twitterre, hogy mikor nem leszel otthon, és emiatt kirabolnak, akkor TE vagy a hülye, nem a Twitter.

-Megbízható cégeknek (Google, PayPal, Amazon) megadott bankkártya adatokkal még nem történt sose a cégek részéről szándékos visszaélés. Azt meg gondolom tudod, hogy a sarki kisboltban is megbuherálhatják azt a leolvasót.

-Igen, a streetview autók wifi forgalmat rögzítettek is, amit a Google (GPS nélküli) location adatbázisának pontosítására használtak. Ez ugye a felhasználónak jó, mert javul a location szolgáltatás minősége. Ezzel kapcsolatban: 1. Az összes Androidos telefon rögzít és küld a környező wifikról adatot a Googlenek. (És ez jó.) 2. Aki nem titkosítja a wifijét, annak bárki belenézhet a forgalmába, erről nem a Google tehet.

-Hogy ne tudnád kikerülni a Facebookot? Nem kötelező lájkolni meg kommentelni.

-Nekem még sosem érkezett banktól olyan spam, amit a szűrő ne fogott volna meg.

A többi amit írtál ("magánszervezetek kotorásznak az adataimban", "ideológiai harcok megvívására alkalmas adatbázisok") alaptalan pletykák csupán. Ha van valami konkrét bizonyítékod akkor muti, egyébként felesleges leírnod.

Továbbá, ha fejlesztettél az elmúlt 10 évben bármilyen végfelhasználói web, mobil, vagy asztali alkalmazást akkor tudhatod, hogy a fejlesztő számára az egyik legértékesebb kincs a felhasználóktól gyűjtött adat. Végtelenül megkönnyíti a hibakeresést, ha minden crash után normális reportot küld az alkalmazás. Ha tudod, hogy az emberek mit néznek, mennyi ideig, honnan jönnek, akkor optimalizálni tudod a tartalmat és a felhasználó felületet. És igen, azt is optimalizálhatod, hogy hova érdemes rakni a hirdetést, hogy a felhasználó a legtöbbet kattintson rá, de ugye bevétel nélkül szolgáltatás sem lenne.

Ezek olyan gonosz dolgok lennének? Ma már minden weboldalon ott figyel a Google Analytics (természetesen itt is...), ami folyamatosan gyűjti rólad az adatot ebben a pillanatban is. Emiatt valahogy mégsem kárognak az emberek. Miért lenne más (hogy az eredeti témához visszatérjünk) a Chrome adatgyűjtése?

Végül: én minden végfelhasználói termékemet telepakolom adatgyűjtő részekkel. Gonosz vagyok-e?

namkuzu 2011.05.28. 18:44:51

Elég szomorú, hogy egyesek szerint az adatvédelem álprobléma.

Senkinek semmi köze azokhoz az adatokhoz, amiket a gépemen tartok, azok az én magántulajdonomat/szellemi termékeimet stb képzik, a sok idióta meg itt élteti ezt az elbaszott online CIA-t, ami a google-facebook usw.

Nem annyira ide tartozik, de a facebook állítólag azzal a szöveggel gyűjti a nem regisztrált netezőkről az adatokat, hogy milyen jó lesz majd nekik ha regisztrálnak, mert micsoda személyreszabott élmény lesz...

ÉS EZ KI A FASZNAK JÓ?!

Bambano 2011.05.28. 21:42:36

[@Álmos](#): néhány apróság:

- a gugli docs első felhasználói szerződése úgy szólt, hogy amit a gugli docsba beírsz, az a guglié. Utána néztek nagy kerek szemekkel, hogy a népek elküldték őket a picsába.

- nem tudhatod, hogy miket gyűjt a gugli és mit tesz közzé. azt sem tudhattad, hogy a streetview autók wifi adatokat gyűjtenek.

- sosem tudhatod, hogy a gugli milyen hatóságoknak adja ki azokat az adatokat, amiket nem amcsi felségterületen gyűjtött, tehát nyugodtan tojhatnak az összes törvényre.

- mit is mondott nemrég egy titkosszolgá? hogy mennyire örülnek annak, hogy a népek elvégzik helyettük a munkát? ez nekem miért jó?

- megbízható cégeknél még sosem történt semmi a bankkártyákkal? ezt le mered írni egy olyan időszakban, amikor a sony hálózatait hetek óta folyamatosan felborogatják a crackerek? persze így könnyű vitázni, hogy a világ hírei nem jutnak el hozzád, de akkor nem a valódi világban élsz. és a sony csak egy példa, nem ők az egyetlenek, akik veszítettek már el hitelkártya adatot... amit ember titkosít, azt ember fel is töri. ergo ne gyűjtsön semmit, mert nem lehet garantálni, hogy az nála marad.

- ugye tudod (volt róla hír mértékadó internetes lapokon), hogy a facebook akkor is nyomon követi a tevékenységedet a lájkoló gombon keresztül, ha nem vagy facebook tag? miféle mocskos szemét rablás már ez, hogy nem jelentkezek be és mégis adatot gyűjt rólam?

- a gugli sem borogatta ki a teljes kapcsolatrendszeredet mindenki számára a buzzon vagy min keresztül... ahha. tehát ki mered jelenteni, hogy a gugli meg a facebook programozók soha nem fognak tévedni és soha nem fog infó szivárogni programozási hiba miatt? naiv lennél, ha megtennéd

- te még nem jártál úgy, hogy valamelyik asshole ismerősöd úgy regisztrált a facebookra, hogy megadta a postafiókjai elérési adatait is és a facebook rögtön leszívta az összes email címet belőle? Én pl. így került be a nagy facebookos adatdarálóba, és hetekig kellett küzdenem, hogy az a fos facebook ne küldözzessen folyamatosan mindenféle feliratkozási emaileket. Elmennek az anyjukba azok, akik a saját ostobaságukkal nekem ekkora bajt okoznak. Ne mondd, hogy ez nem facebook probléma, mert ők programozták, nem az a hülye, aki regisztrál rá.

- arról nem a google tehet, hogy felkerültek a wifi antennák a kocsira? ne már. valamelyik autópálya felüljáróról hajigálták rá a streetview kocsikra az antennákat, vagy hogy? Ja és a notebookba is csak úgy beszivárgott az a programkód, ami bekapcsolta az antennához tartozó wifi rádiót és elkezdte snoopolni a hálózatot és lerakta a teljes forgalmat. Ezek mind valami intergalaktikus véletlen részei és nem a google rakta oda, szándékosan.

- és nem a google az a cég, amelyik nem hajlandó rendesen végrehajtani azokat az utasításokat, miszerint törölje az illegálisan szerzett streetview adatokat? bizonyítandó, hogy jogkövető magatartást akarnak nyújtani?

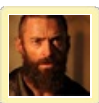
- ideológiai harcokra alkalmas adatbázis az összes pártokkal kapcsolatban elkövetett népi konzultáció és hasonlók. mind a két nagy párt arra használta fel a különböző ilyen megmozdulásokat, hogy adatbázist építsen a szavazókról, akiket később meg lehet támadni politikai hirdetésekkel. Nem véletlenül vonták be a mostani fülkeforradalmas össznépi konzultációba a 16 éveseket is, akikből a következő kanyarban már választópolgár lesz. jóreggelt. Olvass blogokat, erről is volt szó nemrégiben.

- az pedig, hogy a gugli helymeghatározója milyen pontos, ki a francot érdekel? engem nem. És az is életszerűtlen, hogy egy montanai porfészekben lakó usákoknak fontos az, hogy az én wifimnek tudják a helyét. Valami igen erősen azt súgja nekem, hogy Joe bácsit qrvára nem érdekli, hogy mi van itt nálam. És ez kölcsönös.

webes alkalmazást már fejlesztettem, de én nem szoktam crasht belefejleszteni. és szögezzük le, hogy teljesen más dolog az, hogy amikor összeomlik egy alkalmazás (rotfl, ilyet is csak a microsoft szemetjei óta tűrünk el, hogy alkalmazás összeomolhasson, előtte sosem volt ilyen), akkor feltesz egy kérdést a rendszer, hogy küldhet-e bugreportot és ha azt válaszolod, hogy igen, akkor küld, mint az, hogy a hátad mögött, az előzetes megkérdézésed nélkül olyan adatokat is küld, aminek semmi köze a tevékenységedhez, mindezt üzemszerűen.

félreértés ne essék, attól, hogy most főleg a gugliról húztam le a keresztvizet, attól még a norcot meg a passportot meg a többi is utálom.

Igen, gonosz vagy. csak még nem tartasz ott, hogy mindenkinek kötelező legyen a lomodat használni.



Epokit Drive 2011.05.28. 21:47:08

@Álmos: Igazad is van, meg nem is. Az adatvédelem mellett érvelők elcsúsznak azon a pusztán tényen, hogy a zemberek minden szart feltesznek a fészükre ("na, jövő héten megyünk nyaralni" - értsd: üres lesz a kérés, kedves betörők) és hasonlók. Csak egyet kérek: legyen mindenhol "kikapcsolom az adatgyűjtést" gomb, és kész. Btw. az Iron fényesen bevált, semmivel nem rosszabb a hétköznapi aktív használatban, mint a Chrome. És csak a portable verzióról beszélek, továbbra is. (6 klf. böngésző van a gépemen, és ennél maradtam végül.)

Bambano 2011.05.28. 21:50:15

@Epokit Drive: "hogy a zemberek minden szart feltesznek a fészükre": helyesen: az emberek zöme. de aki abba a kisebbségbe tartozik, hogy foglalkozni akar az adatvédelemmel, azt megszivátja minden szolgáltató.

Kuruttya 2011.05.28. 22:17:55

@Bambano:

"nem tudhatod", "sosem tudhatod", stb. Igen, mint ahogy te sem tudod. Meg azt sem, hogy a szomszéd néni mennyit tud az életeredől, vagy hogy lehallgat-e a KGB. A paranoiával nem tudok mit kezdeni, ezek nem tények.

"megbízható cégeknél még sosem történt semmi a bankkártyákkal? ezt le mered írni egy olyan időszakban, amikor a sony

hálózatait hetek óta folyamatosan felborogatják a crackerek?"

Mondatértelmezés.. azt írtam: "még nem történt sose *a cégek részéről szándékos* visszaélés". Persze, ha jön a cracker és feltöri a rendszert, az szopás. De ne gondold, hogy ez csak akkor fordulhat elő, ha megadtad a Googlenek/Sony-nak/Apple-nak az adataid, egy bank biztonsági rendszerét is elkúrhatja valaki, meg mint mondtam, a sarki bolti leolvasót is megbuherálhatják. Ilyenkor lehullik pár fej, aztán felvesznek valakit aki ért is a biztonsághoz. Az emberi hiba mindig benne van a pakliban.

"a facebook akkor is nyomon követi a tevékenységedet a lájkoló gombon keresztül, ha nem vagy facebook tag"

Aha. A blog.hu is. Bizony! De hogy (facebook profil hiányában) mit is tudnak meg rólad pontosan? Semmit, ami ne lenne publikus pusztán attól, hogy megnyitottad a böngésződet. Nem zárkozhatsz be teljesen, ez van. Minden lépésedről keletkezik valahol egy log bejegyzés, de ez így van amióta internet létezik...

"a gugli sem borogatta ki a teljes kapcsolatrendszeredet mindenki számára a buzzon vagy min keresztül"

Ez a tipikus álproblémák egyike. Senkinek semmi baja nem származott ebből, csak néhányan szeretnek hisztizni.. mint te. (Elég csak egy levlistára feliratkozni, és máris a fél világ az ismerősöd lehet, nem sokat érnek ezek az adatok.)

"te még nem jártál úgy, hogy valamelyik asshole ismerősöd úgy regisztrált a facebookra"

Természetesen regisztrálva vagyok facebookra én is, mint minden ember aki nem ilyen hisztigép. Tehát én nem járhattam így, mert legfeljebb csak bejelölt ismerősnek az illető. Egyébként pedig ez is egy akkora álprobléma, mint a ház: bármelyik email klienssel pillanatok alatt megoldható, hogy a facebooktól érkező levelek egyenesen a kukában landoljanak.

"arról nem a google tehet, hogy felkerültek a wifi antennák a kocsira?"

Hm? Valamit félreértettél. Persze hogy szándékosan gyűjtöttek wifi adatokat. Én azt mondom, hogy ezzel nincs semmi baj. Te is megteheted, végiggurulsz az utcákon, és máris tudod, hogy melyik házban milyen néven fut a wifi. Eddig ez ugye nem túl nagy probléma. Ha találsz olyat, ami nincs titkosítva, pillanatok alatt az illető összes jelszavát is tudhatod, sőt ha logolsz, akkor a jelszavak anélkül fognak a te gépedre is felkerülni, hogy bármi különösezt tettél volna. Utóbbi már probléma, de elsősorban annál, aki nem titkosította le a wifijét.. azt meg ugye azért nem gondold, hogy a Google szándékosan az emberek jelszavaira pályázott.

"és nem a google az a cég, amelyik nem hajlandó rendesen végrehajtani azokat az utasításokat, miszerint törölje az illegálisan szerzett streetview adatokat?"

Ez az ügyvédek dolga, de szerintem ebben nincs semmi illegális. Akár a wifi adatokra, akár a fényképekre gondolsz, nehogymár illegális legyen közterületen fényképezni, vagy wifiket scannelni.. esetleg le kéne törölni flickr-ről is az összes közterületen készült képet? Vicc.

"ideológiai harcokra alkalmas adatbázis"

A pártok faszágait meg most ebben a konkrét helyzetben leszárom. A Google-höz nem sok közük van. Nem ez velük a legnagyobb baj amúgy sem...

"az pedig, hogy a gugli helymeghatározója milyen pontos, ki a francot érdekel?"

Engem pl. nagyon is érdekel, mert én használom napi rendszerességgel. Nem csak az amerikaiaknak van ám okostelefonjuk... (ami szerinted minden bizonnyal egy kémberendezés :D)

"rotfl, ilyet is csak a microsoft szemetjei óta tűrünk el, hogy alkalmazás összeomolhasson, előtte sosem volt ilyen"

Ez most egy vicc? Mert akkor nem értem. Az alkalmazások bugosak voltak, és bugosak is lesznek amíg világ a világ. Semmi köze ennek az ms-hez. Minden hello world-nél bonyolultabb programban lehetnek hibák.

"hátaid mögött, az előzetes megkérdezésed nélkül"

Szinte minden eddig felsorolt adatgyűjtés a felhasználó engedélyével történik. Az összes alkalmazás EULA-jában benne van (különben perelhetőek lennének a cégek), és a jobban neveltek külön is rákérdeznek, illetve engedik, hogy kikapcsold. Megjegyzem a Chrome pl. ebbe a kategóriába tartozik, a beállításokban mindent ki lehet kapcsolni. Kivételt képez persze ezek alól a szerver oldali webes adatgyűjtés, hiszen egyrészt nem lehetne megoldani, hogy minden felhasználótól engedélyt kérjenek (ismét: a blog.hu kért tőled engedélyt?), másrészt ezek olyannyira semmitmondó adatok egy személyről, hogy zéró adatvédelmi problémát jelentenek. Ha meg feltöltesz adatokat a felhőbe, az ugye implikálja, hogy ott is lesznek, tehát furcsa dolog meglepődni rajta:))

"Igen, gonosz vagy."

Hát, akkor ez a világ már csak ilyen gonosz:) A felhasználók meg biztos nagyon utálják, hogy pl. mindenféle egzotikus hibákat

fel tudok deríteni és ki tudok javítani az érkezett adatok alapján.

Bambano 2011.05.28. 22:49:05

@Álmos: "A paranoiával nem tudok mit kezdeni, ezek nem tények.": ha titkosszolgálati alkalmazott nyilatkozza, hogy örül, hogy elvégzik helyette a munkát, akkor a paranoiának van alapja.

Ha kikerültek a cégektől a bankkártya adataid és elvitték a pénzed, többet vagy kevesebbet anyázol, ha tudod, hogy szándékosan vagy nem szándékosan került ki? Ami nincs ott, az nem kerül ki. Ez az egyetlen működőképes védelem. A bank biztonsági rendszerével kapcsolatban meg azt tudom mondani: minden jogod és lehetőséged megvan arra, hogy ne használj bankot. Ugyanez már messze nem igaz sem a guglira, sem a facebookra. A bank nem száll be velem a liftbe, hogy titokban kilopja és lefotózza a bankkártyámat. Ha kell banki szolgáltatás, szerződök, ha nem kell, nem. A bank önkéntes. A facebook meg a gugli nem.

"Természetesen regisztrálva vagyok facebookra": ja értem. Tehát te önként szórod szét az adataidat, emelett mint fejlesztő, olyan alkalmazásokat is fejlesztesz, amik hasonló gonosz módon működnek, mint a gugli meg a facebook. Következésképpen te itt most nem is önérdékből vitatkozol, hanem saját őszinte véleményedet mondod. Ahham, majd el is hiszem.

"A Google-höz nem sok közük van": nem a google az egyetlen, akire zabos vagyok az adatkezelési disznóságai miatt.

"Az alkalmazások bugosak voltak, és bugosak is lesznek amíg világ a világ": dehogy voltak bugosak... ilyen szinten szemét szoftvert senki nem gyártott előtte. Egy OS/360-nal, egy vmssal közel sem volt ennyi baj soha. Igazából semmi baj nem volt velük. De sorolhatnám a 3.12-es novellt, a latexet, azokban nem volt beépített crasreport küldő, mert ott nem a felhasználót használták bétatesztelőnek.

"Szinte minden eddig felsorolt adatgyűjtés a felhasználó engedélyével történik." Ezt a véleményedet a bíróság nem osztja és egyelőre nekem ők hitelesebb forrás.

Felhőt sem kell használnom. Egyébként is a felhő pont az a dolog, amit pár év múlva vidáman fogunk temetni valami aktuálisabb marketing bullshit miatt. Azt a kis időt már megvárom.

"A felhasználók meg biztos nagyon utálják, hogy pl. mindenféle egzotikus hibákat fel tudok deríteni és ki tudok javítani az érkezett adatok alapján.": a célzott, szűk körű specifikus adatgyűjtéssel kapcsolatban sokkal kevesebb kifogás van. Ezt kellene elfogadni, hogy amit te csinálsz a programjaiddal, az nem karcol bele olyan mélyen a privát szférába, mint amit a gugli meg a többi hulladék.

De miután rájöttem, hogy önérdékből vitázol, nem szakmai alapon, szerintem hagyjuk, a továbbiakban ne válaszolj, mert nem lesz hihető.

Kuruttya 2011.05.28. 23:01:46

@Bambano: "minden jogod és lehetőséged megvan arra, hogy ne használj bankot. Ugyanez már messze nem igaz sem a guglira, sem a facebookra"

??? Komolyan azt akarod nekem mondani, hogy hamarabb lehet a bankokat kikerülni, mint a Facebookot? :D Na itt vesztetted el minden hitelességedet.

"Következésképpen te itt most nem is önérdékből vitatkozol, hanem saját őszinte véleményedet mondod."

Tehát ha valaki regisztrált Facebookon (internetező 20-as fiatalok 90%-a), és közben olyan alkalmazást fejleszt, ami gyűjt felhasználói adatokat, az nem gondolhatja őszintén, hogy az adatgyűjtési problémák 99%-a hiszti? Haha. Amúgy látom már rám is kiterjedt a paranoiád.

"egy vmssal közel sem volt ennyi baj soha. Igazából semmi baj nem volt velük."

:D:D:D:D Te is sok vms-t láttál közlekedni életedben :D Meg vms rendszergazdát :D Ha gondold bemutatlak egynek, aki a mai napig tereget egy vms gépet, elbeszélgethettek róla, hogy milyen problémamentes is az üzemeltetés így 2011-ben :D

"Ezt a véleményedet a bíróság nem osztja és egyelőre nekem ők hitelesebb forrás."

Arra azért válaszolj: ha a streetview nem legális, a flickr-re feltöltött többmillió közterületen készült kép sem az?

"amit te csinálsz a programjaiddal, az nem karcol bele olyan mélyen a privát szférába, mint amit a gugli meg a többi hulladék."

A Google nagyobb, tehát több mindent lát. Ugyan azt csinálják, mint én, csak a méret más.

"De miután rájöttem, hogy önérekből vitázol, nem szakmai alapon, szerintem hagyjuk, a továbbiakban ne válaszolj, mert nem lesz hihető."

És ezzel fel is oldottad a fejedben eddig lappangó, őrzítő ellentétet (hogy egy "felhasználó" miért is mond ilyeneket) azzal, hogy én valójában a gonosz nagytetvére része vagyok, és csak valami világméretű marketing terv részeként vitatkozom 1-2 emberrel egy istenhátamögötti magyar blogon, valójában nyilván nem így gondolom. Gratulálok!

Bambano 2011.05.28. 23:11:18

@Álmos: "az nem gondolhatja őszintén": nyilván véletlenül esik egybe a véleményed a melós érdekeiddel. persze, én meg most jöttem a fényemmel a k-paxról...

"a flickr-re feltöltött többmillió közterületen készült kép sem az?" azok a képek, amelyek alkalmasak arra, hogy felismerjék a rajta levő embereket, biztosan nem legálisak.

Mutass be nyugodtan a vms-es haverodnak, majd kiderül, ki ismeri régebből...

Kuruttya 2011.05.28. 23:13:55

@Bambano: "persze, én meg most jöttem a fényemmel a k-paxról..."

:D vitát azzal lezárni, hogy "hazucc", vicces.

"azok a képek, amelyek alkalmasak arra, hogy felismerjék a rajta levő embereket"

Node a streetview képek erre pont nem alkalmasak. Akkor?

"Mutass be nyugodtan a vms-es haverodnak, majd kiderül, ki ismeri régebből..."

Leírnám a nevét, csak tudod beindexeli a google... :D És nem haverom, hanem kollégám ;)

Bambano 2011.05.28. 23:47:41

@Álmos: idéznék tőled:

"a flickr-re feltöltött többmillió közterületen készült kép sem az?" a flickr-t kérdezted, nem a streetview-t.

"vitát azzal lezárni, hogy "hazucc", vicces.": nem is tudom, ki irkált ilyeneket először: "Na itt vesztetted el minden hitelességedet." a fagyvi visszanyalt?

de nem ártana, ha a felsorolt érveket cáfolnád, az sem baj, ha tételelesen, mert ez még nagyon hiányzik innen.

Kuruttya 2011.05.28. 23:55:08

@Bambano: "flickr-t kérdezted, nem a streetview-t"

Akkor olvassunk vissza, szépen, lassan:

-ha a streetview nem legális, a flickr-re feltöltött többmillió közterületen készült kép sem az?

-azok a képek, amelyek alkalmasak arra, hogy felismerjék a rajta levő embereket, biztosan nem legálisak

-a streetview képek erre pont nem alkalmasak

Ha újraolvasás után sincs meg: ha a flickr képek akkor illegálisak, ha felismerhetőek rajtuk az emberek, akkor a streetview képek miért lennének azok? Hiszen azokon nem ismerni fel őket. Így már érted?

"nem is tudom, ki irkált ilyeneket először"

Te. Basszus olvass már vissza. Az, hogy "Következőképpen te itt most nem is önérekből vitatkozol" előbb volt, mint az, hogy "Na itt vesztetted el minden hitelességedet.". Arról már ne is beszéljünk, hogy teljesen más kérdés kapcsán írtam én, mint te.

"ha a felsorolt érveket cáfolnád, az sem baj"

Szintén megvolt, olvass vissza.

Ez egy ilyen visszaolvasós, nosztalgizációs komment lett.

Bambano 2011.05.29. 00:00:32

[@Álmos](#): gyengébbek kedvéért a streetview képei nem csak akkor illegálisak, ha felismerhetők rajta az emberek. Emellett még sértik a szerzői és szomszédos jogokról szóló törvényt is.

de akárhogy is csűröd-csavarod, a második tagmondatod szerint a flickr-re voltál kíváncsi és én arra válaszoltam. most elegánsan felejtjük el azt a tényt, hogy a streetview kitakaró algoritmus sz.r és egy csomó felismerhető arc meg rendszám maradt rajta.

azt mindig is nagyon szerettem, amikor számomra ismeretlenek akarják megmondani, hogy én mit tudok vagy nem tudok, mit csináltam, stb. na mindegy.

Kuruttya 2011.05.29. 00:02:24

[@Bambano](#): "gyengébbek kedvéért a streetview képei nem csak akkor illegálisak, ha felismerhetők rajta az emberek"

A kérdés az, hogy MIÉRT, és hogy a flickr MIÉRT NEM. Tényleg ennyire nehéz? Tehát: miért nem ugyan azok a szabályok érvényesek a flickr képeire, mint a streetview-éra?

Bambano 2011.05.29. 00:17:56

[@Álmos](#): például azért, mert a flickr méretei beleférnek a magáncélú felhasználásba, a streetview meg nem.

A magáncélú felhasználásnál mennyiségi korlát is van, amibe belefér az, hogy lefotózkod a barátnődet és felrakod a flickr-re, de az nem, hogy egy az egyben lefilmezel egy egész várost. Az sem mindegy, hogy a fotón például egy épület csak mint háttér szerepel vagy pedig maga az épület nagy tömegben a téma.

Kuruttya 2011.05.29. 00:26:29

[@Bambano](#): találatok száma "new york" keresésre flickr-en: 11516697. Sokhoz GPS koordináta is rendelve van. Budapestről készült képek térképen a panoramioról (érdemes a belvárosban bezoomolni):

www.panoramio.com/map/#lt=47.4984056&ln=19.0407578&z=4&k=2

Nem nagyon van olyan pontja a városnak, amiről ne lenne kép...

De akkor ez a pármillió darab még belefér gondolom a magánfelhasználásba. Vagy ha minden képet más csinál úgy már oké? És elég sok kép van köztük, amin egy épület maga a téma... Érzed te is, hogy elég labilis lábakon áll ez az érv.

Bambano 2011.05.29. 00:47:54

[@Álmos](#): abból a 11.5 millió képből hányat csinált vállalat üzleti céllal és hányat magánszemély magáncéllal?

másrészt meg lehet, hogy nem a streetview lesz az egyetlen, amit jogi útra terelnek, legfeljebb az első lesz.

cworm 2011.05.30. 11:53:52

Én Álmossal értek egyet, nem kell a műhiszti.

atila68 (törölt) 2011.05.31. 14:30:58

A lányom kapott egy levelet Orbán Viktortól.

A lányom kiskamasz, és alaposan be van oltva, bizton nem adta ki a laccímét, soha semmilyen formában a neten.

...és mi a Chrome, meg az iPhone spywarekénti üzemelésén polemizálunk.

Ugyan!

Orosz cég állhat a hamis Mac antivírusok mögött

2011.05.30. 12:01 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [mac](#) [hamis](#) [antivirus](#) [defender](#) [brian](#) [krebs](#) [chronopay](#)

Erősödni látszik a ráfordított munka mennyisége a Macintosht célzó hamis antivírusok frontján. Ez utóbbit már a **sorozatos, célzott domainigénylések** is szemléletesen mutatják.



Nem először köszönhetünk érdekes felfedezést Brian Krebsnek, [legutóbb éppen az orosz ChronoPay cég ambivalens tevékenysége kapcsán](#) idéztük gondolatait, és ehhez némiképp kapcsolódunk ezúttal is, mivel a **feltételezések szerint** [közük lehet a Mac Defenderes bulihoz is](#).



Mint ismeretes, eleinte mérgezett Google Image Search találatokban játszódtott a dolog, itt a telepítéshez még kért admin jelszót, ám **az Intego vizsgálatai szerint** [a későbbi változatok már nem kértek ilyesmit](#).



[Krebs legfrissebb felfedezése szerint](#) a [mac-defence.com](#) és a [macbookprotection.com](#) domainhez tartozó WHOIS információ **mindkét helyen tartalmazza azt az fc@mail-eye.com emailcímet**, amely egy tavalyi incidens kapcsán került a figyelmük középpontjába. Az akkori vizsgálatok szerint - amely dokumentumok és emailek kiszivárgásával volt kapcsolatos - az derült ki, ezt az email címet **a ChronoPay tulajdonosa fizeti és birtokolja egy Németországban futtatott virtuális szerveren**.



A korábbi feljegyzések azt is mutatják, hogy **a hivatkozott fc@mail-eye.com címet egy Alexandra Volkova nevű ChronoPayes pénzügyi alkalmazott már korábban is használta**. És ez a cím aztán **további gyanús domainregisztrációkat is kezdeményezett, ilyen például az appledefence.com és az appleprodefence.com** lefoglalása.



Nyilvánvalóan itt is a bizonyítás a legnehezebb feladat. A [ChronoPay nyilatkozatban tagad](#) - **aki akar, az persze hihet ennek** a látszat ellenére is, ez állampolgári joga. Ám lényeg a lényeg, a jelek szerint egyre több különböző néven, egyre több hitelesnek tűnő domainen, és gyaníthatóan egyre gyakrabban fogunk sajnos ilyesmivel találkozni.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Safe mód a Mechagodzilla ellen](#)

- [Dropbox csalival terjedtek a kémprogramok](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2942817>

Kommentek:

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

Nincsenek hozzászólások.

Előadókat vár a Hacktivity

2011.05.31. 09:45 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [hacktivity konferencia 2011](#)

[Kelet-Közép-Európa legnagyobb hackerkonferenciája](#) - ez a szó illik az eseményre, amely idén ősszel is megrendezésre kerül a szeptember 17-18.-i hétvégén.



A következő témakörökben biztosít lehetőséget jelentkezőknek klasszikus előadásokra, vagy pedig akár gyakorlati workshopra is: mobil eszközök sérülékenységei, hardver hacking, telekommunikációs hálózatok támadási vektorai, hálózatbiztonság, operációs rendszerek biztonsága, böngésző alapú támadások, visszaélés közkezdvelt alkalmazásokkal, adatbázis biztonsága, szerver hibáinak kihasználása, üzleti alkalmazásokból információgyűjtés, rosszindulatú mobil kódok, hacking eszközök, információs háború, hacker szubkultúra, social engineering, digitális kriminalisztika, adatvédelem, szellemi tulajdonnal összefüggő kérdések.



Ha szeretnél előadni a Hacktivity 2011 konferencián, akkor pályázatot küldd el június 10-ig a cfp@hacktivity.com címre! Minden további részlet [a hivatalos honlapon olvasható](#). Viszlát szeptemberben!



Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- ["Szösölmédia" és nyaralás](#)
- [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/2945232>

Kommentek:

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

Nincsenek hozzászólások.



A nőket nem érdekli a védekezés

2011.06.01. 10:35 | [Csizmazia István \[Rambo\]](#) | [1 komment](#)

Címkék: [frissítés](#) [felmérés](#) [vizsgálat](#) [vírusirtó](#) [eset](#)

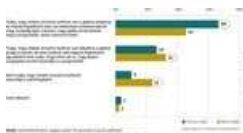
Az ESET megbízásából elkészített friss kutatásból az derül ki, hogy **a magyar internetezők jelentős része azt sem tudja, milyen vírusirtó van a számítógépre telepítve**. Az internetes kártevők elleni védekezés a hölgyeket foglalkoztatja a legkevésbé.



A heti rendszerességgel internetező felnőttek több mint fele gondosan frissíti, és az értesítéseknek megfelelően karbantartja a számítógépére telepített vírusirtó szoftvert. Megközelítőleg **harmaduk azonban ugyan tisztában van a szoftver nevével, de nem foglalkozik a frissítésekkel, 16 százalékuk pedig a számítógépe biztonságáért felelős program nevét sem tudja**.



A jó hír az, hogy a felnőttek fele odafigyel a vírusirtójának frissítésére. Ám az, hogy a másik felük gyakran még azt sem tudja, milyen vírusvédelmi rendszer van a számítógépén, jelzi, hogy a magyar internetezők jelentős részének fogalma sincs arról, hogyan védheti meg számítógépét a kártevőkkel szemben.



A vírusirtó szoftver karbantartásával kapcsolatban leginkább a nemek között mutatkozik eltérés: **több mint 20 százalékkal több férfi figyel oda a beállításokra, mint nő, mialatt az internetező nők majdnem negyede vallotta azt, hogy semmit sem tud a vírusirtójáról**. Azok az internet-felhasználók, akik nem figyelnek oda operációs rendszerük és vírusirtójuk frissítésére, könnyedén vírustámadás áldozatává válhatnak.



Az a legrosszabb, hogy a mai kártevők célja **már nem a rombolás, hanem a pénzszerzés**. Így a fertőzött gépek tulajdonosai sokszor észre sem veszik a támadást, mialatt **az internetes bűnözők távolról ellophatják** hitelkártya adataikat, vagy levélszemét küldésére használhatják fel a számítógépüket. A védekezés első lépése, hogy megtanuljunk használni vírusirtó szoftverünket.



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés traceback címe:

<http://antivirus.blog.hu/api/trackback/id/2945603>

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](#).

Advocatus Diaboli 2011.08.24. 17:41:02

A létező legjobb vírusvédelemnek 5 betű a neve: Linux.

Biztonsági riadó a böngészőben

2011.06.03. 17:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [firefox](#) [böngésző](#) [ablak](#) [hamis](#) [antivírus](#)

Mi jöhet még? - kérdezhettük [a szélvédő alá csúsztatott kamu parkolási büntetésnél](#) és a [hamis szerzői jogi büntetési ablak](#) láttán. Van új a nap alatt - jelenthetjük ki bátran, hiszen ezúttal itt a böngészőkliens üzenetben manifesztálódott hamis antivírus.



Akik törzsolvasók, azoknak az emlékezetében még ott élhet valamilyen halvány emlék, mintha ilyesmi vagy hasonló történt volna már. Igazából valóban volt némi kis előjáték, akkor [hamis Bejelentett támadó webhely üzenet érkezett](#), és anno jól meg is állapítottuk, **aki egy ilyen saját ablakban kínáló linkről reméli letölteni a gyógyírt jelentő megoldást**, az egyúttal orbitális mértékű naivságról is tanúbizonyságot tesz.



A mostani próbálkozás már ezen is továbblép egyvel, mindezek a haladócsoporthoz tartozó továbbgondolását láthatjuk, hiszen **itt a böngésző üzenetnek látszó tárgy már maga a hamis antivírus riasztás**. Vagyis nem weblapszerű a megtévesztő ablakunk, hanem sokkal inkább szabványos hibaüzenetszerű. [A Firefox esetén azért érdekesebb ez, mert akkor egy tűzrőkézés riasztási ablak jelenik meg](#), míg az Internet Explorerrel böngészve a már jól ismert hagyományos, Tesco gazdaságos Sajátgép ablakos megoldás érkezik. A forgatókönyv innen már ismert, **a Start Protection gomb megnyomása** - minő meglepetés - nem a védelem, hanem a fertőzés kezdetét jelenti.



Mivel **a kártevőterjesztők láthatóan folyamatosan keresik az új utakat**, friss módszereket - lám [a Macseket is már három különböző nevű hamis antivírral szórakoztatták](#) - ezért valószínű, hogy előbb-utóbb a különböző operációs rendszerek és a főbb böngészőfajták is megkapják majd így a magukét.

 Tetszik  10 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászárral](#)
- [Elégedetlenség vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2954237>

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.

Privát böngészés vagy mégsem

2011.06.06. 15:55 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [microsoft](#) [facebook](#) [privát böngésző mód](#) [chrome](#)

Már korábban is látszottak bizonyos hiányosságok a sokak által biztosnak vélt Privát böngészési módról, amiről a szakemberek azért tudták, hogy nem bombabiztos, sőt.



"-Hát... kicsoda ön... Mr. Irving? Nem Mr. ... Irving?

- [Én inkognitóban vagyok.](#)

- Az miféle viselet?

- Inkognitó az, ha valaki álnéven él...

- Nagyszerű! Akkor én is inkognitóban vagyok! Szintén szélhámos?

- Haha! Igazán kedves alattvaló maga, José pincér, de megyek, mert Mr. Gould még észreveszi a távolmaradásomat."



Az inkognitó, vagy privát mód (egyes említésekben pornó mód) az a lehetőség (lenne), amikor a netező névtelen és beazonosítatlan maradna. Ez aztán sokféleképpen megdőlt már. **Először, mikor kiderült, a dolog alaptól nem egészen úgy működik, ahogy kellene:** "A vizsgált szoftverek az Internet Explorer 8, a Firefox 3.5, a Chrome 5 és a Safari 4 voltak. A tapasztalatok lesújtóak: a megvizsgált alkalmazások egyike sem volt képes teljes mértékben megvédeni használoi magánszféráját. A legnagyobb problémát az jelentette, hogy egyik szoftver sem rejtette el maradéktalanul a böngészés nyomait és a folyamat után számos árucódos jel maradt a számítógépeken. Külön gondot okoz, hogy az adattárolás nem titkosítva történik. Vagyis, ha valaki utólag nem törli ki ezeket a nyomokat, akkor gyorsan megállapítható, hogy az illető milyen oldalakon járt." Aztán jött a második menet, amikor kiderült, **a kiegészítők sem kezelik ezt korrekten, és ezzel jól megghiúsítják a dolog lényegét.** Végül szintén komoly csapás volt az imperializmusra, mikor a [Panopticlick féle](#) [újnyomtatás képzés a telepített kiegészítők valamint font típusok, továbbá a nyelvbeállítás alapján 90%](#) feletti azonosítási rátát lehet produkálni.



A fentiek fényében és pontos ismeretében mégis sokaknak meglepő lehet, mikor **a webhely a böngésző privát mód ellenére barátságosan hátbavereget és kedélyesen a keresztnévünkön szólít.** De találkozhatunk ezzel úgy is, hogy a Facebookon [az Azonnali Személyreszabás / Instant Personalization beállításain](#) nem elég figyelmesen rágtuk át magunkat hetente. De [a Google Chrome böngésző esetében mindegy is, a funkció használata kioltja az előzőleg beállított privátmódot.](#)



És ez az a pont, ahol hajlamosak lehetünk inkább egy Graham Clueley vagy Randy Abrams véleményével egyetérteni: **nem lehet mindent kizárólag a felhasználó nyakába zúdítni, a szolgáltatóknak is lehetne/kellene felelőssége** figyelmeztetni a felhasználót: ha ezt kipipálod, akkor a privát módnak annyi, de természetesen **a beállítások rendszeres (és szándékos?) túlbonyolítottága is hozzájárul** a kialakult áttekinthetetlen helyzethez.



f Megosztás

+1 0

Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2961610>

Kommentek:

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



[atko 2011.06.06. 20:06:19](#)

A chromium figyelmeztet ha kiegészítők beállításainál, hogy a privát módba fusson, vagy sem, és ha igen akkor nem garantálja a privátot. Ettől függetlenül a usert minden alól felmentem. Az összes katyvasz a szolgáltató és a fejlesztők felelőssége. Attól fogva, hogy a pc-t úgy adják el, mint egy otthon is használható gépet (háztartási gép, hifi , tv, stb...) úgy is kéne működnie. A rádióban max elemet cserélek és nem támadják meg a rádióhullámok.

[nyos 2011.06.07. 21:49:32](#)

A szolgáltatonak az a feladata, hogy adjon egy drotot, es onnantol kezdve transzparens legyen. Ha megprobal beleszolni, hogy milyen programot es milyen beallitasokkal hasznalok azon a droton, olyan szolgáltathoz megyek, aki nem szol bele. A fejlesztoknek az a dolga, hogy megertessek a felhasznalokkal, hogy ha ezt csinalod ez tortenik, ha azt, akkor az. Ha bekapcsolja a porno modot de kozben a facebook kiegeszitot direkt aktiválja, akkor ne csodalkozzon, ha a neven szolitjak. Ugyanugy ne csodalkozzon, ha a bekapcsolt porno mod ellenere kivagjak a netkavezobol mert nyilvánosan a farkaval játszik. Az ellen nem ved.

Az Apple bemutatta az iPhone 5-öt. Vagy mégsem?

2011.06.08. 12:00 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [spam](#) [apple](#) [trójai](#) [iphone5g](#)

Úgy tűnik, mostanában hétmérföldes lépésekkel szaporítjuk a "Vagy mégsem?" típusú posztjaink számát. Ehhez a [még meg sem jelent, de mi máris bemutatjuk](#) tipikus esete szolgáltatott újfent muníciót.



A technikai fejlődés sebessége lassan eléri a [Mézga Aladár Különös kalandjaiból ismert szintet](#), ahol a gyártó gépsor végén már azonnal **be is zúzzák a terméket, mert mire végigért rajta, már el is avult**. Ami a mobiltelefonokat illeti, néhány havonta, félévente jönnek a még újabb, még többet tudó modellek. Néha valós bennfentes infók is kiszivárognak, szintén néha a fejlesztők erős izgalmi állapotban ottfelejtik a mintadarabot a kocsmában, sőt még szintén néhanéha pedig [a Gizmodo jól bemutatja azt legelsőként, majd ezekután jönnek a jól "megérdemelt" házkutatások](#). Ám sokkal többször történik meg az, hogy kéréstlen emailben, üzenetben, linkben kapunk kamu értesítést arról, hogy megjelent a 100.100.



Most [nem más írt nekünk levelet, mint a noreply@apple.com](#), már csak emiatt is dagadhat a keblünk a büszkeségtől. Az üzenet tárgya "Finally. The amazing iPhone 5. Now available in black edition.", benne pedig az alábbi szöveg: **"Még mindig az ósdi, őskövület fatengelyes iPhone4-edet használod te lúzer a szuper iPhone 5G helyett? Pedig ez tényleg vékonyabb, gyorsabb és kisebb mint valaha."** Kicsit rímel mindez egy korábbi posztunkkal, melynek stílszerűen: **"Még nem is létezik, de mi már letölthetjük"** volt a címe. Nagyjából itt is hasonló a helyzet, a kéréstlenül érkezett sudribunkók levele helyett inkább bátran hagyatkozzunk például a mértékadó Appleblogra: az **iPhone 5G ugyanis még nem kapható, nincs is készen**.



Ámbátor a mellékelt kép igen tetszetős, hitelesnek igyekszik mutatkozni, ez ne tévesszen meg senkit. **A szétcsúsztható hardveres billentyűzet inkább csak néhány megszállott szirupos vágýálma**, ilyesmi a hivatalos specifikációk, megerősített tervek között nem szerepelt, [lásd "különálló billentyűzet: esély 0%"](#).



Nem vágýalom viszont a spam levéllel terjedő Windows .EXE formátumú trójai kártevő, amely azért szerencsére 65% feletti VirusTotal felismerést bír produkálni.



Érdekes, hogy ez a [próbálkozás már nem is az első](#) ebben a témában, már májusban is volt egy hasonló, ám [az is biztos, a telefon végleges megjelenéséig nem is ez lesz az utolsó](#) a sorban. Már csak emiatt is: **Apple híreket kizárólag csak őstermelőtől!**



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.





Ajánlott bejegyzések:

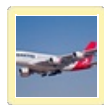
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2966025>

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](#).



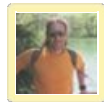
thepret • <http://teneriferepulojegys.hu/> **2011.06.11. 06:45:15**

fogyasztói társadalom...



¡Viva La Onda! **2011.06.29. 10:53:36**

Epll? Csak sznoboknak. :)



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2011.06.29. 11:46:21

Csak óvatosan itten az ilyen flamewar gerjesztő szurkapiszkákkal :-)

Tapasztalatból mondhatom, lehet szeretni a Mac-et, még ha az ára természetesen - főleg nekünk magyar pénztárcával mérve - valóban nem kevés. Kártevő ügyileg sem rossz választás. A telefon az már más tészta, ahogy látom a környezetemben, a fél-egy évenkénti csere mármár konzervatív szenilitásnak számít ;-)

Microsoft Update vagy mégsem?

2011.06.10. 16:00 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [windows update](#) [hamis](#) [antivirus](#) [msrt](#)

[A látszat megtévesztő benyomásairól](#) már elmélkedtek korábban igen színvonalasan mások is, mi azonban ezúttal a hamis vírus evolúció következő lépcsőfokát mutatjuk be azzal, hogy ez azért valóban egy nice try.



Éppen csak pár napja, hogy a törzsfeljedési vonalat végignézve megállapítottuk, mindig sikerül csavarniuk egyet a dolgon: akkor [a Firefox böngésző üzenetben érkező rogue programot](#) vettük górcső alá. [Ezúttal egyenesen egy Microsoft Windows Update-tel van kikövezve a hamis vírusokhoz vezető út.](#)



A látvány **pontos koppintása a klasszikus frissítő ablak kinézetének, ám** a kattintás nem fontos és kevésbé fontos frissítéseket, javítófoltokat hoz a házhoz, hanem a már említett kamu riasztásos képernyőt.



Van benne persze némi perverzió is, hogy ez a hamis frissítés éppen a **Windows Malicious Software Removal Tool** képében és hasonlatosságában ajánlatja magát, mindenesetre ne kattintsunk bambán kizárólag a képernyő kinézet alapján, hanem **mindig ellenőrizzük az URL sort**, (haladó csoportosak az IP címet is ;-)) mert csodák nincsenek.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés **trackback** címe:

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](#).

Tryptich 2011.06.13. 02:47:54

Hello!

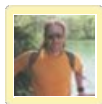
Érdekelne, hogy mit gondolsz erről. Valami megváltoztatta a böngészőm kezdőoldalát facebook.com-ra, de mikor bejelentkeznék, az alábbi üzenetet kapom:

noob.hu/2011/06/13/facebook.bmp

Az oldal amire irányít:

www.facebook.com/home.php?secureverification

Nem hinném, hogy ez valódi oldal lenne, már csak a helyesírási hibák miatt sem. Kérlek ha tudsz erről valamit, vagy hogy hová kellene fordulnom ezzel, válaszolj.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.06.13. 09:27:43**

Szia!

Valóban nem szokványosnak látszik a dolog, és más nyelvterületeken is panaszkodnak, például franciául:
<http://translate.google.com/translate?u=http%3A//www.commentcamarche.net/forum/affich-21989429-virus-sur-facebook&hl=hu&langpair=auto|hu&tbb=1&ie=ISO-8859-1>

Úgy tűnik, ez valamilyen trójai cookie lopó cucc lehet:

pastebin.com/Pebij7Zn

Szerintem ne kattints rá, ellenőrizd az engedélyezett appjaidat, gyomlálj, ha kell, csinálj a gépeden teljes vírusellenőrzést, és persze jelentheted a Facebookos bácsiknak.

Manatwork (törölt) 2011.06.15. 08:53:44

"mindig ellenőrizzük az URL sort"

Ez így van! De mi lesz akkor amikor a böngészőkben eltüntetik a címsor mezőt? Ezt már kezdik pedzegetni a Chrome fejlesztők. Igaz még csak dev verzióban van ilyen feature, de ha kijön végleges verzióban is akkor a többi böngészőgyártó is szinte biztos beépíti ezt a saját cuccába... Az éles verseny miatt gyakorlatilag rá lesznek kényszerítve.

Jön az adathalászkok mennyországa? :(

Az ATM védelem új útjai

2011.06.14. 18:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hangfelismerés](#) [ellenőrzés](#) [ujjlenyomat](#) [atm](#)

Láttunk már korábban [kártevővel fertőzött pénzjegykiadó automatát](#), aztán volt a történet a [bárki által szabadon megvehető/vizsgálható/akár üzembeállítható használt ATM](#)-ekről is, és végül, de nem utolsó sorban [az alapértelmezett jelszóval kapcsolatos trükkökről](#) is megemlékeztünk. Ezúttal ~~brit~~ [tudósok orosz szakértők új módszerekkel próbálják a csalókat kiszűrni](#) a pénzjegykiadó automatáknál.



Elképzelésük szerint az **ATM ujjlenyomatfelismeréssel is kiegészítené** a kártya technikai és a begépt PIN kód ellenőrzést, de **emellett rendelkezne egyéb módszerekkel, például hangfelismeréssel is, ami a csalók ideges hangját vagy a hazugságot lenne hivatott kiszűrni.**



Maga az elképzelés érdekes, például a **háromdimenziós arcfelismerés, az ujjlenyomatok eltávolítása, az útleveél beolvasási képesség** mind hasznosnak látszik. Hogy aztán a hangdetektor mennyire képes valóban megkülönböztetni a normális és kártékony idegességet, nem tudni, emellett pedig adatvédelmi, adatkezelési szempontból is jelentkezhetnek még aggályok a tervezett módszerrel kapcsolatban.



Meglátjuk, mi lesz belőle a Sperbanknál folyó élestesztelés után, és hogy a gyakorlatban **mennyire bizonyít jól az ilyesfajta kiegészítő szűrés.**



Végül pedig **további jó kérdés lehet még**, hogy mit lép majd arra, mikor [komor tekintetű szótlan egyének drótkötéllal a kezükben közelítenek](#) a pénzjegykiadó automata felé ;-)

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2983684

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.

Megérkeztek a vadonatúj, 2012-es modellek

2011.06.16. 13:45 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hamis 2012](#) [antivirus](#)

[Időben egyre korábbra tolódik](#) a (nevében) új generációs hamis vírus példányok megjelenése. A készítőik idén június idusán már szemlátomást elérkezettnek látták az időt arra, hogy egy egész raklap új programot zúdítsanak a boldog és lelki szegény felhasználók nyakába.



A hamis vírus már [egy elég régi műfaj](#), [egy olyan fajta csalás](#), amit teljesen megszüntetni sajnos lehetetlen. Megszokhattuk, hogy minden évben változó időpontokban színrelépnek az új szériás rogue programok, legfedve a Windows minden verzióját és árnyalatát. [A 2012-es eresztés széles választéka már meg is érkezett: Win 7 Antispyware 2012, Vista Antivirus 2012, vagy akár XP Security 2012](#), ki mire gerjed. De tudják ezt lovon és trapézon is, íme a fajták rendszertanából egy kis táblázatos ízelítő, minden van itt, mi szem-szájnak ingere, és irtani is tereh ;-)

Windows XP Antispyware 2012	Windows Vista Antispyware 2012	Windows 7 Antispyware 2012
XP Antispyware 2012	Vista Antispyware 2012	Win 7 Antispyware 2012
XP Antispyware 2012	Vista Antispyware 2012	Win 7 Antispyware 2012
XP Antispyware 2012	Vista Antispyware 2012	Win 7 Antispyware 2012
XP Antispyware 2012	Vista Antispyware 2012	Win 7 Antispyware 2012
XP Antispyware 2012	Vista Antispyware 2012	Win 7 Antispyware 2012

Jól láthatóan a klasszikus hagyományos ágat sem hagyják veszendőbe, ezt is folyamatosan fejlesztik annak ellenére, hogy az újítások is megszokottak: a hamis RIAA felszólításon át a [manipulált Firefox üzeneteken át](#) az egyéb [válogatott zsidványságokig bezárólag](#) minden új eszközt, módszert, fortélyt bevetnek.



A dolog kivédésére érdemes lehet már eleve **egy valódi internetbiztonsági csomag naprakész változatával védekezni, mellette meg nem elhinni, nem kattintani**. Ha pedig hadrafogható védelem hiányában mégis sikerül valahogyan beletenyernelni egy ilyenbe, olyankor a megbízható helyekről [letölthető how2remove instrukciók](#) húzhatják ki a szekerünket a bajból.



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2987351>

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.

Telefonos support vagy mégsem

2011.06.20. 14:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [telefon](#) [csalás](#) [hamis support](#)

Vagy mégsem rovatunkban ezúttal arról lesz szó, komoly **divatja lett a hamis technikai támogatást kínáló telefonhívásoknak**, ahol sok esetben létező, valódi cég munkatársaként mutatkozott be valaki. Volt ez már korábban is hébe-hóba, ám a **Microsoft legújabb felmérése szerint a jelenség kimutathatóan erősödött**.



Ha az előzményeket vizslatjuk, egy ősi, 2007-es mégsem poszt utalt arra elsőként, hogy [Koreában nemzeti sport lett a hamis banki ügyfélszolgálati hívás](#), **érdemes résen lenni**, nem csacsogni, adatokat megadni. Nyilvánvalóan egy ilyen lépése a csalóknak óhatatlanul devalválta egy adott pénzintézet jóhírnevét, renomóját is, és ebből [a hírnév tépázásból aztán újabb népi sportág vált](#), amint arról egy első és [egy második írásban is](#) beszámoltunk már. Ezek hátán, mintegy továbbépítkezve jön elő újabban az a jelenség, hogy **létező, ismert számítógépes, biztonságtechnikai cégek nevében supportot kínálva telefonálnak a csalók**, és próbálják a maguk 5% áldozatát megtalálni.



A történet lefolyása azoknak lehet ismert, akik a hamis antivírus bizniszt már követik egy ideje: **letöltetnek a gyanútlan áldozattal valamilyen fertőző állományt, ezzel hátsó ajtót nyitnak a rendszerben, magyarán távoli hozzáférést szereznek a géphez**, és ezzel gyakorlatilag a jelszavait, bankkártya adatait próbálják meg kinyerni. Hétezer embert kérdeztek meg [angol nyelvterületen - Egyesült Királyság, Írország, Egyesült Államok és Kanada - és a felmérés azt mutatta, hogy mind a négy országban a számítógépfelhasználók 15 százaléka már kapott ilyen hívást csalóktól. Hétezerből ezerötvenen](#) - ez már nem elhanyagolható arány, nem csupán hébe-hóba, vagy olykor-olykor, hanem ilyen nagyságrendnél - ami idővel vélhetően nem csökkenni, hanem még növekedni is fog - már muszáj tudatosan felkészülni. Az elszennvedett károk mértéke 875 USD (164 ezer HUF) összegtől 4800 USD-ig (904 ezer HUF) terjedt, ez szintén nem kevés, mondjuk tegye fel a kezét az, [akinek ennyi felesleges, csalóknak önként és örömmel adható pénze van](#).



Tulajdonképpen **az számítana jó eredménynek**, ha a gyanakvó hozzáállás és a gyanús szituációs minta gyűjtana mindenki fejében isteni szikrát minden ilyen helyzetben. Mert az bizonyos, hogy aki ilyen blogokból, újságokból, hírekből csak és kizárólag mindig csak egy konkrét esetre készül fel, [az mindig vesztes helyzetben és hátrányban marad](#). Egy "ugyan diktáld már be a frissen vásárolt feltöltőkártyád sorszámát" esetből kevés az a levont tanulság, hogy jó, a feltöltő kártyát akkor most nem diktálom be. A megfelelő hozzáállás az, hogy nem diktálok be soha senkinek semmit, és hoppácska, gondolkozzunk csak, honnan tudhatnám, hogy az aki jelentkezett, az biztosan az, akinek mondja magát? Ez utóbbi szkeptikus gondolat az, ami már egy jó védelmi minta része lehet, sőt a dolog ellenőrzése egy evolúció-ügylet szükséges "eye-opening adventure".

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés [trackback címe](#):

<http://antivirus.blog.hu/api/trackback/id/2999768>

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 böngésző a háznál

2011.06.22. 12:10 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [biztonság](#) [böngésző](#) [új firefox5](#) [chrome13](#)

Korábban már többször is pedzegettük, [ab ovo biztonságos böngésző nem létezik](#), de azért ennek ellenére érdemes orientálódni az Internet Explorer 6.0-ról ;-), meg hogy x tonna kiegészítő szolgálhatja a biztonságunkat - például NoScript és barátai. **Ezúttal két új verziós böngészőt nézegettünk röviden**, hogy a kisebb memóriefoglalás, fejlettebb HTML5 támogatás, gyorsabb javascript motor, és a 110/100-as ;-) Acid teszt eredmények mellett **milyen friss biztonsági ficsőrök figyelnek bennük**.



Aki már próbálkozott valamilyen szinten [összezavart Javascript kód kibogozásával](#), annak lehet érdekes az új, 13-as **Chrome De-obfuscate szolgáltatása**, amely ha nem is pottyantja készen sültgalambként az ölünkbe a kártékony URL-t, de azért szinte majdnem, ebben hasznosan segít, emellett töréspontozható, léptethető, etc. Ezenkívül természetesen [számos hibajavítás is történt, és olyan biztonságot szolgáló újítások is](#) megvalósításra kerültek, mint például [az automatikusan HTTPS-re lépés, ha az létezik](#).



A Chrome-nál ha valaki emlékszik, [már jó régóta van sandboxban futó PDF](#), a Firefox pedig éppen [most dolgozik a saját JavaScript alapú biztonságosabb PDF](#) megjelenítőjén. Ha már a rókával folytatjuk, csendben, mindenfajta gigászi hírverés nélkül megérkezett a végleges **Firefox 5.0**, [benne szintén számos biztonsági rés és hiba javításával](#). [A beta utáni viharos gyorsasággal, RC nélkül kiadott változat](#) bennünket egyik legjobban érdeklő része **a felhasználó követésének (persze alapszinten)** való kikapcsolási lehetősége.



Azért azt mindenképpen érdemes megemlíteni, hogy **a Firefoxhoz készült csillió kiegészítő között is találhatunk kedvünkre való JavaScript elemzőt**, ezek közül a két legismertebb a JavaScript Debugger, valamint a kifejezetten összezavart kódok kibontásához használható JavaScript Deobfuscator.



Az új FF verzió megjelenése menetrend szerint szinte minden alkalommal kaotikát okoz, ahogy azt a Leeroy nevű kommentelő találó megfogalmazta: **"Lehet majd megint kidobni a használt add-onok felét, mert biztos nem lesznek kompatíbilisak az új verzióval"**. Hát igen, ez sajnos rendre így igaz, és hivatalos megoldás híján, a lassú add-on frissítések megjelenéséig [jöhet a türelmetlen felhasználó buherátor szellemiségű workaroundja](#).



Ehhez **mindössze az egyelőre még ZIP szerkezetű XPI fájlban az install.rdf nevű állományt kell megpíszkálni egy texteditorral** ahhoz, hogy 99% eséllyel telepíthető és egyben működőképes is legyen. **Garancia nincs rá, de példának okáért** a TinEyeReverseImageSearch és a WebShots képernyőkép készítő kiegészítő ezzel a trükkel itt az 5.0 alatt is simán rábólintott az eperfa lombjára és a felhasználó legnagyobb örömére újfent hadrafoghatóvá avasztált.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

☐ **jánlott bejegyzések:**

- [A PRISM szeme mindent lát](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adatahalászattal](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3005588>

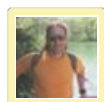
Kommentek:

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



¡Viva La Onda! 2011.06.29. 09:47:42

Az a kommentelő én voltam a hws-w-n. :) Egyébként szerencsére nem kellett a felét kidobni, 2 volt olyan, amelyre kicsit várni kellett, de már ez is megoldódott. És van egy workaround is: a Nightly Tester Tools nevű addonnal ki lehet kapcsolni a kompatibilitásfigyelést, így hacsak nem okoz nagy gubancokat a régebbi brózerverzióhoz készült bővítmény, továbbra is üzemben lehet őket tartani.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.06.29. 11:38:03

Hello ¡Viva La Onda!

Üdv a bárkán :-). Az NTT tényleg egy jó ötlet.

Én anno igazából azért kezdtem el kézzel barkácsolni, mert több, számomra létfontosságú kiegészítő még hónapok múlva sem volt frissítve. Van, amelyik évek múlva sem lett aztán.



¡Viva La Onda! 2011.06.30. 19:01:02

No az valami igen nagy ritkaság addon lehet. :)

Biztonságtudatos-e vagy?

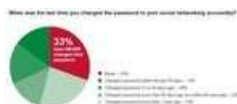
2011.06.24. 13:00 | [Csizmazia István \[Rambo\]](#) | [3 komment](#)

Címkék: [biztonság](#) [facebook](#) [felmérés](#) [privátszféra](#) [közösségi oldalak](#) [eset](#)

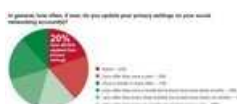
Ezzel a nyakatekert, magyartalan de sokat használt fordulattal vezetjük fel az ESET legfrissebb felmérését, melyben olyan **hétköznapi szokásokról** érdeklődtek, mint például mikor változtattad meg a jelszavadat utóljára, vagy mikor állítottad-ellenőrizted legutóbb az adatvédelmi beállításaidat a közösségi oldaladon - ha egyáltalán. Tornyosultak a strigulák a "soha" oszlop mellett.



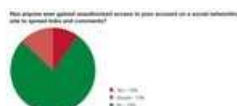
Hogy [Magyarországon mennyien vannak a digitálisan](#) érettek és [éretlenek](#), arról is lehet egyfajta képünk, ám **ha nem csak azt nézzük, ki mit használ, hanem azt is, hogy azt mennyire biztonságos módon, biztonság tudatosan teszi**, az bizonyára jóval kisebb tortaszeletet reprezentál. [Az ESET amerikai felnőttek körében nemrég elvégzett kutatása szerint](#) például a közösségi oldalakon jelszavukat soha nem változtatók aránya 33%, magyarán a felhasználók harmada egyszer megadja, aztán kalap-kabát és többet nem foglalkozik vele.



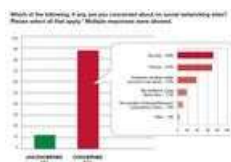
Ha a Facebook esetén rendszeresen változó biztonsági beállításokat nézzük, akkor **legalább a beállítások és/vagy felhasználói szerződés változása esetén** (esetleg ha valamilyen incidensről olvasunk) érdemes volna ezeket felülvizsgálni, módosítani, már az is több, mint a semmi.



Arra a kérdésre pedig, hogy észlelték-e már, hogy valaki jogosulatlanul érte el a közösségi oldalhoz tartozó accountjukat, **10% mondta, hogy már tapasztalt ilyet**. Itt a biztos szavazók mellett nyilvánvalóan van valamilyen kisebb-nagyobb látens százalék is, amely nem is vette/veszi észre (időben), ha ilyesmi történik vele.



Amikor viszont azt nézzük, **mitől tartanak leginkább a közösségi oldalakon, akkor az aggodalmak jól mutatják, hogy mindattól, amiért sokan a kisujjukat sem mozdítják: biztonság, privátszféra sérülése, hamis profilok és egyéb visszaélési lehetőségek**. [Az erős jelszóról](#) és a megfelelő biztonsági kérdésekről már mi is sokat papoltunk ehelyütt, és sokszor emlegettük [elrettető példaként a Sarah Palin esetet](#) is.



Jótanácsként az erős, és viszonylagos rendszerességgel cserélt jelszó használatának fontosságát emelhetjük ki, ismeretlen nyitott wifin ne lépkedjünk be semmilyen fiókunkba, tájékozódjunk a neten vagy barátainktól [a biztonságos és privátszférát védő beállítási lehetőségekről, programokról, technikákról](#), valamint érdemes [rendet tartani az ismerősök kezelésében](#) is. Ez nem strigula bajnokság, vagy póker játszma, kinek nagyobb vagy kinek van több, [csak valódi ismerősöket jelöljünk be, illetve igazoljunk vissza](#).



Ha a "segíts magadon, Isten is megsegít" mondást vesszük alapul, akkor ezt ebben a kontextusban értelmezve nem baj, ha nem mindenki számítógép guru vagy adatvédelmi non plus ultra, **de azért alapszinten előbb mindenki tegyen meg minden tőle telhetőt sajátmagér** és aztán adott esetben **ne féljen szakértő segítséget sem kérni** a környezetéből, ha úgy érzi, olyan helyzetbe került, amit nem tud

egyedül kezelni.



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Safe mód a Mechagodzilla ellen](#)
- [25-ször több a mobilos kártevő](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3010683>

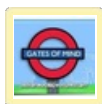
Kommentek:

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



TrueY • <http://qltura.blog.hu> 2011.06.26. 23:43:44

Be kell állítani, hogy 3 havonta kötelező legyen és akkor máris lehet újrarajzolni a grafikonokat. ;)



nemethv • <http://backtotheukblog.wordpress.com>
2011.06.27. 18:21:33

Szerintem azzal egyáltalán nincs semmi gond onmagában hogy valaki kitalál egy viszonylag erős jelszót (mondjuk kis/nagy/+szám de nem extra karakterekkel) és úgy hagyja. Miert kellene változtatgatni állandóan?
Azzal van a baj amikor valaki minden szar appot feltesz vagy a gépére, vagy a facebook accountjára, meg mindenhova rákattint, aztán azok meg szépen kiadják kitűdjahová az adatokat.

ps.

Két számítógépes rendszergazda beszélget:

- Te, hogy lehetsz olyan hülye, hogy a kutyád nevét adod meg jelszónak?
- Miért, mi a bajod azzal, hogy wfK41a2s?



TrueY • <http://qltura.blog.hu> 2011.07.04. 10:53:03

@NViktor: Az a gond, hogy ha sokáig próbálják feltörni, akkor sikerülni fog nekik. Ha legalább 14 karakter és van benne kis/nagybetű, szám és írásjel is, akkor 3 hónap alatt nem nagyon fogják feltörni. De 2 év alatt akár sikerülhet is.

Ha tovább nehezítetted a dolgot, hogy a user neved is hasonló nehézségű, akkor duplán nehezítesz... :)

Hús deka Twitter követőt kérek. Fél kiló maradhat?

2011.06.27. 11:00 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [csalás](#) [twitter](#) [vip](#) [követő](#) [tagság](#) [pénzért](#)

Nem az első, és biztos nem is az utolsó csalás az, amely (ismét) felbukkant és zavart okoz az Erőben. A dolog úgy kezdődik, hogy **kapunk** egy kéréstlen üzenetet egy linkkel: "Ha te követsz engem, én követlek téged, és mindenki jól jár." Vagy nem.



A weboldal aztán kínál VIP szolgáltatást, ami fizetős (hű, de meglepő), vagy pedig lehetőség van ingyenes próbára is (wow, dőlnek a kattintások ;-)) ami párszáz követővel növeli majd a béketáborunkat. Most, hogy a csalit akkor így átbeszéltük, lássuk mi is történik valójában. A külső szolgáltatás - merthát arról van szó - bekéri az azonosítónkat és jelszavunkat ([mint egy jólnevelt Hű](#)) és aki megadja, hát ugye...



Ez a fajta strigulabajnok versenyszellem már [egy hazajáró lélek kötelességtudó rendszerességével](#) teszi legmélyebb tiszteletét az emberi naívság bugyrai előtt, például [alig háromnegyed éve írtak egy pont elég hasonlóról](#). Ott a VIP tagság azzal kecsegtetett, hogy a díj befizetése után napi 400-1000 követőt kapunk. Ezzel a tempóval [röpke 30 és fél éve alatt lenyomhatjuk Lady Gágát a trónról](#), igaz az optimista verziós forgatókönyv szerint, hogy ő közben nem növeli tovább, mi pedig napi ezer új követővel számolunk ;-)) Nosza, a puding próbája az evés, **egy tesztfiókkal elvégzett kísérlet azonban csak azt bizonyította, hogy amikor a pénzt befizették, az be lett fizetve :-)**



Magyarán lett egy semmire jó VIP tagság - tisztára mint a hamis vírusirtó biznicsben, **nem jöttek a beígért követő hegyek**, az account a kutyaké lett és nem mellesleg a kiperkált díjra is keresztet lehetett vetni. Abban Clueley és minden biztonsági szakértő is egyetért, hogy **ilyesfajta alkalmazásoknak sose szavazzunk bizalmat** - dettó, mint [a Facebookon szintúgy visszatérő "Megmondom ki nézte meg a profilodot"](#) című örökzöld és kiirthatatlan opusz.



Soha ne adjuk ki harmadik félnek a név-jelszó párosunkat, ha pedig esetleg mégis megtettük, a korábbi jelszótól gyökeresen eltérő, jelszó változtatási szokásaink ismeretében sem kitalálható, **erős újat válasszunk haladéktalanul**.



[Vagy pedig ne csodálkozzunk](#), és válasszunk valamilyen megbízható erdei búvóhelyet a nevünkben megspammelt, felbőszült ismerőseink haragja elől ;-)

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

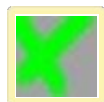
- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Ez történik a weben egy perc alatt](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3017971>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói tartalomnak minősülnek, értük a [szolgáltatás technikái](#) 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/> 2011.06.27. 17:22:41

Hihetetlen, hogy valaki(k) csak úgy tud(nak) ejszaka jól aludni ha a Twitteren van pár ezer követőjük.



[valójábannemberci](#) 2011.06.27. 17:53:10

Hát igen, a pebkac ellen még nincs tökéletes védelem.



[külföldi bankszámla](#) •
<http://www.kulfoldibankszamlainfo.info/> 2011.06.27. 17:53:45

A "megmondom ki követ" az orkut egyik legnagyobb sikerű okossága volt. Aztán jött, hogy meg lehet nézni más profilját úgy, hogy nem jelenik meg automatikusan, na ezt is imádták az emberek.

Autorun és Iframe szélelbelevé jönnek

2011.06.29. 15:40 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [magyar adatok](#) [nod32](#) [eset](#) [havi](#) [threatsense](#) [vírusstatisztika](#)

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



A [Cseh Tamást idéző főcím](#) szerint a Conficker korszak után látszólag Autorun korszak köszöntött ránk. Messzemenő következtetéseket persze még korai lenne levonni, mindenesetre a **korábbi örök második helyezett Autorun vírus már második alkalommal vezeti a mezőnyt**. Mint az közismert, a bűnözők előszeretettel építenek arra, hogy [a legtöbb felhasználó kényelemből nem tiltja le](#) az automatikus futtatást a Windows operációs rendszerek alatt, és ezzel fertőzésnek teszi ki a gépét. Bár a Microsoft felmérése szerint az időközben kiadott frissítéseknek köszönhetően az Autorun veszély **általánosságban csökkenő tendenciát mutat, nálunk ez egyelőre még nem éreztette a hatását**. A **Windows automatikus futtatás funkcióját kihasználó kártevők USB kulcsokon és más külső adathordozókon terjednek**.



Túl sok mozgást ezúttal nem lehetett észlelni a tízes listánkban, egyedül a HTML/Iframe.B vírus megjelenése bolygatta fel némileg a kialakult sorrendet. A hatodik helyre érkező újonc egyfajta gyűjtőneve az olyan vírusoknak, amelyek **HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítják át a böngészőt a felhasználó tudta és engedélye nélkül**.



Ilyen kártékony kódokat tartalmazó **weboldallal manapság már bárhol találkozhatunk**, és rég [nem igaz, hogy emiatt csak a pornográf vagy warez oldalak látogatói lennének veszélyben](#), hiszen banner hirdetések, ártatlan szavakra való Google keresés találatai is tartalmazhatnak ilyet.



Ahogy előző havi statisztikáinkban is utaltunk már arra, hogy internetböngészőnk biztonsági beállításait érdemes rendszeresen felülvizsgálni, továbbá a weblapok látogatása alkalmával automatikusan lefutó, és esetlegesen kártékony JavaScript kódok ellen a **böngészőbe épülő modulokkal is érdemes megerősíteni webes védelmünket**.



Az ESET több százezer magyarországi felhasználó visszajelzéseire alapuló statisztikai rendszere szerint **2011. májusában a következő 10 károkozó terjedt a legnagyobb számban, és volt együttesen felelős az összes fertőzés 22.97 %-áért**.



1. INF/Autorun vírus

Elterjedtsége a májusi fertőzések között: **5.08%**

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.



A számítógépre kerülés módja: Fertőzött adathordozókon (akár MP3-lejátszókon) terjed.

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



2. Win32/Conficker féreg

Elterjedtsége a májusi fertőzések között: 4.68%

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 eljárashívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárason 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.



A számítógépre kerülés módja: 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. JS/Redirector trójai

Elterjedtsége a májusi fertőzések között: 2.48%

Előző havi helyezés: 3

Működés: A JS/Redirector trójai egy olyan kártékony JavaScript, amely lefutva kényszeríti a böngésző ablakokat jelenít meg, emellett hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/redirector>



4. Win32/HackMS trójai

Elterjedtsége a májusi fertőzések között: 1.86%

Előző havi helyezés: 5.

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítésekor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>

5. Win32/PSW.OnLineGames trójai

Elterjedtsége a májusi fertőzések között: 1.99%

Előző havi helyezés: 4.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományaikat és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatokat titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyet aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>

6. HTML/Iframe.B vírus

Elterjedtsége a májusi fertőzések között: 1.32%

Előző havi helyezés: -

Működés: A HTML/Iframe.B 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.



A számítógépre kerülés módja: Fertőzött weboldalakon terjed.

Bővebb információ: Részletes leírása szerkesztés alatt

7. Win32/VB féreg

Elterjedtsége a májusi fertőzések között: 1.32%

Előző havi helyezés: 6.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>

8. Win32/Shutdowner trójai

Elterjedtsége a májusi fertőzések között: 1.27%

Előző havi helyezés: 7.

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>

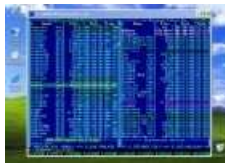


9. Win32/Tifaut trójai

Elterjedtsége a májusi fertőzések között: 0.96%

Előző havi helyezés: 8.

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csres.exe és autorun.inf néven. A kártékony EXE fájl automatikus lefuttatásához külön bejegyzést is készít a rendszerleíró-adatbázisban. Működése során több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21tifaut>



10. HTML/ScrInject trójai

Elterjedtsége a májusi fertőzések között: 0.69%

Előző havi helyezés: 10.

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Akiknek a Captcha kényszerűsége](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/3022201

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.

Magyar átverések a Facebookon

2011.07.01. 10:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [magyar scam facebook veronika adathalászat vv4](#)

Valószínűsíthető, hogy magyar adathalászok dolgoznak a Facebookon. A beugratós módszerrel gyűjtött e-mail címeket feltehetően kéretlen reklámok küldésére használják.



A Facebook üzenőfalán megjelenő, általában meglehetősen féltékeny képet, videót és sztorit tartalmazó bejegyzések sokszor olyan kártékony alkalmazásokhoz vezetnek a felhasználókat, melyek célja, hogy megszerezzék a személyes adataikat. A <http://facebook.com/biztonsag> oldalon keresztül az ESET magyarországi képviselete folyamatosan gyűjti a Facebook átveréseket, az oldal rajongóit pedig figyelmezteti ezekre. Itt jelezte a napokban több felhasználó, hogy magyar nyelvű átverésekkel találkozott a közösségi portálon.



Az egyik leginkább terjedő üzenet szerint "VV4 Veronika meztelenül pózolt a görög televízióknak". A felhasználók számára nehéz megállni, hogy ne kattintsanak le egy ilyen üzenet. Azok pedig, akik bedőlnek az átverésnek, önkéntelenül átadják adataikat - többek között nevüket és e-mail címüket - az alkalmazás készítőinek, majd az üzenetet maguk is kiposztolják saját üzenőfalukra, ahol az összes ismerősük látja azt.



A készítőik célja valószínűleg az, hogy kéretlen reklámlevelek küldéséhez használják fel a megszerzett adatokat. Sajnos túl könnyű egy ilyen átverést leprogramozni és útjának indítani, és viszonylag gyorsan építhető fel egy pár tízezer e-mail címből álló adatbázis. Kiss Zoltán Gergő, az ESET vírusszakértője szerint a magyar nyelvű adathalász alkalmazások háttérében akár hivatalos üzleti vállalkozások is állhatnak. Mivel a most észlelt átverés egy hazai ingyenes tárhelyszolgáltató oldalára mutatott, a szakember szerint valószínűsíthető, hogy magyar adathalászok állnak a háttérben.



Óvakodni kell azoktól a Facebook bejegyzésektől, melyekhez szerzőjük nem fűzött személyes megjegyzést. Egy pár szavas komment már segít azonosítani, hogy a bejegyzést valóban az ismerősünk írta, nem pedig egy automatikus adathalász alkalmazástól származik. Az erotikus vagy meglehetősen féltékeny képet, videót és történetet ígérő, személyes megjegyzés nélküli üzenetek viszont a legtöbb esetben adathalász alkalmazásoktól származnak.

 Tetszik  117 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0

Ajánlott bejegyzések:

- [Akiknek a Captcha kényszerítés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szösölmédia" és nyaralás](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3029408>

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 hatodik szenved

2011.07.04. 18:15 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [ausztrália](#) [kár](#) [identity theft](#) [cert](#) [személyiséglopás](#)

Egy friss tanulmány szerint **minden hatodik ausztrál netező szenved el** valamilyen személyiséglopással kapcsolatos incidenst.



Az ausztrál [CERT](#) a napokban [negyedmillió üzleti felhasználót értesített kompromitálódott belépési azonosítójáról](#). A főügyész emellett azt is javasolta nekik, hogy **a haladéktalan jelszó cserén kívül vizsgálják meg biztonságukat, és tegyenek lépéseket** a jövőbeni hasonló veszélyek elkerülése érdekében. Egy 1200 felhasználót magában foglaló felmérés eredménye szerint az ausztrál **netezők több, mint 15 százaléka** szenved el [valamilyen személyiség lopással kapcsolatos eseményt](#).



A leggyakoribb forgatókönyv **a személyes adatok ellopása után, hogy az áldozat valamilyen kézzelfogható, hitelkártyával kapcsolatos konkrét anyagi veszteséget is elszenved**. Az ellopott személyes és banki adatok birtokában a bűnelkövetők legtöbbször valamilyen online szolgáltatást vesznek igénybe vagy valamilyen webáruházból beszerezhető nagyértékű terméket rendelnek a lopott account terhére, de gyakran **hamis kölcsönügyletek is indulhatnak az eredeti tulajdonosok nevében és kárára**.



Mivel a modern életben az online üzletmenet egyre elterjedtebb, **minden erőfeszítést meg kell tenni, hogy az [ezzel járó megnövekedett kockázatokat](#) kezelni lehessen**. Többek közt emiatt is vezettek be az Ausztráliában új, **szigorúbb jogszabályokat a nemzetközi számítógépes bűnözéssel** kapcsolatosan.



[Amit emellett bárki megtehet](#), az az erős jelszavak használata, a [biztonságtudatos hozzáállás](#) (nem hiszek el mindent, nem kattintok mindenre), rendszeresen ellenőrizzük bankszámla egyenlegünket, még a kisösszegű terheléseket is. Gyakori módszer, hogy a lopott hitelkártya adatokat előbb letesztelik, és fél-egy dollárt utalnak róla valamilyen jótékonyági szervezetnek (például Vöröskereszt), majd ha a tranzakció sikeres, utána vesznek le csak nagyobb összeget vagy adják tovább a feketepiacon. Egy korábbi [Operás nemzetközi felmérésből jól látszott](#), hogy **bár a felhasználók jelentős része fél, nem minden esetben tesznek meg minden tőlük telhetőt ezek elkerülésére**.



A statisztikák szerint Ausztráliában **évente 15 milliárd dollár az az összeg, amelyet a szervezett elektronikus bűnözés bezsebel**. A hatóságok védekezéséről szóló hírt azonban kissé beárnyalhatja az a tény, hogy az AntiSec keretében feltört, ellopott és [nemrég nyilvánosságra hozott bizalmas adatok között](#) az ausztrál választásokkal kapcsolatos kormányzati adatbázisok is ott szerepeltek.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:



- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3037223>

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](#).



TrueY • <http://qltura.blog.hu> 2011.07.05. 09:54:17

Nálunk erre még nincs szükség. Ha felhajtunk egy hajléktalant, akkor annyi céget vehetünk az ő nevében, hogy nosza és még csak nem is fognak nyomozni utánunk (l. Simicska).

Felfedezték az első 64 bites botnetkártevőt

2011.07.06. 15:40 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [kaspersky botnet rootkit eset bit 64 tdss x64 tdl 4](#)

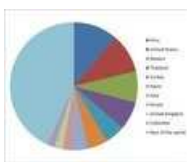
Az ESET és a Kaspersky kutatói egy olyan új botnetes kártevőt azonosítottak be, amely **64 bites rendszereket** is képes megfertőzni.



Szokatlanul mondható, hogy egy kártevő képes legyen a **64 bites rendszereket is támadni**, ami azt jelenti, egy egészen újszerű kódról lehet szó - nyilatkozta David Harley. Vagyis [a kártevő terjesztők részéről nem csupán kisebb módosítások vagy javítások, hanem komoly fejlesztések történnek](#), erre utalnak többek közt a számítógép újraindítást túlélő mechanizmus eddig megismert technikai részletei is.



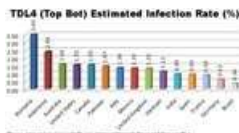
Az ESET kutatási eredményeit megerősítette a Kaspersky Lab is, miszerint a **TDL-4 fejlesztők egy olyan, a korábbinál sokkal ellenállóbb botnet létrehozását tűzték ki célul**, amely mind [a konkurens botnetes versenytársak támadásai](#), minden pedig az antivírusok felismerései ellen védettebb.



[A fertőzés terjesztése a "hagyományosnak" mondható affiliate partneri módszerrel történik](#), ebben a rendszerben **fejpénzt fizetnek a megfertőzött számítógépek után**. A bűnözőknek még arra is kiterjed a figyelme, hogy a malware kódok minél kevésbé vagy lassabban kerüljenek a vírusirtó cégek laborjaiba, így a **"partnerek" figyelmét felhívják, ne töltsék fel a kódot kíváncsiságból olyan tesztoldalakra, mint például a VirusTotal**.



Köztudott, hogy a VirusTotal automatikusan továbbítja az egyes gyártók részére a fel nem ismert mintákat, így idővel be tudnak kerülni a felismerési adatbázisba. **Helyette a bűnözők saját ellenőrzést kínálnak, amely a bérelt szolgáltatás részeként óránként ellenőrzi az EXE kódokat a különféle vírusvédelmi programokkal.**



Mint az közzismert, [a fertőzött botnetes gépek végzik a hamis antivírusok, kéretlen adwarek és spamek terjesztését világszerte](#), így a bűnözők viszonylag [olcsó, havi 100 dollárért kínált anonim szolgáltatása](#) komoly kihívás elé állítja a szakmát, valamint a decentralizált, szerver nélküli botnet hálózat is jócskán megnehezíti a feltérképezésüket. A biztonsági szakemberek szerint valószínűsíthetően további 64 bites

rendszerekre tervezett kártevő is megjelenhet majd a közeljövőben.



6 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- ["Szósölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3043896>

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](#).



[A szerelő 2011.07.07. 02:03:44](#)

Kitaláltam egy mikrokontrolleres megoldást, ami figyeli a bios-t és a boot szektort, nem engedi megváltoztatni csak ha engedélyezve van ill. jelez ilyen kísérletnél. Ezen szoftver nem megy át :)

Nincs hamis AV banki szemhunyas nélkül

2011.07.08. 13:05 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [bank csalás](#) [hamis antivirus](#) [pénzvisszafizetés](#) [fizetésközvetítő](#)

Ahogy régebben nem volt karácsony Corvin nélkül, úgy az "egyedül nem megy" szellemében a hamis antivirus üzletből élők sem tudnának hosszú ideig nyereszkédni bizonyos körülmények, együttállások és egyes bankok támogatása vagy tudatos félrenézése nélkül.



A múltkori posztunkban a botnetes kártevőknél beszéltünk arról, hogy [a bűnözőknek még arra is kiterjed a figyelme](#), hogy bérelhető botnethez használatos fertőző malware kódok minél kevésbé vagy lassabban kerüljenek a vírusirtó cégek laborjaiba, így a "partnerek" figyelmét felhívják, ne töltsék fel a kódot kíváncsiságból olyan tesztoldalakra, mint például a VirusTotal. Köztudott, hogy a VirusTotal automatikusan továbbítja az egyes gyártók részére a fel nem ismert mintákat, így idővel be tudnak kerülni a felismerési adatbázisba. Helyette a bűnözők saját maguk kínálják ellenőrzést, amely a bérelt szolgáltatás részeként óránként ellenőrzi az EXE kódokat a különféle vírusvédelmi programokkal.



Ugyanez a leleplezést lassító, elkerülő taktika figyelhető meg a pénzügyi területen is - ugye ha Al Caponet el akarjuk fogni, akkor adócsalásért lehet. Elvileg a fizetésközvetítő cégek éberben figyelnek arra, ha valaki elégedetlen a vásárolt áruval, akkor a szerződő partnerek biztosítsák a pénzvisszafizetési garanciát, ellenkező esetben gyanússá válhatnak, illetve a fizetésközvetítő (pl. PayPay, AlertPay, ChronoPay, stb.) ideiglenesen vagy véglegesen kitiltja őket, és akkor ezzel elzárja a pénzcspapot. De szintén elvileg azt is figyelik, ha valahol pedig túl nagy számban történik pénzvisszafizetés, akkor ott valószínűleg kétes üzelmek zajlanak. Ezért aztán a hamis antivirussal foglalkozók pedánsan a nem feltűnő megfelelő szinten tartják ezeket a mutatóikat.

Category	Malware	Number of samples	Number of victims	Number of payments
AVG	AVG	1,000,000	100,000	10,000
AVP	AVP	1,000,000	100,000	10,000
AVS	AVS	1,000,000	100,000	10,000
Total		3,000,000	300,000	30,000

Csak egy apró példa, a sorozatban trükköző amerikai "üzletember" egyik magyarokat is beszippantó pilótajátéka, a 7 Day Wealth nevű csalás, ahol a játék 2010. októberi bedőlése, a weblap komplett eltűnése és a pénz vissza nem fizetése után újabb, hasonló jellegű, de teljesen más nevű pilótajátékok indultak. Ekkor a mindezt szervező Company Express nevű cég eleinte időt húzott, majd azt a módszert választotta, hogy egy keves számú embernek a pénze negyedét visszafizette - jellemzően azokat, akik a fizetésközvetítőnél hivatalos úton panaszt nyújtottak be - és ezzel elültette a reményt a többi várkozóban, és elkerülte a számlájának zárolását, látványosan "jószándékot mutatott", majd pár hónap időhúzás után a maradék ellopott pénzzel szépen ellovagolt a naplementébe. [A csalódott károsultak majd egy év után a mai napig is reménykedve levegöznek](#) még egymással a témában.



Akár hisszük, akár nem, ez az egy héten belüli [pénzvisszafizetési garancia jelen van a hamis antivirus biznicsben is](#). Ha valaki nagyon mérgesen, az üzletmenetet veszélyeztetve fellép a saját érdekében, a számla folyamatossága és a botrány elkerülése érdekében a hűzongókat gyorsan kártalanítják jól tudva, a nyereség maximalizálása érdekében megéri ez a kis áldozat az esetek 1-3 százalékában, mert a fizető csendes többség szegyenében, idő hiány miatt vagy mert esélytelennek érzi nem panaszkodik, nem fordul hatóságokhoz, hanem lenyeli az 50-100 USD egyszeri veszteséget. A tényleges vásárlási ráta körülbelül 2%, például az egyik tanulmányozott esetben 8.4 millió telepítés közül 189 342 végződött tényleges "vásárlással", ami vagy egy 6 hónapos, 1 éves licencet jelent 40-60 USD ellenében, vagy van élethosszig tartó konstrukció is :-). 80 USD befizetésével, ez éri ám csak meg igazán :-). Így jön össze a hamis antivirus csalásoknál jellemzően kb. 50 millió dolláros (9.1 milliárd HUF) évi bevétel.

FMBE Bank Limited, Cyprus (SWIFT Code FMBE2222)
Bank Hapoalim BM, Israel (SWIFT Code HAPALI)
Ceska Sporitelna A.S., Czech Republic (SWIFT Code CIBACZ22)
International Bank of Azerbaijan (SWIFT Code IBAZAZ2X)
JSCB Bank Standard, Azerbaijan (SWIFT Code MOSAZ222)

Ennél is tovább megy az az alapos tanulmány, amelyet Brian Krebs weboldalán tett közzé, és a University of California készített a szervezett bűnözés keretében folyó hamis antivirus üzletmenet pénzügyi vonatkozásairól. A több hónapos vizsgálódás eredményeként nem kevesebbet állít, minthogy egyes bankok és a fizetésközvetítő cégek tudva tudják ugyan, hogy mi is történik valójában, ám

mivel közvetlen hasznuk származik belőle, nem tesznek ellene az égvilágon semmit. A csalók pedig több számlát használva, vagy ezek rendszeres, például havi csereberejével is operálnak. **A biztonsági kutatók szerint a VISA és a Mastercard rendszerében is elvileg ott lehetne valamiféle megoldás,** hogy az ilyen gyanús folyamatokat, cégeket, tevékenységeket hatékonyabban kiszűrjék, ha nagyon akarnák.



A harc jegyében ezen a fronton is el lehetne indulni, vélhetően [ha majd a ChronoPay-hez hasonlóan](#) elvezetik borszíjon egy-két további itt felsorolt azerbajdzsán, ciprusi és egyéb pénzügyi intézet főnökét, gyaníthatóan varázsütésre meg is jönne majd a kedv a többieknél az alaposabb ellenőrzésre, a törvényesség betartásának fokozottabb fontosságára. Addig azonban ...

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3049687>

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.

Amikor mások baltázzák el - part III.

2011.07.12. 11:00 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [biztonság](#) [jelszó](#) [post](#) [washington](#) [álláskeresés](#)

Jelent meg itt több hasonló poszt, amelyeknek lényege, hogy [hiába kezeljük mi a gépünket és személyes adatainkat bármilyen gondosan](#), ha a táplálkozási lánc egy másik és eléggé jelentős [felsőbb láncszeme ezenközben](#) erősen gyengélkedik.



Lehet az ember egyébként bármilyen óvatos, haladócsoporthoz tartozó biztonságtudatos, sőt enyhe fokon paranoid, ha az álláskeresési információi, accountja egy harmadik helyen nem védett megfelelően. Pontosan ez történt a Washington Post esetében, ahol [június utolsó napjaiban 1.27 millió belépő azonosító ID adata és emailcíme kerülhetett illetéktelen kezekbe](#), bár a cég közlése szerint állítólag jelszóadatok nem kerültek ki.



A WP elnézést kért az incidensért, a támadást lehetővé tevő sebezhetőséget pedig befoltózták. Pontosan nem tudni, milyen hatása lesz az eltulajdonított adatoknak, de mivel [erősödő tendenciaként rajzolódik ki a tömeges spam és kártevő küldés helyett a kis számú, de egyre szofisztikáltabban jelentkező konkrét célszemélyre vagy csoportokra testreszabott támadó kampányok](#) megjelenése, így [a kikerült email címek tulajdonosait várhatóan álláskereséssel kapcsolatos levelekkel lehet majd hatékony támadni](#).



Könnyen elképzelhető, hogy nem ez volt az első (bevallott) és utolsó ilyen, álláskeresők tömeges adataira utazó támadás. Emiatt lassan át lehet állni arra, hogy [nem csak a kéretlen leveleket, üzeneteket, az ezekben küldött kéretlen linkeket és fájlmelléleteket érdemes kellő óvatossággal](#) elutasítani vagy alaposan ellenőrizni, hanem tulajdonképpen minden ilyen.



Ebben [a vírusirtó webes forgalom szűrése, és URL feketelistája](#), valamint böngészőnk [megfelelő kiegészítő moduljai](#) tehetnek jó [szolgálatot](#) - természetesen a [józan ész és a megfelelő óvatos hozzá állás](#) mellett.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Akiknek a Captcha kinszenvedés](#)
- [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/3059818

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.

Vágtass velem!

2011.07.15. 12:40 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [weboldal orosz per to terjesztés install kártevő ready ride ppi pay](#)

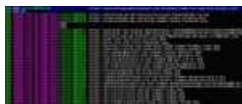
Egy korábbi posztunkban [már megemlítettük a PPI, azaz Pay Per Install](#) kártevő terjesztési rendszert, most pedig pontosan **egy ilyen konkrét szisztémát mutat be részletesen az ESET Threat Blog, íme az orosz származású Ready To Ride.**



[Itt nem nagy hegyeken és zord napokon át](#) kell vágtatni, hanem nemes egyszerűséggel [pénzkereseti lehetőséget ajánl a kártevők terjesztéséért a rendszer](#). Amint azt Aleksandr Matrosov és Eugene Rodionov felfedezte, a Win32/Cycbot kártevő családot terjesztő hálózat ilymódon toboroz önkénteseket, **kétes kereseti lehetőséggel csábít és építi folyamatosan botnethálózatát.**



Az ezer telepítésenkénti 400 USD bevétel valószínűleg sokakat elcsábíthat, és **nemcsak az Oroszországi Föderáció területében kell itt gondolkodni**, hiszen nem véletlenül szerepel az orosz/angol nyelvválasztó zászlócska: az egyik kiemelt célterülete például éppen az Egyesült Államok.



A sikeresen telepített botnet képes részletes riportot szolgáltatni a használt számítógépről, **meghatározható vele, hogy pontosan milyen antivírus program fut a gépen - ha fut rajta ilyen egyáltalán, és amint újabb Win32/Cycbot változat jelenik meg, az automatikusan képes frissülni az új verzióra**, de emellett önellenőrzést is tart, ha azt észleli, valamilyen komponensének futása esetlegesen leállításra került.



A domain 2010-es lefoglalása óta **próbálják a jelentősebb keresők (Google, Bing, Yahoo) találatainak mérgezésével, a linkek észrevétlen átirányításával terjeszteni a fertőzést.** Igen hatékony lehetőség például a JavaScriptes kód módosítása vagy beszúrása weboldalakba, és ahol nincs kézbe tartott script védelem, ott sikeresen meg is történhet a fertőzés.



Emellett a népszerűbb böngésző kliensek (Internet Explorer, Opera, Firefox) esetében **a proxy beállítások manipulálásával is bármilyen átirányítást képesek végrehajtani.** A Win32/Cycbot egy többszálú alkalmazás, amely több tucat feladatot, kéretlen hirdetés megjelenítést vagy webes URL átirányítást tud **villámgyorsan megvalósítani a vezérlő C&C szerverről kapott távoli utasításoknak megfelelően.**



Az említett Ready To Ride weboldal sajnos jelenleg is elérhető, mondhatni éppen felnyergelték azt egy németországi szerverre, aminek nem igazán örülhetünk, mert biztosan nem ilyen lovat akartunk. Az emberi természetet ismerve biztosak lehetünk benne, **ezekben a percekben is vannak olyanok, akik éppen ezt az utat választják maguknak a pénzkeresethez.**



0



□jánlott bejegyzések:

- [□yerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3069492>

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.

Vége itt a nyár, az ATM skimmer vár

2011.07.18. 12:51 | [Csizmazia István \[Rambo\]](#) | [12 komment](#)

Címkék: [csalás](#) [automata](#) [atm](#) [pénzkiadó](#) [skimmer](#)

Az impulzív cím dacára komoly, vagy inkább fontos dolgokról lesz szó. **Mire figyeljünk egy pénzkiadó automatánál, hogy a "moddolt" elemeket sikeresen kiszúrjuk**, illetve milyen egyéb hasznos pénzkivételi szokásaink legyenek, hogy amíg anyu öltözik, addig apu ne legyen ideges.



[Minden más számítógép mod szem-szájnak ingere](#), ám az ATM-eknél valamilyen rejtélyes okból kifolyólag nem igazán szeretjük ezt a műfajt;-) [A miniaturizálás korszakában már nem úgy valamilyen rafinált elemet úgy felszerelni](#), felragasztani egy automatára, hogy az első látásra, második látásra, sőt sokadik látásra is gyárinak, eredetinek tűnjön.



Az alap elemek [lehetnek második billentyűzet az elsőre ragasztva](#) - továbbítva a leütéseket a csalóknak, van aztán a **másodk gyűrű a kártya olvasó nyílásnál**, ami szintén el- és beolvassa a kártyaadatokat. A pénzkiadó és a kártya nyílás blokkolása is egy standard módszer, a segítő idegen ekkor tanácsolja, menjünk panaszra a bankba, akár el is kísér (előtte jól lekaparja a bank telefonszámát tartalmazó matricát) - közben a segítője kipiszkálja a pénzt/kártyát és eltűnik.



Az idegen test lehet valamilyen díszítőcsík, prospektustartó is, ami extra kamerát rejt, mellyel a PIN kód megfigyelésére nyílik lehetőség, de ezt BlueTooth eszközzel végezhetik akár egy közelben parkoló gépkocsiból is. Ha megvan nekik a PIN kód, akkor vagy ellopják a kártyát fizikailag is [vagy a második olvasógyűrűvel másolják, klónozzák, és máris leemelhetők lesznek az összegek](#) - **persze a leleplező SMS értesítésig akinek van ilyen**, ennek hiányában csak a hónap végi egyenleg olvasás közben kell majd repülősöt szagolni a heveny szédülés ellen.



Jóteknony dolog lehet, ha nagyforgalmú, jól belátható, esetleg magában a biztonsági őrrrel és ipari kamerával biztosított banki automatában veszünk fel pénzt - itt a legkisebb az esélye az esetleges megpiszkálásnak idegenek által. Sötét, ismeretlen helyen, vagy ahol az automata éjszaka felügyelet és jó rálátás nélkül esetleg manipulálható, nem érdemes reszkírozni. Célszerű lehet **rendszeresen egy adott ATM-et használni**, ekkor a legnagyobb az esélye, hogy a váratlanul megjelenő idegen elemeket idejében sikeresen felfedezzük.



Érkezéskor meg lehet tapogatni a pénzkidó és kártyabeolvasó nyílás bemenetét, emellett érdemes letakarni a kezünket a PIN kód begépelésekor, illetve [ha valaki hátunk mögött túlzott érdeklődést mutat](#), akár el is halasztani a tranzakciót és távozni. Ugyancsak **érdemes a távozást választani, ha az automata sérült, hiányos, horpadt, vagy ragasztónyomok látszanak rajta.** [A pénzkivétel fontos dolog](#), ezért bár meleg az idő, sose siessünk annyira, hogy nem figyelünk ezekre a részletekre.



A PIN kódot **never-ever** tartsuk a tárcánkban közvetlenül a kártya mellett, használjunk limit korlátozásokat az egyszeri tranzakciókhoz a nagyobb veszteség elkerülése érdekében. Ugyancsak hasznos, ha a PIN kódot nem csak úgy olvashatóan beírjuk a telefonunk noteszába, azt el is veszíthetjük vagy megbízhatatlan szervizeshez kerülve illetéktelen kezekbe kerülhet. Ugyancsak óvakodjunk ilyen bizalmas adatot online dokumentum kezelőben, például Google naptárban tárolni. Amikor [ez a 2007-es cikk készült, és ismeretlen emberek Calendar bejegyzéseit is olvasgathatta bárki, számtalan PIN kódos bejegyzést lehetett itt anno olvasni.](#)



[Minden ellen persze nincs orvosság](#), de azért ha bármilyen gyanús dolog történt, a gép nem adja ki a pénzt, a Mégse gombra visszatartja a bankkártyát, **haladéktalanul lépünk kapcsolatba a bankunkkal, és szükség esetén tiltassuk le a kártyát.**



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



Ajánlott bejegyzések:

- [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](#)
- ["Szösölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/3076287>

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](#).

[atila68 \(törölt\) 2011.07.18. 18:53:24](#)

Személy szerint csak(!) bankfiókban elhelyezett automatánál tranzaktálok, lehetőleg olyan helyen ahol a helységbe (ha van) csak kártyával lehet belépni.

Vészhelyzetben Tescoban elhelyezett ATM, szerintem elképzelhetetlen, hogy észrevétlenül megbuherálhassa bárki is.

[nzo 2011.07.18. 20:31:20](#)

[@atila68](#): Amúgy felhívpm a figyelmedet arra, hogy az sem biztosíték, hogy csak olyan helyre mész be, ahol bankkártya nyitja az ajtót. Jó ha tudod, hogy oda bármilyen mágneses kártya (pl. tesco hűségkártya, Lidl kártya, stb.) jó, nem kell használni a bankkártyádat. Sőt, inkább ne is qazt használj, mert oda is szoktak fals kártyalehúzókat tenni. Az Unicredit pl. már le is szerelte ezeket, egy sima gombbal nyitható az ajtó.

n80qd 2011.07.18. 20:35:57

@nzo: Volot, ahol nem ezért szerlték le az ajtó nyitó kártyaolvasókat, hanem mert az emberek nem tudták használni. :)

Egyébként az emberek nagy része annyira agyatlan, hogy nem csak egy plusz feltétet nem vesz észre egy atm-n, de ha mondjuk fogna valaki egy nagy papir dobozt, kiszinezne, ráírná pár bank nevét, és kiülne egy forgalmas helyre, azt is atmnek néznék, és tolnák be a kártyájukat ész nélkül :D :D :D :D

nzo 2011.07.18. 20:49:22

@n80qd: Hidd el, Te sem vennéd észre, elsőre, hogy moddolt atm-t használsz.

n80qd 2011.07.18. 20:59:20

Hááát... sajnos észrevenném... :D (Áll mögöttem vagy 16 éves atm szervizesi tapasztalat)

Kiszámoló • <http://kiszamolo.hu/> 2011.07.18. 22:45:33

@n80qd: ezért szedték le. Mert még a pin-t is bepötyögték a lelkes emberek a csalóknak.

Aki ellen meg volt (csövesek pl.) annak meg már mindnek van kártyája.

Kiszámoló • <http://kiszamolo.hu/> 2011.07.18. 22:49:44

Kedves blogíró ,nem bántani akarlak, hanem bátorítani: ebből a témából egy nagyon jó cikket lehetett volna írni, ez meg elég soványka lett. Nincs kedved jobban körbejárni a témát?

Hogyan védekeznek a bankok (zöld előtét, remeg a kártya, amikor behúzza, chipkártya, stb, stb), ezt hogyan játsszák ki a tolvajok.

Hogyan lopják nagyüzemben a kártyát internetes felhasználásra.

Stb.

n80qd itt is van, biztos segít neked. :)

Várjuk a profi folytatást. :)

Kiszámoló • <http://kiszamolo.hu/> 2011.07.18. 22:52:26

@n80qd: volt egy olyan csalás, hogy egy cég vett hivatalosan egy atm-et, kirakta egy westend méretű bevásárlóközpontba és várt.

Jöttek sorba a népek, kártya be, pin kód be, a gép kiírta utána, hogy jelenleg nincs elég pénze az automatában, bocs. Kártya vissza.

Zseniális.

Jackni Konzol 2011.07.18. 23:36:00

Anti! Hol itt a vírus?

n80qd 2011.07.19. 06:59:47

@Kiszámoló: Sajnos az eddigi tapasztalatom ez, az emberek szinte bármibe beleerőszakolják a kártyájukat, nem néznek semmit, és nem gyanakszanak semmire... :(



Csizmazia István [Rambo] <http://antivirus.blog.hu> **2011.07.19. 08:47:59**

Szia Kiszámoló!

A zöldelőtét, meg rezege a kártya jó dolgok, és folyamatosan változnak, javulnak a módszerek. Az igazán szomorú azonban valóban az, ha egy szakállas trukknek meg evek múlva is bedolnek egy csomóan. Még a megboldogult eredeti IPM magazinban volt egyszer egy összefoglaló, ahol egy Donald kacsa képregényben szerepelt, hogy egy papírdobozt tett a bank bejáratahoz: elnevezést, technikai hiba, kerjük ide betenni a pénzt, és 3 órán belül lekonyveljük. Ember ezt vette mintának, és egy az egyben mukodott. Akinek nem erre a rugóra jár az agya, nem hajlando vigyazni, az csak saját karan tanulja meg végül.

@n80qd: ha gondolod és van kedved felvenni velem a kapcsolatot, dobj egy emailt.

@Jackni Konzol:

Minden számítógéppel elkövetett csalás, kémkedés idetartozik már az IT biztonság témakörbe. Ha valaki kap egy bankinak látszó adathalász levelet, akkor hol az Anti, hol a Virus? De van helyett megadott account, és ha azt vesszük, a mai kartevek donto többsége sem klasszikus, fájlfertőző vírus, hanem trojai, fereg, stb. Ennek ellenére "virusirtot" használunk ellene, és nagyon is ontópik szerintem, ezért érintjük időnként, és fogjuk is.



Pista bá **2011.07.19. 13:49:29**

[@n80qd](#): a skimming miatt szedték le

Az Autorun az új király

2011.07.20. 10:55 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [magyar adatok nod32 eset havi threatsense vírusstatisztika](#)

Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik a hazai felhasználók számítógépeit. Úgy tűnik, ezúttal egy Autorun korszak vette kezdetét, ezt látszik igazolni, hogy immár megszakítás nélkül harmadik hónapja listavezető.



Ha végignézzük a Microsoft az automatikus futtatással terjedő fertőzések ellen megtett erőfeszítéseit, azt láthatjuk, évekig kivárt a hatékony közbeavatkozással. Először aztán a Windows7 esetén kapcsolták ki végre alapértelmezetten az Autorunt, a régebbi operációs rendszerek esetén pedig előbb csak egy választható javítófoltként elkészített kikapcsolás készült, majd végül a rendszeres biztonsági frissítések közé is beemelték ezt. Vajon mi lehet mégis az oka annak, hogy miközben a Microsoft saját felmérése szerint az időközben kiadott frissítéseknek köszönhetően az Autorun veszély általánosságban csökkenő tendenciát mutat, nálunk ez egyelőre még nem éreztette a hatását?



Az észlelések azt mutatják, hogy a kártevők még mindig széles körben próbálkoznak ezzel a módszerrel, hiszen a korábbi Windows verziók, vagy a hivatalos támogatásból már kikerült OS változatok, valamint a nem legális Windows példányok esetén a biztonsági frissítések egyáltalán nem történnek meg. Az ESET ThreatSense.NET rendszerben észlelt fertőzési kísérletek összesített eredményei pedig azt mutatják, hogy a fenti okok miatt a kártevő terjesztők még jó ideig fognak próbálkozni, így ezek nyilvánvalóan jó ideig befolyásolják, átírják az arányokat a toplistákban is.



Túl sok mozgást ezúttal sem történt a tízes listánkban, egyedül talán a Win32/Tifaut trójait kiszorító JS/TrojanClicker.Agent ismételt felbukkanása fodorozta fel a víztükröt. A rögtön harmadik helyen szereplő JS/TrojanClicker.Agent trójai egy olyan kártékony JavaScript kód, amely lefutva kártékony kódokat helyez el a Windows kulcsfontosságú (Windows, Windows/System32) mappáiba, és az ott el található fertőző komponensek automatikus lefutását biztosító Registry bejegyzéseket készít, amelyek a számítógép minden újraindítása után lefutnak. Ezen felül hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



Az ESET több százezer magyarországi felhasználó visszajelzése alapján statisztikai rendszere szerint 2011. júniusában a következő 10 károkozó terjedt a legnagyobb számban, és volt együttesen felelős az összes fertőzés 24.67 %-áért.



1. INF/Autorun vírus

Elterjedtsége a júniusi fertőzések között: 5.50%

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.



A számítógépre kerülés módja: Fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun>



2. Win32/Conficker féreg

Elterjedtsége a júniusi fertőzések között: 4.00%

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 eljárás 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.



A számítógépre kerülés módja: 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 trójai

Elterjedtsége a júniusi fertőzések között: 3.22%

Előző havi helyezés: 10.

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



4. JS/TrojanClicker.Agent trójai

Elterjedtsége a júniusi fertőzések között: 2.80%

Előző havi helyezés: -

Működés: A JS/TrojanClicker.Agent trójai egy olyan kártékony JavaScript kód, amely lefutva kártékony kódokat helyez el a Windows kulcsfontosságú (Windows, Windows/System32) mappáiba, és az ott el található fertőző komponensek automatikus lefutását biztosító Registry bejegyzéseket készít, amely a számítógép minden újraindítása után lefut. Ezen felül hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



A számítógépre kerülés módja: A felhasználó maga telepíti.

5. Win32/HackMS trójai

Elterjedtsége a júniusi fertőzések között: 2.15%

Előző havi helyezés: 4.

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítésekor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>

6. Win32/PSW.OnLineGames trójai

Elterjedtsége a júniusi fertőzések között: 1.74%

Előző havi helyezés: 5.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományaikat és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatok titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>

7. JS/Redirector trójai

Elterjedtsége a júniusi fertőzések között: 1.48%

Előző havi helyezés: 3

Működés: A JS/Redirector trójai egy olyan kártékony JavaScript, amely lefutva kényszeríti a böngésző ablakokat jelenít meg, emellett hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalakról.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/redirector>

8. Win32/VB féreg

Elterjedtsége a júniusi fertőzések között: 1.38%

Előző havi helyezés: 7.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) férgek hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



9. Win32/Shutdowner trójai

Elterjedtsége a júniusi fertőzések között: 1.21%

Előző havi helyezés: 8.

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>



10. HTML/Iframe.B vírus

Elterjedtsége a júniusi fertőzések között: 1.19%

Előző havi helyezés: 6

Működés: A HTML/Iframe.B 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.



A számítógépre kerülés módja: Fertőzött weboldalakon terjed.

Bővebb információ: [Részletes leírása szerkesztés alatt](#)



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés traceback címe:

http://antivirus.blog.hu/api/trackback/id/3082538

☐ommentek:

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.

Google+ meghívó vagy mégsem?

2011.07.22. 16:10 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [google spam meghívó hamis plus mégsem adathalász](#)

Vagy mégsem rovatunkban arról lesz szó, hogy a korábbi vasfüggönnyel ékesített hiánypiaci korszakunk hön áhított státusszimbólumaihoz (Commodore64, Fa szappan, HiFi torony, nyugati autó, Levis farmer, Frey csoki, stb.) hasonlóan a spam levelek mézesmadzagjai mindig is illeszkednek az aktuális kor igénylistájához.



Manapság állást, [sőt könnyű de jól fizető állást](#), kiemelkedő jackpotot vagy éppenséggel Google Plus meghívót ígérnek. Az ígéretekkel kapcsolatban azonban egy baj van, ha valaki ezeket tényleg elhiszi. Mivel eleinte csak meghívásos, jelentkezéses zárt körben folyt a tesztelés, így [a kártevőterjesztők jó érzékkel ismerték fel](#), hogy a gyors adóvisszatérítés és hasonló sablonok mellé remekül beilleszthető a vágy titokzatos tárgya, a [Google Plus meghívó is](#).



Az első változatok, amikbe Graham Cluley beleütközött, **egyelőre "ártalmatlanok" voltak**, és vírusmentesen Csehov, A három nővér: [Viagra, Cialis és Levitra irányába továbbítottak az önfeledt rákattintás után](#). Nyilván nem marad ez mindig így, ezért **minden ilyen kéretlen levélhez hasonlatosan a feladó személye és a link ellenőrzése előzze meg a Delete gomb lenyomását, de természetesen fordítva is helyes lehet a válasz :-)**



Szóval nem árt vigyázni ilyen bizonytalan időkben, mikor manapság a fekete 7-es busz bármikor simán megelőzheti a piros 7-est, vagy [feltörhetik bárkinek a Facebook fiókját](#), esetleg mi magunk is kézhez kaphatunk egy csodás reggelen egy ilyen fentemlített [Google+ meghívónak látszó tárgyat](#), **de** már egy továbbfejlesztett, adathalászos (Üsd be itten szépen és gyorsan a te Gmail accountodat és utána várj szépen türelmesen, hehe) vagy egyéb kártékony melléklettel, linkhivatkozással. Ezért Google Plus meghívót továbbra is csak őstermelőtől.



4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3088718>

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](#).

privateer 2011.07.23. 00:46:43

Cikk legjobb mondata ez volt: manapság a fekete 7-es busz bármikor simán megelőzheti a piros 7-est.
Ez milyen igaz néhanapján. :)

Kártékony antivirus linkek - villám őrjárat 4.

2011.07.25. 13:45 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [link hamis antivirus](#) [kártékony patrol](#)

Egyfajta röpke "Link Patrol" keretében teszünk időnként kisebb őrjáratot hamis vírusok, a hamis antivírust terítő linkek nyomában, különösebb sallangok, terjedelmesebb tiszteletkörök nélkül. Ezúttal a [Blue Flare Antivirus perdült ki középre](#), hogy táncával szórakoztassa a vendégeket.



Időről időre kipécézzünk 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 darabunk is illeszkedik ebbe a logikai sorba, **ám van benne valami újszerűtű agyafúrt evolúciós extra részlet, amely miatt kiválik az eddigi szürke hamis AV tömegből**, mondhatni kiemelkedik mint gladiátor az eunuchok táborából.



A minden csoda három napig tart jegyében annak lesz érdekes a Szellemvasút is, aki már nem száznegyvedharmadszor utazik vele körbe. Ugyanígy az **unalomig ismert xxx trojan found, yyy virus detected már sokaknak nem okoz csontig ható riadalmat**, így hát a készítőknak megint spirázni kellett egyet a korábbi ügymeneten, fokozandó az izgalmakat.



Erre remekül alkalmas az a fajta félelem, amikor [figyelmetlenségéből rossz címzettnek küldünk ki levelet](#). Ez megtörténhet úgy is, hogy emberi hibából adódóan **kapkodunk, de a véletlen Reply to All is bekavarhat az ügymenetbe**, és persze fertőzött számítógép is tehet hasonlót. Akivel már történt ilyesmi, az tudhatja, milyen változó kort megszegyenítő hőhullámok törhetnek így rá az emberre nagy hirtelen. Nos hát erre lehet építkezni - gondolták a rossz fiúk - és a már megszokott mukinyulas kamuriasztások mellett nosza [ilyen figyelmeztetések is megjelennek legott: Figyelem, "F*ck blondy" tárgyú levél megpróbálta elhagyni a postafiókunkat](#), ám megkönnyebülhetünk, mert a derék becsületes jóra való Blue Flare tábornok ezt lám ügyesen és szolgálatkészen megakadályozta. Ugye mi jóbarátok vagyunk?



Nyilván az angol nyelvterület lesz inkább ennek a módszernek a hálásabb balek közönsége, ettől függetlenül azonban újfent megállapíthatjuk: **aki így akar pénzt keresni, annak fáradhatatlanul meg kell újulnia**, márpedig a kártevőterjesztők erre szemlátomást nem hogy képesek, de láthatóan a tárgykör Főnix madarat megszegyenítő művészei.



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.”**



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)

- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3095438>

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 7DB szeptember 17-18.

2011.07.27. 11:55 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hacktivity 2011 hackerkonferencia](#)

2011. szeptember 17-18-án újra itt a Hacktivity, Kelet-Közép-Európa legnagyobb hackerkonferenciája, ezúttal a Millenárison. Az esemény két napján igazi fesztiválhangulat várható, előadások, workshopok, játékok, a The Global Cyberlympics Közép-Kelet-Európai döntője, hardver hacking, esti buli és 1000+ hacker a világ minden részéről!



Idén nyolcadik alkalommal kerül sor a mára már teljes mértékben [nemzetközi Hacktivity-re, amely a legrégebbi független hazai IT biztonsági rendezvény](#). Az előadók között, ahogy már megszokhattuk, az információbiztonsági szakma legrangosabb képviselőit találjuk. Az előadási jogért évek óta pályázni kell, a Hacktivity-n előadni komoly szakmai rangnak számít. Idén 15 országból több mint 60 pályázat érkezett be a programbizottsághoz, amelyből a legjobb 28-at választotta be a zsűri. A szervezők **idén a nagy érdeklődésre való tekintettel 1000-1200 érdeklődőre számítanak**. A helyszín is megújult, idén a **Millenáris B csarnokába várnak mindenkit profi infrastruktúrával, saját étteremmel, 4590nm-es területen**, ahol két nagy és több kisebb terem alakítanak ki úgy, hogy a legnagyobb teremben egy időben 1000 fő is le tudjon ülni.



A szombati napot a **magyar származású, Amerikában élő Szőr Péter nyitja meg**, akit méltán nevezhetünk a vírusvédelem atyjának. A nemrég magyarul is megjelent könyve „A vírusvédelem művészete” 650 oldalas terjedelmének köszönhetően nem csupán tudományos súllyal bír, de a legátfogóbb mű, amelyet eddig a számítógépes vírusokról írtak. Szőr Péter a **Veszprémi Egyetemen végzett informatikusként és 1990-es években megírta első saját Pasteur névre keresztelt vírusirtóját** – amit akkoriban az OTP is használt, majd 1996-ban Finnországba, a mai F-Secure elődjéhez került, majd 1999-ben a Symantec vezető mérnöke lett, végül a közelmúltban átigazolt a McAfee-hoz.



A vasárnapi nyitóelőadó **Raoul „Nobody” Chiesa Olaszországból, aki Európa legismertebb kiber hadviselési és bűnügyi szakértője**. A nyolcvanas-kilencvenes években egyike volt az első olasz hackereknek, majd 1997-ben megalapította gyártófüggetlen biztonsági tanácsadó cégét, a @Mediaservice.net Srl-t. Raoul 2003 óta működik együtt az ENSZ “UNICRI” Interregionális és Bűn-és Igazságügyi Kutató Intézetével és 2010-ban beválasztották a 30 legjobb európai biztonsági szakértő közé, akik az ENISA (Európai Hálózat- és Információbiztonsági Ügynökség) igazgatóját segítik 2012-ig a PSG Érdekeltek Állandó Csoportjában.



Ám ezzel még közel sincs vége a külföldi előadók sorának. **Vivek Ramachandran** a securitytube.net alapítója Indiából érkezik, **Joseph McCray** Air Force veterán, az EC-Council többszörösen kitüntetett előadója az USA-ból, **Ertunga Arsal**, SAP szakértő és **Alexander Kornbrust** Oracle szakértő Németországból, **Pavol Luptak** a szlovákiai OWASP szervezet vezetője, **Michele Orru** a Royal Bank of Scotland betörési tesztek végző szakembere Olaszországból. Természetesen a rangos külföldi megszólalók mellett sok neves magyar előadónk is lesz. Közülük is kiemelnénk a Deloitte Zrt. biztonsági tanácsadóját, a Hackers Halted legjobb előadóját, **Barta Csabát** aki Computer Forensics témában fog előadást tartani, a szintén deloitte-os, nemzetközileg elismert adatbázis-biztonsági szakértőt, **Tóth Lászlót**, a kancellar.hu-tól **Klock Lászlót** a tavalyi Hacktivity Wargame győztesét, aki virtualizáció biztonsága témakörében végzett kutatásairól számol be valamint **Bodor Pétert** az ELTE docensét, aki a napjainkban egyre népszerűbb az emberek megtévesztésén alapú támadás és pszichológia kapcsolatáról ad majd elő.

Az előadásokon túl számos egyéb program is várja a résztvevőket. Interaktív hello workshopok, hardver hacking [lockpicking azaz a roncsolásmentes zárnyitás](#) és arduino tesztelés témában, játékok: Wargame, CTF, hacker tanösvény, életre keltett ősrégi számítógépek, szombat esti fergeteges buli és **idén először a Hacktivity 2011-en lesz a The Global Cyberlympics Közép-Kelet-Európai döntője! Az idén induló, az EC-Council által szervezett** világméretű biztonsági versenyen 6 fős csapatok mérkőzhetnek meg a világ 7 régiójából, a győztesek pedig az Egyesült Államokban megrendezésre kerülő döntőbe kapnak meghívást.



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3103623>

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 nap és mindenhowyan egyre jobban és jobban

2011.07.28. 15:10 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [flash plugin youtube facebook hamis antivirus retrovirus](#)

Úgy tűnik, egyre komolyabb szinten tör borsot az orrunk alá [a hamis antivirus ipar](#). A módszerek folyamatosan változnak, finomodnak, és egyáltalán nem lehet elintézni egy - áh, ez csak a buták ötven dolláros lehúzása típusú sommás ítélettel.



Ha mogyoróhéjban összefoglaljuk a hamis AV történetét, akkor a történelmi időkben még egy kósza magyar szálát is láthatunk, mert [az úgynevezett Furkó Antivírusról is érdemes megemlékezni](#) mint a **pénzért semmit módszer** egyik első darabjáról, de természetesen a mainstream az angol nyelvterületen úgy 2007 tájékán kezdett megerősödni a SpySheriff, az [Antivirus XP 2008 és társai képében és hasonlatosságában](#). Ezek aztán folyamatos új neveken, apró változtatásokkal, ügyeskedésekkel - [hamis RIAA fenyegetés](#), kamu vírus riasztás helyett/mellett [kamu levélküldési riasztás](#), riasztás a [böngésző hibaablakban](#), etc. - [próbálták a maguk betevő 50-100 USD-jüket sikerrel begyűjteni](#).



Volt aztán olyan szál, ami [a kreatív névadással kapcsolatban](#) felhasznált már létező, IT biztonságban jól csengő ismert neveket, és volt olyan is, ami ezen túlmenve már [valódi vírus cégek hírnevének rombolásával](#), webhelyük, termékük [hamisításával igyekezett pontokat szerezni](#) magának. Úgy tűnik, most még újabb fejezethez érkezünk, az új módszer miatt a Facebook és YouTube felhasználók tömegének érdemes figyelmesebbnek lenni.



A video formájában terjedő megtévesztés sok áldozatot tud szedni, mert látszólag baráttól érkezik. A hamis YouTube videó esetében a mi saját nevünk is megjelenik, így fokozva a megtévesztést, a "hitelességet". Kattintás után video helyett - hű micsoda meglepetés - Flash plugint szeretne frissíteni: "You need upgrade your Adobe Flash Player!".



A zöld disznós és [hamis kodekes meséken](#) szocializálódott felhasználók tömegei itt kaján vigyorral már azt mondhatják: na persze, nice try, fotomemóriájú olvasóinknak pedig a [majd három éves hamis Flash plugines történetünk](#) is bevillanhat - a többiek viszont kattintanak.



A "Flash Plugin" frissítés leánykori nevén [a települt Trojan.FakeAV kártevő igyekszik hatástalanítani az esetleges valódi vírusirtót, sőt a tűzfal üzenetek feletti irányítást is](#) átveszi. Ezt úgy éri el - és itt jön az érdekesség - hogy **megkeresi pontosan milyen antivírust használunk a gépen, majd ennek a programnak az üzenet ablakát imitálva a megfelelő nyelven hamisítva csökkentett módú újraindítást kér állítólagos kártevők mentesítésére hivatkozva**. Az újraindítás után azonban a csökkentett módban Registry átírással kikapcsolja a valódi vírusvédelmet és átveszi a fertőzött gépen az uralmat. Valljuk be, ez azért nem ügyetlen dolog. A BitDefender szakértői szerint [már legalább 16 különböző vírus hatástalanítására van felkészítve az említett trójai](#)



Milyen tanácsokat lehetne összegyűjteni a hatékony védekezéshez? Telepíteni, [kattintani továbbra is csak óvatosan](#), legyen naprakész a Windows és a böngészőkliens is, továbbá Flash plugint csak östermelőtől, illetve izé csak és kizárólag az Adobe oldaláról.



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- ["Szösölmédia" és nyaralás](#)
- [25-ször több a mobilos kártevő](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

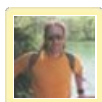
<http://antivirus.blog.hu/api/trackback/id/3106581>

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](#).

[felszopó 2011.07.29. 12:03:00](#)

vírusirtót csak az aldíból



[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
[2011.08.03. 14:38:02](#)

Rádtromfolok:-) merevlemezt csak az Aldiból :-)

www.zdnet.co.uk/news/security-threats/2011/08/01/aldi-confirms-malware-in-hard-drives-40093575/



[gothmog](#) [2011.08.07. 00:20:22](#)

[@Csizmazia István \[Rambo\]](#): 2011 Augusztus 1. És a conficker még mindig tart!

Fej vagy gyomor?

2011.08.01. 15:10 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [facebook](#) [csalás](#) [killer](#) [amy](#) [geoip](#) [whitehouse](#)

Teszi fel az ellenállhatatlan eldöntendő kérdést Bruce Willis az Utolsó cserkész című filmben. Valahova valamilyen számítógépes csapás mindig érkezik, és ez a valahova újabban már jellemzően **nem az email postafiók, hanem sokkal inkább átverős Facebook üzenet**. Aztán azon belül már színes a paletta, **most éppen Amy Whitehouse utolsó drogos videója a soros** vagy egyenesen maga a Facebookos Gyilkos személyesen.



"Ha mellűtök is meghalsz" jegyében ha csak a felhasználók 5 százaléka dől be az ilyennek, akkor is ez **a mai 750 milliós számnál már 37 millió ember**. A csalás pedig roppant könnyen kivitelezhető: kell hozzá egy ötletember, egy Osztap Bender, aki aztán a Google trendsből, meg a napi bulvár hírek feneketlen bugyraiból összemazsolázza a napi betevő csali híreket, és már jöhetnek is a balekok kattintásai.



Az egyik esetben [Amy Whitehouse állítólagos véletlenül kiszivárgott, csak most, csak nekünk utolsó drogos videóját](#) ajánlgatják az érdeklődőknek. **A hozzábiggyesztett "Warning: 18+" valódi feladata pedig** egyáltalán nem holmi szűrés, hanem sokkal inkább az érdeklődés további csigázása a várható nézőszám felszólolása okán.



A kéréstlen tartalom lájkolása ismerőseink üzenőfalának bepiszkításán túlmenően **mindenféle online felmérésekhez, vagy emeldíjas szolgáltatásokhoz vezet el, melyek után a csalók jutalékot kapnak**.



Akik valamilyen rejtélyes ok folytán esetleg távoltartják magukat a rothadó kapitalizmus ilyen jellegű ópiumától, azoknak sem kell betevő kattintás nélkül maguk elé meredniük üveges tekintettel, **mert van itt nekik Facebook Killer is**, amely egy az Egyesült Államokban tanyázó **sorozatgyilkosról számol be megint csak most, csak nekünk egy YouTube videó formájában**. Ahol ugye előbb kattintanunk kell, elmúltunk-e már 13 évesek.



Minő meglepetés, a gomb pedig erre **a "szokásos módon" mindenféle video nézegetés előtt/nélkül már suttymban szépen meg is osztja azt a barátaink felé**. Ez ráadásul duplán vicces, hiszen eredetileg maga a Facebook regisztráció is ezen 13 éves korhatáron alapul - persze szigorúan elvileg ugyebár, másfelől megnézve azt a kódot, ami **az életkor ellenőrzés mögött található, további érdekesség vár minket**:



Magyarán **a GEO-IP adatok alapján továbbbemelik a kíváncsiság tétjét**, hiszen ki az a szőrös szívű fráter, aki még egy nyavalyás kattintást is sajnál akkor, mikor világosan látszik, hogy az emlegetett sorozatgyilkos pontosan az ő településén található.



A bulvár hírek esetleges rideg elutasítói pedig **iPhone 4, MacBook Air vagy iPad 2** nyereményekről álmodozhatnak két megosztó kattintás között: "You have been selected as today's winner!, juhééé".



Jó kérdés, mi lesz majd akkor, [ha tényleg egymilliárd Facebook felhasználó](#) lesz a Földön. **Egy fix pont azonban már látszik: egymilliárdnak nagyobb az 5 százaléka, mint a hétszázötven-milliónak :-)**



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Ez történik a weben egy perc alatt](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3116895>

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.

Jobban fertőzödünk, mint 4 éve

2011.08.03. 14:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [napi emelkedés](#) [vírusminta](#) [150000](#)

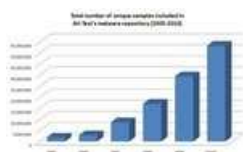
A félkomoly cím inkább csak arra utal, néha érdemes szusszanni egyet és megnézni az aktuális számokat. Még a svájci frank elképesztő szárnyalását is lepipálja az a napi megjelenő új kártevőminta mennyiség, amit a víruslaboroknak fel kell dolgozniuk.



A Sophos legutóbbi kimutatásai szerint [naponta átlag 150 ezer új kártevő minta érkezik](#), ez pedig a 2010-es esztendőhöz viszonyítva mintegy 60 százalékos növekedésnek felel meg. Ha játszani akarnánk a statisztikai számokkal, akkor úgy is lehetne fogalmazni, hogy minden fél másodpercben keletkezik egy új egyedi kártevő.



Azt is tudjuk, sejtjük, hogy [évek óta emelkedik a fertőző weboldalak száma](#), meg realisan nézve nem is várhatjuk hogy csökkenjen, de megintcsak az aktuális számokat nézegetve feltörhet a sétarepüléses dugóhúzó közbeni klasszikus mondat: [na erre azért nem gondoltam](#). Szóval a számok ezt mutatják: 19 000 kártékony URL naponta, és ezek 80 százaléka olyan korábban ártalmatlan oldal, amely valamilyen feltörés miatt fertőződik meg.



Érdemes időnként év közben is [felidézni az antivírus cégek](#) tavaly évvégi [2011-re szóló jóslatait](#). A Stuxnet szerű [támadások folytatódását éppúgy beigazolódni](#) látjuk, akárcsak a [korábbi Windows változatok](#) fertőzöttségét, vagy [Facebook és okostelefon platformok](#) iránti egyre intenzívebb támadásokat.



Esetleg az év vége felé egy laza posztban, [mikor majd az új üveggömbös jóslatok jönnek](#), kiértékelünk néhány korábbi trendet és kijelentést, vajon 640 kB elég lett-e mindenkinek;-) Egyelőre azonban úgy tűnik, megyünk a kijelölt úton, tehetjük sorra a pipákat a várható trendek mellé és a megbízható vírusirtó továbbra is nélkülözhetetlen kellékünk marad.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

• [1 trackback](#)

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szósölmédia" és nyaralás](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3122693>

Trackbackek, pingbackek:

[Trackback: Kapd be a hoaxomat!](#) 2011.08.04. 09:13:56

Most a Mars közelebb kerül a Földhöz, mint valaha bármikor és legközelebb 2287-ben lesz ilyen. Bonsai macskákat tenyésztettek ki New Yorkban, a kismacskák izomlazítót kaptak és üvegbe gyömöszölték őket, hogy hátralévő életüket ott töltsék. Bill Gates 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](#).

Nincsenek hozzászólások.

Enhanced Átverési Mode

2011.08.08. 15:30 | [Csizmazia István \[Rambo\]](#) | [2 komment](#)

Címkék: [hamis kaspersky mode nod32 eset antivirus protection enhanced](#)

Haditudósítóink jelentik: jelentős légvédelmi és aknatűz alatt a legális vírusvédelmi programok, a korábbi himi-humi Antivirus XP 2010 és hasonló kamuszagú nevek helyett újabban csupa valódi program nevét hamisítják egy "ENHANCED PROTECTION MODE" nevű felbukkanó ablakban.



A dolog kezdődhet ártatlanul, éppen keresünk valamit a Google-ben, mire szemünkbe ötlük egy ["Oh, kapjunk hát ingyen iPodot most" feliratú hirdetés](#), de Facebookon is be lehet szerezni mindezt, elég hozzá például Gertruda Infikovanaval kedélyesen cseverészni, majd az ajánlgatott videolinknek látszó tárgyra kattintani.



[Robert Lipovsky barátunk a mellékelt screenshot alapján megtalálta a hangot vele a diskurzusban](#) már a "Hi malware" köszönés se semmi, de mindezt tudja még fokozni is: "It's you on the video, want to see it? Yes, yes, yes, gimme a malware sample", és odaadja, és LOL. Aki átlagfelhasználóként még 2011-ben is így akar egy video reményében kodeket vagy Adobe Flasht letölteni, frissíteni, arra a legjobb indulattal sem mondhatjuk, hogy óvatos lenne.



Ha már sikerül letölteni és futtatni a kártevőt, akkor jönnek az érdekes részek, keményen **hamisítják, lejáratják az olyan valódi neveket, mint a Kaspersky vagy a NOD32**. A mellékelt képeken a valódi és a hamis képernyőképek következnek, amiből jól látszik, a hamis riasztási popup ablakokhoz ezúttal sem kell eredetiségvizsgáló törvényszéki szakértő csapatot hívni, hisz ezek most is nagyjából egykaptafára készülnek nagyipari eljárással, optimalizált ráfordítással profit orientáltan. **Ennek ellenére így is biztosan lesz majd elég gyanútlan rákattintó.**



A felhasználók oldaláról nézve a megoldás talán abban rejlik, hogy a közhelyes sztereotípiák: szereltesünk lakásunkba valamilyen riasztót, telepítsünk valamilyen vírusirtót, etc. helyett arra is **fordítsunk gondot, hogy mit, kivel, milyen - ezeket a feladatokat ne csak szimplán "letudjuk", kipipáljuk, hanem egy megbízható cég megbízható megoldását válasszuk**. Érdemes-e riasztót szereltetni a lakásunkba olyannal, akiről semmit nem tudunk, a hirdetésében név, cím nem is szerepel, csak egy villanyoszlopra ragasztott mobiltelefonszám? Vagy inkább végezze el ezt a feladatot egy olyan szakember, akinek már utánanéztünk, van neve, címe, telephelye, garanciát vállal, és ismerjük egy-két referenciáját, esetleg ismerőseinknél kitűnő munkát végzett?



A vírusvédelemben is hasonlóan alaposan tájékozódjunk. Minden online fizetéskor ellenőrizzük a digitális aláírást, de **soha ne fizessünk kéretlenül települő vírusirtóért, ami éppen "fertőzést" talál a gépünkön**. Emellett kezeljük a helyén, ha egy cikket olvasunk, például egyetlen újságpéldány vagy online cikk teszteredményéből még nem szabad messzemenő következtetéseket levonni, csak az

AMTSO elvek alapján elvégzett teszt számíthat egyáltalán mérvadónak, és **ott is az lényeges szempont, mely programok teljesítenek jól hosszútávon, évek óta stabilan**, ezekre érdemes rábízni gépünket, adatainkat.



Vajon milyen súlyos fertőzés lehet az, amit a nevesincs AntiSpySafeguard, Major Defense Kit, Peak Protection, Pest Detector és Red Cross előzőkenyen felismer, míg az F-Secure, Kaspersky, McAfee, NOD32 és a Symantec szoftverei nem detektálnak?

És ha már használunk egy adott megfelelő terméket, ismerjük meg azt alaposan és gyanakodjunk holmi furcsa, ugyan céglogós, de idegen kinézetű ablak láttán. Persze [a hamis AV elleni harc](#)hoz jól jöhetne még emellett, [ha a bankok is hatékonyabban fellépnének ellenük](#), de ennek az "érdek a világ ura" jegyében kb. annyi az esélye, mint hogy soha ne módosítsanak egyoldalúan szerződést vagy [a svájci frank hitelesek esetében önként lemondjanak a nyereségük egy részéről](#) (nyerghh), magyarul vélhetően erősen konvergál ez a nullához. Most hogy az "ENHANCED PROTECTION MODE" jelenséget ilyen jól kibeszéltük, várhatjuk, [milyen újabb felugró ablak átverési trükkkel próbálkoznak](#) majd a csalók - legközelebb.

 Tetszik  Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Majdnem mindenki átverhető adathalászzal](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/3133481>

Kommentek:

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



[atko 2011.08.08. 20:48:41](#)

Nem csalók azok hanem üzletemberek, akik a gyártók és fejlesztők által létrehozott piactéren próbálnak megélni. Vajon miért van az, hogy nálunk és gondolom még számos országban nincs hamis apple store, de valahol van (www.sg.hu/cikkek/83473/hamis_apple_bolt_kinaban)?

A számítógép legalább annyira sarlatánság, mint az atomenergia. És ezt csak félig mondtam viccesen. :-)



**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
2011.08.08. 21:25:02**

Guten abend!

A zavarosban halászás, a megoldom okosba, a trükközés mára már sajnos annyira általános, hogy aki túl becsületes, annak lassan a lúzer címkét himzik bele az ingébe.

Egy ismerősöm, amúgy jó fej, úgy alakított azonos profilú céget anno, hogy pontosan a konkurencia neve lett, de akkor még lehetett ugyanaz a név bt és kft. A cél: hátha véletlenül áttéved megrendelés, ügyfél.

De ilyen bocsánatos dolgok mellett ma már durvábbak is vannak, cimbora mai FB üzenete azt hiszem magáért beszél:

'Ismerős meséli: "XY egy adott cég domainjeit szerette volna bejegyezni, és egy adott cég domaines keresőjében ellenőrizte, hogy a domainek léteznek-e. Nem léteztek. Másnapig, amikor egy másik bizonyos cég bejegyezte őket." Tanulság: ha domain nevet ellenőrzöl, használd a domain.hu keresőjét, vagy külföldi domainek esetén pl. az Internic www.internic.net/whois.html keresőjét, hogy a domain még holnap se létezzen - valaki másnál.'

A kínai Apple Stoert is olvastam, azért nem kevés pénz lehet valakinek abban sem,

Vegyük meg legalább a szelvényt

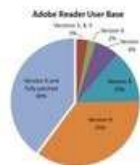
2011.08.10. 14:00 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [reader](#) [adobe](#) [rég](#) [verzió](#) [sebezhető](#) [vállalatok](#) [exploit](#) [elavult](#)

Vannak bizonyos szükséges hozzávalók a biztonságban a céges környezetben (is), ahol olyan elemek szerepelnek, mint adatvagyon felmérése, biztonsági szabályzat, mentés szabályozott rendje, hozzáférés védelem, vírusvédelmi programok szabályozott és távmenedzselt használata meg hasonló. **Ám minden lánc olyan erős, mint a leggyengébb láncszeme.**



A klasszikus vicc szerint a lottósorsolás délelőttjén a szegény skót imádkozva jár föl-alá a szobájában, és hangosan imádkozik: "Jaj Istenem, csak most segíts meg, hogy enyém legyen a főnyeremény! Csak most az egyszer segíts, hogy én nyerjek!" Egy idő után elunja a Teremtő az imádkozást és így szól a skóthoz: "Szívesen segítek, jóember! De legalább vedd el egy szelvényt!" Kicsit ehhez hasonló, amikor a Zscaler legutóbbi State of Web felmérés eredményeit nézzük, különös tekintettel az Adobe Readerre. A tanulmányból az derül ki, hogy [a vállalati felhasználók körében a számítógépek több, mint 56%-a régi, elavult, sebezhető PDF olvasót futtat.](#)



Hogy ez a szám nem túlzás, hanem nagyjából megfelelhet a valóságnak, azt az is igazolhatja, hogy ugyanerre [az Avast cég felmérése is közel ilyen, 60%-os használatot](#) mutatott. Ráadásul a címadó Adobe frissítések ingyen érhetők el, így kevésbé fogadható el az a magyarázat, ha a válságra meg a monetáris restrikczióra kenik az el nem végzett feladatot.



Nyilván nem a mult cégek, hanem inkább a közsféra, na meg a kis- és közép vállalatok használnak még emellett [biztonsági szempontból erősen támadható Windows XP operációs rendszert](#) (másfél évvel ezelőtt egy budapesti kórházban még a saját szememmel láttam ügyfélfeladatokat rögzítő Windows 98-at Epson FX-1000-es mátrixnyomtatóval).



A biztonságért vívott küzdelemben megtett erőfeszítések csak akkor érnek valamit, ha annak minden frontján egyidejűleg tesszük meg a szükséges erőfeszítéseket, magyarul hiába használ valaki vírusirtót az ajtóban, ha közben nem teszi mellé az operációs rendszer, az alkalmazói programok és a benne a böngésző pluginok ugyancsak kulcsfontosságú biztonsági frissítéseit az ablakban. (Már ezt a linket is csak frissített olvasóval ér megnézni :-). Ezt többek közt a Windows automatikus frissítések bekapcsolásával, alkalmazói programok esetén például az [ingyenes Secunia PSI-vel](#), és mondjuk Firefox esetén [a Plugincheck weboldallal](#) tehetjük meg könnyedén.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrző 8.](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3139484>

☐ **ommentek:**

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](#).



TrueY • <http://qltura.blog.hu> **2011.08.11. 11:03:52**

Szerintem a Win98 már újra biztonságos, mert olyan kevés van már belőlük, hogy már nem írnak olyan vírust, ami fut rajta. :) Nekem otthon 2 gépemen is van Win98. Sőt nemérg egy WfW3.11-et installátam. :)

Unicode, én így szeretlek

2011.08.12. 11:20 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [trójai cirill unicode hosts](#)

Ha Rodolfósan azt mondják, csak a kezemet figyeljék, akkor **könnyen lehet, hogy becsap a szemünk: két hosts fájl nem fér meg egy csárdában**. De csodák nincsenek, az ilyen látszólag tökéletes kártevő trükknek is van logikus magyarázata - mikromágiaügyi miniszterünk le is leplezi azt némi vizsgálódás és elemzés után.



Hihetünk-e a szemünknek? - nem véletlenül ez a címe annak az írásnak, ahol **egy trójairól van szó, ám az orosz közösségi oldalakra való kéretlen átirányításnak a kártevő kódjában látszólag nyoma sincs, nem lelni a kódban az orosz domaineket**. Van helyette azonban valami más, és ez fog majd elvezetni minket a helyes megoldás irányába.



Nicsak, a C:\WINDOWS\System32\drivers\etc folderünkben két hosts fájl is szerepel. Hoppá, hogy is van ez? Mivel bármilyen könyvtári bejegyzés is fájlbejegyzésnek számít, még a fájljal azonos nevű könyvtár sem lehetne, nem hogy két azonos nevű állomány.



De vajon valóban azonos a név vagy csak kinézetre azonos? A magyarázat előtt nézzük meg egyik korábbi posztunkat, attól fog megjönni az "Aha élmény". [A Raural furmány egy ékes példája](#) a bűnözői kreativitásnak, és persze arra is, hogy a látja, nem látja, na látja remekül működik, **magyarán sosem a szemünknek kell hinni, hanem inkább a kódoknak**.



Igaza volt Obi-Wan Kenobinak, harcolni valóban sokféleképpen lehet, ebben a kódkiostással való játék is egy extra lehetőség, amivel megtéveszthetők vagyunk.



Szóval tűzre, vízre, Unicode-ra vigyázni kell, és ebben remélhetőleg az ehhez hasonló tanulságos esetek is segíthetnek valamennyire.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [25-ször több a mobilos kártevő](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés [trackback](#) címe:

<http://antivirus.blog.hu/api/trackback/id/3147638>

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](#).

[Uzi 2011.08.12. 14:09:41](#)

Mi értelme volt mindkét fájlt ott hagyni? Az "optikailag" hosts file nem zavar vizet. Esetleg az igazit elrejtették?

A Twitter bejelentkező oldala. Vagy mégsem?

2011.08.15. 17:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [jelszó](#) [twitter](#) [phishing](#) [elgépelés](#) [adathalász](#) [typosquatting](#)

Osama Bin Laden él, vírúl, sőt horgászik. Aki nem hiszi, az vethet egy pillantást azokra a **kéretlen Twitter üzenetekre, amikre kattintva nem érdemes begépelni** Twitteres accountunkat.



Pedig látszólag milyen érdekes, hogy vadidegen ismeretlenek milyen gálánsan - és kéretlenül - átadják nekünk ezeket a páratlan infókat, ez az amire vágytunk.



A linkekre kattintva azonban érdekesebb a helyzet, nem kártevő jön, **hanem a Twitter bejelentkező oldala. Vagy mégsem?** Pedig a kinézet már szép munka, [nem magyar bankos fércmunka](#), simán megjelenhetne a Füles Vedd észre a két kép között az 5 különbséget című rovatban.



Tetézi a "szép" kivitelezést, hogy az adathalász webhely [az úgynevezett Typosquatting terén is mutat fel érdemi eredményeket](#), hiszen az oldal URL címe ugyanis mindössze néhány betű eltéréssel igyekszik hasonlítani az eredetire. Mit is takar ez a szépcsengésű fogalom?



Typosquatter az az úriember, aki kihasználva a nagyforgalmú, nagylátogatottságú webhelyeket, tudatosan ezek URL neveihez egy-két betű eltéréssel hasonló domaineket foglal, és ezzel visszaélve adathalászik, kártevőt terjeszt, vagy éppen csak hirdetéseket tesz ki, ami az elgépelés miatt elképesztő mennyiségű látogatást produkál. Az egyik leghíresebb ilyen oldal például a Goggle.com.



Újabban már az is divatba jött, hogy [az unicode karakterekkel jelölt URL neveknél kinézetre elgépelésmentes, teljesen azonosnak látszó weboldalakat is hamisítsanak](#). Bár jelen esetben a "twitter" "itwittler" formájú elgépeléséhez előzőleg már elég sok kórsó sört [kell inni](#), azért a sötét szándék lólába így is vastagon kilóg.



Most, hogy [az idő vasfoga így elrepült](#) fölöttünk, **[tanácsaink a szokásosak](#)**: sok sör elfogyasztása után még véletlenül se gépeljük félre a **Twitter** urlt;-), ha pedig esetleg mégis belefutnánk egy hasonló oldalba, vegyük észre ha azt mondjuk Kínában hosztolják. Ha léprementünk, akkor pedig **mihamarabb váltsunk erős Twitter jelszót**.



Ha pedig netalántán azok táborába tartozunk, **[akik mindenhol egyforma és ráadásul gyenge jelszót használnak](#)**, akkor pedig mindenhol...

 Tetszik  2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0

Ajánlott bejegyzések:

- [Android-kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Hogyan szűrjük 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/3155758>

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.

Júliusi galopperedmények: Autorun a befutó

2011.08.17. 14:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [magyar adatok](#) [nod32](#) [eset](#) [havi](#) [threatsense](#) [vírusstatisztika](#)

Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik a hazai felhasználók számítógépeit. Úgy tűnik, marad az Autorun korszak, és a Conficker sem mozdul a második helyről.



Nincs jelentős változás a júliusi víruslistában, maga a kéttagú élmezőny pedig immár negyedik hónapja őrzi pozícióját. Az első helyen szereplő **INF/Autorun vírus régi motorosnak számít, amely terjedéséhez a Windows automatikus futtatás lehetőségét használja ki.** A bűnözők előszeretettel építenek arra, hogy a legtöbb felhasználó nem tiltja le az automatikus futtatást a Windows operációs rendszerek alatt. **Második a Conficker féreg, amely az operációs rendszer frissítéseinek hiányát, a gyenge jelszavakat és az automatikus futtatás lehetőségét** kihasználva terjed, és bár a sebezhetőséget bezáró frissítés már régóta megjelent, több, mint egy esztendőn keresztül mégis vezette a toplistát.



A harmadik helyezett Win32/HackMS alkalmazás **eredetileg egy Microsoft programokhoz készített kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz.** Hetedik helyre lépett a korábbi kilencedikről a Win32/ShutDowner trójai is, amely fertőzés esetén módosítja a Registryben az automatikus lefutás egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. **Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal.** Legfőbb és legszembetűnőbb hatása azonban, hogy **büntetőrutinja lekapcsolja az éppen futó Windows rendszert,** és ezzel zavarja meg a munkát, de akár adatvesztést is okozhat.



A biztonságért vívott küzdelemben megtett erőfeszítések **csak akkor érnek valamit, ha annak minden frontján egyidejűleg tesszük meg a szükséges erőfeszítéseket,** magyarul a naprakész vírusirtó mellett mind az operációs rendszer biztonsági frissítéseit, mind pedig felhasználói programok javítófoltjait, új verziók telepítését el kell végezni, hogy a sebezhetőségeket bezárjuk. Ebben minden apróságra figyelni kell, legyen friss az Adobe PDF olvasója ugyanúgy, akár a böngésző Flash pluginje és a további egyéb, böngésző kiegészítők. **Míg a Windows rendszer biztonsági frissítéseire a NOD32 és ESET Smart Security is képes figyelmeztetni, a többi segédprogram naprakészen tartását olyan segédprogramokkal oldhatjuk meg, mint például az ingyenes Secunia Personal Software Inspector, vagy a Firefox böngésző esetében az ugyancsak ingyenes Plugincheck.**



Az ESET **több százezer magyarországi felhasználó visszajelzése**in alapuló statisztikai rendszere szerint **2011. júliusában** a következő 10 károkozó terjedt a legnagyobb számban, és volt együttesen felelős az összes fertőzés 20.34 %-áért.



1. INF/Autorun vírus

Elterjedtsége a júliusi fertőzések között: 5.24%

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.



A számítógépre kerülés módja: Fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun>



2. Win32/Conficker féreg

Elterjedtsége a júliusi fertőzések között: 4.02%

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 eljárashívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárason 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.



A számítógépre kerülés módja: 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. Win32/HackMS trójai

Elterjedtsége a júliusi fertőzések között: 2.41%

Előző havi helyezés: 5.

Működés: A Win32/HackMS alkalmazás eredetileg egy kalóz kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítéskor rejtett állományokat és olyan bejegyzéseket is létrehoz a rendszerleíró-adatbázisban, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A számítógépre kerülés módja: A felhasználó maga telepíti.
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/hackkms-a>



4. Win32/PSW.OnLineGames trójai

Elterjedtsége a júliusi fertőzések között: 1.50%

Előző havi helyezés: 6.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozóknak rootkit komponensei is vannak, melyek segítségével igyekeznek állományaikat és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatok titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: A felhasználó maga telepíti.
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



5. HTML/Iframe vírus

Elterjedtsége a júliusi fertőzések között: 1.47%

Előző havi helyezés: 10

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.



A számítógépre kerülés módja: Fertőzött weboldalakon terjed.

Bővebb információ: Részletes leírása szerkesztés alatt



6. HTML/ScrInject trójai

Elterjedtsége a júliusi fertőzések között: 1.44%

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.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



7. Win32/Shutdowner trójai

Elterjedtsége a júliusi fertőzések között: 1.36%

Előző havi helyezés: 9.

Működés: A Win32/Shutdowner trójai fertőzés esetén módosítja a rendszerleíró-adatbázisban az automatikus lefutas egy kulcsát, hogy a kártevő minden rendszerindításkor lefuthasson. Rootkit komponenssel is rendelkezik, így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Legfőbb és legszembetűnőbb hatása, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja a munkát, de akár adatvesztést is okozhat.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/shutdowner-aa>



8. Win32/VB féreg

Elterjedtsége a júliusi fertőzések között: 1.35%

Előző havi helyezés: 8.

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon terjed. Fertőzés esetén megkísérel további káros kódokat letölteni az 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.



A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



9. Win32/Tifaut trójai

Elterjedtsége a júliusi fertőzések között: 0.86%

Előző havi helyezés: -

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csrsc.exe és autorun.inf néven. A kártékony EXE fájl automatikus lefuttatásához külön bejegyzést is készít a rendszerleíró-adatbázisban. Működése során több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21tifaut>



10. JS/TrojanClicker.Agent trójai

Elterjedtsége a júliusi fertőzések között: 0.69%

Előző havi helyezés: 4.

Működés: A JS/TrojanClicker.Agent trójai egy olyan kártékony JavaScript kód, amely lefutva kártékony kódokat helyez el a Windows kulcsfontosságú (Windows, Windows/System32) mappákba, és az ott található fertőző komponensek automatikus lefutását biztosító Registry bejegyzéseket készít, amely a számítógép minden újraindítása után lefut. Ezen felül hátsóajtót nyit a rendszerben, és további kártékony kódokat próbál meg letölteni különféle távoli weboldalokról.



A számítógépre kerülés módja: A felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok!/trojanclicker-agent>

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászáttal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/3159739

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.

Ezer nap az élmezőnyben

2011.08.19. 10:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [frissítés](#) [féreg](#) [autorun](#) [conficker](#)

Aki szokott olvasgatni havi vírusstatisztikákat (állítólag valóban léteznek ilyen hús-vér emberek), annak biztosan feltűnt már, hogy **volt egy olyan szereplő, amely szokatlanul hosszú ideig szerepelt, sőt szerepel a toplisták élbolyában.**



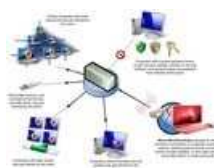
Ez pedig nem más, mint [a Conficker féreg, amely éppen ezer napja keseríti meg a felhasználók életét.](#) **Nem hétköznapi ez a 2008. november 21-én megjelent kártevő, sokszor és sokat beszéltünk már róla,** a magyar víruslistát is alapvetően tizennyolc hónapon át vezette. Sokféle kérdés felmerül az emberben, az egyik talán az, hogy egy olyan régeinek számító kártevő, amelyre [már 2008 október óta van a keresztségben MS08-06 Critical nevet kapott security patch](#), hogy az ördögben tud mégis ennyire terjedni, ennyi gépet fertőzni, ennyi kárt okozni. A válasz nem egyszerű, sőt egyértelmű autentikus nem is létezik, de több körülmény is fontos lehet ennek kapcsán.



Az észlelések azt mutatják, hogy a kártevők még mindig széles körben próbálkoznak ezzel a módszerrel, hiszen a korábbi Windows verziók, vagy a hivatalos támogatásból már kikerült OS változatok, valamint **a nem legális Windo** ☐ **példányok esetén a biztonsági frissítések egyáltalán nem történnek meg.** Aztán belejátszhat még, hogy nagyobb **céges környezetben, ahol nem fordítanak elég gondot, pénzt, időt, erőforrást a frissítésekre, biztonságra,** a felhasználók összevissza telepíthetnek, mindent rendszergazdai jogosultsággal használnak, emiatt gyakorlatilag kiirthatatlan, hol itt bukkan fel újra a fertőzés, hol ott.



Ugyancsak lényeges szempont, hogy a Conficker féreg [egyik fertőzési módszere éppen az az Autorun,](#) amelyik a **Conficker korszak után most nyitott szezon magának.** A hordozható meghajtókon egyre rafináltabban és kifinomultabb módszerekkel terjedő Autorunos kártevők igen sok kárt képesek okozni, így ezeken is kiemelt veszélyforrást jelenthetnek, így a naprakész antivírus mellett a naprakész Windows javító foltok megléte is kiemelt jelentőségű, valamint a külső adathordozók automatikus indulását is érdemes letiltani saját biztonságunk érdekében. ☐ **gy tűnik, a felhasználók vagy nem törődtek ezzel a veszélyforrással, vagy pedig nem szívesen mondtak le a kényelmi funkcióról.**



Ha az ezer napos hossz okait kutatjuk ebből a szempontból, és végignézzük a Microsoft az automatikus futtatással terjedő fertőzések ellen tett erőfeszítéseit, azt láthatjuk, sajnos évekig kivárt a hatékony közbeavatkozással. **Először aztán a Windows** ☐ **esetén ki kapcsolta ki végre alapértelmezetten az Autorun**, a régebbi operációs rendszerek esetén pedig előbb egy választható javítófoltként elkészített kikapcsolás készült, majd végül a rendszeres biztonsági frissítések közé is beemelték ezt. **Hogy mindezt majd az utókor "jobb később mint soha" érzésekkel fog-e gondolni, majd elvállik.**



Arra, hogy a botnetek mekkora problémát jelentenek, és fertőzések milyen mértékben terjednek, arra álljon itt egy 2009-es adat: az F-Secure szerint mindössze [négy nap leforgása alatt 2. milliőról 8.9 millióra emelkedett a Conficker egyik variánsával fertőzött számítógépek száma.](#) **A harcban a lokális védekezés egy dolog, a fertőzés globális okozóira mért csapás pedig egy másik, és szerencsére ez utóbbi fronton is történtek idővel kedvező események, [kitűzött vérdíjak](#),** sőt domainek kitiltása, illetve olyan jelentős botnetek leállítása, mint a Waledac, Coreflood vagy Rustock.



Hogy a Conficker mikor tűnik el a süllyesztőben, nem tudni, **a toplistákról idővel valóban eltűnhet, ám a fertőzési kísérletek közül biztosan nem fog**, erre pedig jó példa, hogy mind a mai napig akad fent próbálkozó Blaster, SQL Slammer és hasonló őskövíletnek számító kártevő a szűrésen.



Végezetül az ezer nap [intelmei mellett](#) gondoljunk egy kicsit az ezer évre is, ez alkalomból pedig **minden kedves István nevű olvasónknak boldog névnapot kívánunk!**



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3164394>

Kommentek:

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

Nincsenek hozzászólások.

Facebook biztonsági útmutató

2011.08.22. 11:11 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [facebook security pdf guide](#)

Örömmel üdvözljük azt a kezdeményezést, amely a Facebook használatával, biztonságos beállításaival és a lehetséges veszélyekkel foglalkozik kimondottan fiatalok, szülők és tanárok számára.



Ha azon gondolkodunk, ki is lenne a legfelelőbb arra, hogy egy ilyen összefoglalót készítsen, arra a megállapításra juthatunk, éppen maga a Facebook látszik a leglogikusabbnak (úgyis ők változtatgatják havonta a felhasználói szerződést, így majd könnyebben és gyorsabban frissíthetik a saját leírásukat ;-).



[Sok fontos részletre kiterjed az összefoglaló](#), beleértve olyan dolgokat, mint például legyen a jelszó erős, mindenhol használjunk egyedit, ha már nem Facebookozunk, lépünk ki a kijelentkezés gombbal, mert a böngésző bezárása nem elég, és hasonló tanácsok szerepelnek a [14 oldalas képes PDF formátumú kiadványban](#). Ismertetnek benne [jellegzetes csalási típusokat, amelyek kéretlenül érdekes videókat, játéklehetőségeket ígérnek](#), kitérnek arra, miért cél az identitás ellopása, mire használhatják azt a bűnözők.



A tanácsok között szerepel hasznos, biztonsággal kapcsolatos böngészőklens kiegészítők használata éppúgy, mint a HTTPS választás előnyeinek ismertetése, illetve az óvatos, biztonság tudatos letöltés, a linkek kattintás előtti ellenőrzése és hasonlók.



Az applikációk, üzenetek helyesírása vagy annak erőteljes hiánya is lehet egyfajta intő jel, és [ez nemcsak a kéretlen álláshirdetésekre](#) igaz.



Mindenesetre a Facebook a maga levelét megírta, hogy aztán könnyeivel is telesírta-e, azt nem tudhatjuk, de mindenképpen hiánypotló a munka, amelynek egyértelműen csak örülni lehet.



Hogy aztán hányan olvassák majd el a célcsoportból, közülük hányan szívlelik meg a benne foglaltakat, és aztán ennek hatására javul-e majd számottevően a 210 országban több, mind 500 millós felhasználói tábor biztonsági helyzete, majd idővel elválnak, ha lesz ilyen, mi szívesen beszámolunk róla.



43 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



1



Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3170467>

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.

Bankolás idegen gépről, levelezés nyitott wifiről

2011.08.24. 11:30 | [Csizmazia István \[Rambol\]](#) | [12 komment](#)

Címkék: [open wifi](#) [jelszó veszély](#) [felmérés](#) [hotspot](#) [bankolás](#)

A magyar felhasználók jelentős része veszélynek teszi ki személyes adatait azzal, hogy nyilvános számítógépekről is bejelentkezik e-mail és Facebook fiókjába, vagy akár internetbankjába.



Az ESET Magyarország felmérése szerint a magyar internet-felhasználók 58 százaléka alkalomadtán barátja vagy munkatársa számítógépét használja e-mailjei ellenőrzésére, 34 százalékuk pedig nyilvános számítógépekről is belép postafiókjába. Emellett a felhasználók 10 százaléka ismerősei számítógépén is bankol, 4 százalékuk pedig különböző - például internetkávézóban elhelyezett - nyilvános számítógépeket használ utalásainak elintézésére.



Barátai számítógépéről a felhasználók 3 százaléka vásárol olykor hitelkártyával, 1 százalékuk pedig nyilvános számítógépről. Különösen a fiatalok óvatlanok, a 18-29 évesek 71 százaléka használta már ismerőse számítógépét arra, hogy azon keresztül ellenőrizze saját levelezését, 46 százaléka pedig arra, hogy belépjen Facebook fiókjába.



A legbiztonságosabb, ha kizárólag saját számítógépünket használjuk levelezésre és banki ügyeink intézésére. A nyilvános számítógépek többségére szinte bárki telepíthet olyan kémprogramot, ami ellophatja jelszavainkat. Ezért ezeken lehetőleg ne adjuk meg jelszavainkat, és **semmiképpen se lépünk be internetbankunkba**. Ha a gépünk nélkül indulunk nyaralni, akkor készítsünk egy olyan ideiglenes e-mail címet, amit csak az utazás során használunk, és ennek segítségével tartsuk a kapcsolatot ismerőseinkkel.



Emellett érdemes **óvatosan eljárni akkor is, ha saját számítógépünket nyilvános vezeték nélküli hálózatokban használjuk**. Ilyenkor is jobb elkerülni a személyes adatainkat is tartalmazó internetes szolgáltatások használatát, és fontos az is, hogy olyan biztonsági programcsomagot használjunk, melynek tűzfala elrejtí számítógépünket a nyilvános hálózatra csatlakozott többi gép tulajdonosa elől.

Tetszik 25 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Majdnem mindenki átverhető adathalászárral](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3175426>

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](#).

Udi • <http://blog.udi.hu> 2011.08.24. 13:47:08

És hányan használnak például két utas autentikációt? Hányan tudnak arról, hogy létezik a (például) google account mellé ingyen?

"tűzfala elrejtí számítógépünket a nyilvános hálózatra csatlakozott többi gép tulajdonosa elől" Ezt nem is értem.

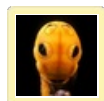
Szóval nem kötekedni akarok, de úgy gondolom, hogy hiba ledermedni azon a ponton, hogy használj vírusirtót, meg peccselt oprendszer, meg ne netezz openwifiről. Egyre több az olcsón (ingyen), kényelmesen elérhető megoldás, ami fényévekkel megnöveli az acc biztonságát.

Zoli (SSDB) 2011.08.24. 14:02:33

Kicsit ez "...a gépünk nélkül indulunk nyaralni, akkor készítsünk egy olyan ideiglenes e-mail címet, amit csak az utazás során használunk, és ennek segítségével tartsuk a kapcsolatot ismerőseinkkel..." HÜLYESÉG. sőt nem kicsit NAGYON, ama klasszikust idézve.

Miért? Mert alapesetbe külföldön, internetcaféból, egyetemi könyvtárból egy fiatal nem géppel megy és a levelezését, az arra érkezett méleket szeretné megtekinteni és arról válaszolni. (ugyanígy a fészbuk üzikkel is) Egy tök üres emailcím csak kevert okozna. Eccerübb lenne ha a jelszóváltoztatást javasolnátok előtte és utána. Mer ez így egy betarthatatlan hülyeség, amit TI sem gondoltok komolyan.

A cikk többirészevel egyetértek, open wifit nehasználjunk meg inkább a sajátot, de belátható, h ez nem mindig kivitelezhető.



Sir Nyű 2011.08.24. 14:27:29

Magyarán ha az ember elmegy otthonról, akkor visszaugrik 20 évet az időben és marad a sorállás meg a papíron kitöltött átutalási megbízás?

Hogy intézzek mondjuk valami hirtelen jött banki/vásárlásos cuccot, ha nem othon vagyok?

B Tomi 2011.08.24. 14:59:57

[@Zoli \(SSDB\)](#): "a levelezését, az arra érkezett méleket szeretné megtekinteni ... Egy tök üres emailcím csak kevert okozna." - a saját, valódi fiókodban az utazás idejére beállíthatod, hogy az ideiglenes címre forwardoljon, az ideiglenes fiókban pedig a reply-to mezőt kell a saját címedre állítani. Így az eredeti fiókba való bejelentkezés nélkül látod mit kaptál, és írhat sz is a címzettek összezavarása nélkül.

ace22 2011.08.24. 15:56:40

A két utas autentikációt (értem ez alatt a bejelentkezés után SMS-ben elküldött egyszerhasználatos kódot) az általam ismert

netbankok is használják.

A gmail-nek létezik https-es változata - meg tudja valaki mondani, hogy open wifi-n keresztül a https-es oldalak használata vajon biztonságos-e? A POP/SMTP valószínűleg nem az.

Az internetkávéházakat / idegen gépeket nem kérdezem, oda a rendszergazda telepíthet keyloggert...

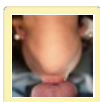
[□ hi \(□ □ □\) 2011.08.24. 16:00:26](#)

@B Tomi: Ha még el is fogadom, hogy email esetében működhet (nem feltételezve, hogy mondjuk valami régebbi emailt kéne elővakarni a postafiókomból, ami kellene a válaszhoz és csak a régi vagyis eredeti postafiókomban van meg). Fészbukon tutti nem működik... vagy mégis hogy? Kapok egy üzit válaszolni másképp nehezen tudok, jó esetleg még játszhat az email, de a news feed meg h újat írj mindenképp bekell lépni, a Fészbuk csetről nem is beszélve...

Szal kicsit ez a része nekem még mindig járhatatlan. Jó az alap h olyan cuccokra egy más jelszót és ugyanazt használok, amivel belépek nem csak saját gépen is. (értsd fb, mail, msn)

[Zoli \(SSDB\) 2011.08.24. 16:01:45](#)

Hogy mivel nem vitatkozom és tiszta legyen: a netbank, átutalás, kártyás fizetés tényleg csak otthoni gépen és/vagy saját telefonon mobilnettel.



[mxplanet 2011.08.24. 17:16:05](#)

@Zoli (SSDB): facebookon is be lehet allítani az sms kodkerest, ha idegen geprol jelentkezels be.

[felszopó 2011.08.24. 18:32:54](#)

én még itt értelmes dolgot soha nem bírtam olvasni, pedig nézegetem már egy ideje

[Dr. Shit Pál \(törölt\) 2011.08.24. 18:34:11](#)

K&H netbanknál külön kell sms a belépéshez és egy másik, hogy utalj, Budapest Bank netbankjánál pedig időkorlátos, de ott is kell sms a belépéshez, szóval ez azt hiszem elegendő. Kártyaszám bepötyögése már rizikósabb.

Mail, FB cinkes, de érdemes és egyszerűbb inkább a jelszót átállítani az utazás idejére, utána vissza. Nyaralós jelszó. :P

[különvélemény 2011.08.24. 18:40:33](#)

1, a netbank (értelmes banknál) eleve többlépcsős, persze érdemes óvatosnak lenni, de a paranoiának nincs helye. Nyilván külföldről, idegen gépről, csak vészhelyzetben, egyszer szabad belépni, akkor is inkább mi kérjünk kölcsön egy notit valakitől, mintsem nyilvános helyről. A sms terhelésértesítés eléggé követhetővé tesz mindent.

2, ki nem tojja le a faszbuk jelszavát? :D

3, saját gépen, idegen wifin, https felületen elenyésző az esélye, hogy valaki heteket töltene az adatfolyam visszafejtésével.

[különvélemény 2011.08.24. 18:47:18](#)

De aki nagyon paranoiás, az nyugodtan leragaszthatja/lefestheti a kártyája hátulján lévő 3 jegyű kódot, ugyanis azzal a legkönnyebb visszaélni.

Az legtöbb kasszánál kamera veszi a pénztárakat, így aki a kamerát nézi az láthatja a bankkártyaadatokat, a hátulján lévő kóddal együtt (mivel a pénztáros megfordítja a kártyát az aláírás miatt) így simán vásárolhat vele a neten.

Jelek

2011.08.26. 13:40 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [malware fertőzés jelek](#)

Milyen intő jelekre figyeljünk, hogy észrevegyük: kártevővel fertőzött a számítógépünk? A fő visszatérő szállóige a következőkben a váratlan és a kéretlen lesz. Szájabarágó, összefoglaló.



Az egyik legjellemzőbb, hogy **váratlanul és kéretlenül popup ablakok bukkannak elő azzal, fertőzött a gépünk**. Nem jellemző, hogy pont egy weboldal tudná megmondani kézzel elindított keresés nélkül így interurbán, mi van a gépünkkel, [kivéve mondjuk a confickertest oldalán](#), de oda sem váratlanul vagy kéretlenül jutunk, hanem direkte a vizsgálat szándékával. A felbukkannó ablakok különbözőek lehetnek, eleinte elég volt a becsapáshoz a Windows Antivirus XP stílusú ablak is, [később már a böngészők testreszabott hibaablaka jelent meg](#), hogy mindez **"hitelesebben"** nézzen ki. Egy másik alfaja **nem fertőzési üzenettel, hanem számítógép optimalizálási blablával próbálkozik, egyiknek se dőlünk be**. Mind a vírus- és kémprogramvédelemre, mind az optimalizálásokra (CCleaner, Ausloglic Defrag, etc.) válasszunk saját profi programot, és higgyünk inkább azok eredményeinek.



Szintén **váratlanul fájlok, könyvtárak, ikonok tűnnek el, vagy változnak meg látszólag ok nélkül**. Jel - bár önmagában nem a fertőzés szinonimája - ha számítógépünk váratlanul és látványosan lelassul. **A kihasznált, kompromittált gép a saját programjaink futtatásán kívül még egy rakás más kéretlen feladatot is ellát**: kémked, spammel, elosztott támadásokban vesz részt, stb, és ezek erőforrásokat emésztenek fel, magyarul lassul a gép. Ugyancsak [gyanús lehet, ha olyan weboldalhoz próbál meg gépünk kapcsolódni, amit nem is ismerünk, nem mi kezdeményeztük azt](#), olyan ismeretlen alkalmazás próbál meg magától elindulni, amit nem mi kértünk.



Szintén egy tipikus jel, ha **felbukkanó ablakokban pornográf vagy reklám tartalmú képek jelennek meg**. Ha esetleg mi telepítettünk ilyen kétes, titokban kémkedő vagy reklámokat megjelenítő alkalmazást, akkor szabauljunk meg tőle. Ha NOD32-t vagy ESET Smart Security programot használunk, akkor pedig **pipáljuk ki a Kéretlen alkalmazások keresése jelölőnégyzetet**, ez a rossz hírű, pl. túl sok személyes adatot összegyűjtő leplezett kétes alkalmazásokra - választásunknak megfelelően - a jövőben már riasztani fog.



Az eseti elhárítás és a hosszútávú távoltartás biztonság tudatos lépéseinél sem találtunk fel új verziós spanyolviaszt: **ez az operációs rendszer biztonsági frissítésekkel való naprakész ellátását, igazi és uptodate vírus- és kémprogramvédelmi alkalmazás használatát, megfelelő biztonsági kiegészítőkkel felvértezett böngészőkliensre való áttérést és nem utolsósorban gondosan mérlegelt, és alaposan lekáderezett programok jövőbeni telepítését jelenti**. Komolyabb malware támadás esetében az eltávolításhoz esetenként csökkentett módban való rendszerindítás, vagy bootolható mentő CD lemezről történő helyreállítás szükséges, illetve kérhetjük még a support csoport technikai támogatását is.



Érdemes tehát néha felfigyelni, ha számítógépünkön szokatlan események történnek, és időnként a [Zombi-e vagy című kiskátét is praktikus lehet újraolvasni](#). Ha pedig **valaki olyan kártevőt ismer, amely váratlanul és kéretlenül nem lelassítja, hanem éppen felgyorsítja a**

számítógépet, az kommentezzen bátran;-)



20 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Ez történik a weben egy perc alatt](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3181915>

Kommentek:

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

[cworm](#) 2011.08.27. 22:17:36

Jaj, nem bírtam végigolvasni a postot, túl sok benne az elírás, gépelési hiba...:(Légyszi kicsit figyelj oda jobban, mert így "élvezhetetlen". (a grammar nazi kommenteknek meg álllok elébe:D)



[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu> 2011.08.28. 09:43:31

Halihó!

Természetesen teljes mértékben igazad van, de 35 fok meleg volt, ritka gyenge szakadozó mobilnetes idegen számítógépen és közelebbről meg nem nevezett (nem akarod tudni) extrém körülmények közt született ez a poszt. Mostanra már viszont kijavítottam a betűhibákat.



[TrueY](#) • <http://qltura.blog.hu> 2011.08.28. 17:22:42

Nekem Linux alatt még nem volt vírusom. Igaz windows alatt sem. Bár DOS 3.1 alatt már fogtam párat. :) Az is igaz, hogy az ember soha nem lehet biztos benne, hogy nem vírusos a gépe...

És mai hívószavunk pedig: OpenCloud

2011.08.30. 17:11 | [Csizmazia István \[Rambo\]](#) | [1 komment](#)

Címkék: [antivirus](#) [rogue](#) [opencloud](#) [álvírusirtó](#)

A mai modern vírusok egy része már támaszkodik valamennyire a cloud technológiára. Például az [új 5-ös NOD32 leírása szerint a felhő alapú védelem](#) esetében a felhasználók számítógépeire telepített védelmi szoftverek folyamatosan kapcsolatban állnak az ESET szervereivel, és egy új károkozó ellenszerének kibocsátása után szinte azonnal frissíteni fogják a védelmüket.



Hasonló felhős szlogenek kísérik a viccesnek szánt videóval beharangozott Kaspersky 2012-es programverziójának ismertetését is: "[a combination of cloud and local detections](#)". A fentiek fényében ha egy új vírusirtó **neve mellett láthatjuk a "Cloud" szócskát**, az eredeti szereplőkön kívül na vajon ki profitálhat még ebből? Bingó, igen, úgy van, jól mondja, az nyerte meg a hangszórót, aki arra tippelt, **az ehetséges hamis vírusirtók aktuális nevei is ezt fogják tartalmazni**.



Az unalomig ismert zöld csíkos pajzs, az unalomig ismert "fizessél, mert szeretjük a sok pénzt" szabvány ablakok: vele szemben néz farkasszemet látszólag hiába a rengeteg poszt, cikk, [a pénz útját is leleplező biztonsági szakértő](#), csilliónyi figyelmeztetés világszerte - és mindez mégis kevés. [Az OpenCloud Antivirus már köztünk jár](#), és **valójában annyi köze van a felhő alapú technológiához**, mint a versenyszférában működő munkáltatóknak az egykulcsos jövedelemadóából adódó bércsökkenések kompenzációjához ;-). Ám nem kétséges, [mégis van pénz a számlájukon](#).



Ára mindössze 52.95 USD, ami ahhoz képest, hogy Open is, meg Cloud is, sőt az Antivirus nevet szintén viseli: baráti és jutányos, ám ahhoz képest hogy nem csinál semmit, sőt még meg is fertőzi a gépet, kifejezetten sok. Egyetlen pozitívuma talán mégis lehet a dolognak, ez pedig a megértés. Mert más az látni az árat valamin, és más azt ki is fizetni. Nekünk nem kell a hajunkat tépni olyan ["mi kerül ezen a Darius fotelon 7200 forintba"](#) jellegű kérdéseken, tisztán és világosan tudjuk, látjuk, értjük, a semmi kerül ennyibe, és persze az is nyilvánvaló, [hogyan lehet mindezzel 32 milliót keresni hetente](#).



Talán az, aki az ilyen tanulópenzt egyszer már sajátpénztárcájúlag kifizette, remélhetőleg utána már egy életre megjegyzi az idevágó tanulságokat. Reménykedjünk.



5 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



0



Ajánlott bejegyzések:

- [Akiknek a Captcha kinszenvedés](#)

- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3190026>

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! 2011.09.05. 19:16:54](#)

Begyűrűztek az új trendek hát. Az aljas kamuantivírusírók pedig százával (ezrével?) fogják a madarakat. Meg kell tanulni: cipőt a cipőboltból, megbízható vírusirtót csakis jól csengő, bejáratott névtől.

Fidel Castro halott vagy mégsem?

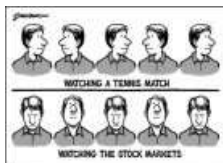
2011.09.01. 14:10 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [csalás](#) [fidel](#) [trójai](#) [castro](#) [kártevő](#) [kryptik](#) [halálhír](#)

A posztíró életkora okán még úttörőnyakkendősen osztályostól ki volt vezényelve az utcára anno, hogy hurkapálcika nyelvű magyarázóslócskával személyesen integethessen a hazánkba látogató és fenegyerekesen nyitott kocsiban érkező Fidel Castronak. **Vajon most tényleg meghalt**, ahogy a kérértlen email írja?



Egész kazalnyi irodalma van már a "Döbbenet, meghalt a híresség, kattints ide most!" kezdetű spam és kártevő terjesztő kampányoknak, hogy csak két emlékeztető példával rukkoljunk elő, [nálunk is meghalt már blogon egyszer Johnny Depp](#), és még az állítólagos autóbalesetben összeroncsolódott állítólagos gépkocsiról is volt állítólagos fotó, de említhetjük akár [Eminemet is, akiről futószalagon készülnek hamis üzenetek](#) a naív kattintások reményében, és talán akkor kezdhethetünk el egészségi állapotával kapcsolatosan komolyabban aggódni, ha váratlanul egy hétig szünetelnek az ilyen halálhírek.



Még egy hónapja sincs, amikor a Nakedsecurity beszámolt a [Fidel Castro állítólagos halálhírét közlő kérértlen emailről](#), amely még **koporsós fotót is közölt**, ami 21 évvel a Photoshop megszületése után persze nem is akkora teljesítmény. Az augusztus elejei levél arról értesített bennünket, hogy **a kubai diktátort otthonában érte a halál**, és szívrohamban hunyt el. Persze a rákattintás különféle trójai kártevővel gazdagította a naiv felhasználókat, akik végig sem gondolták, vajon egy CNN vagy BBC miért nem számol be erről a jelentős hírről. Nyilvánvalóan azért nem, mert nem igaz.



Az álhír nagy valószínűséggel azért lehetett ilyen sikeres, mert **erős a titkolózás Castro egészségi állapota körül**. Állítólag Castro négy alkalommal vett már részt kemoterápiás kezelésen, ám az első hamis halálhírt leleplező beszámoló után [a spam terjesztés nem állt le, azt látszólag azóta is küldöztetik](#) a Foxnews beszámolója szerint.



Kiknek jó a hamis hírek zavaros vízében halászni? A kártevőterjesztés részen túlmenően a különféle hamis hírekkel operálva olyan folyamatokat is lehet befolyásolni (dezinformáció), [amelyek közvetlen vagy közvetett haszna van egyes érdekcsoportoknak](#). Ez lehet az olaj ára, de azok, akik shortolnak szintén **jelentősen befolyásolhatják a gazdasági folyamatokat, sőt akár bankcsődöt is okozhatnak, és olykor a hír valóságától teljesen függetlenül**.



Ilyen, a pénzügyi piacok ingadozását meglovagoló úgynevezett [pump and dump csalási forma](#) további erősödéséről számol be a Symantec jelentése is, amely [2011 első hét hónapjának vizsgálatára alapul](#). Magunkat idézve, a "pump and dump" módszer olyan részvénytulajdonosi taktikát jelent, amikor a számítógépes bűnözők a gyors meggazdagodás reményében egyes, főleg **kis cégek részvényeiről olyan hamis híreket, ál előrejelzéseket, információkat közölnek (például spam üzenet formájában)**, amelyből a potenciális befektetők tévesen úgy gondolják, emelkedni fognak a cég papírai. A mesterségesen felkeltett érdeklődésnek a spam kampány végeztével azonban vége szakad, **a papírok árai gyorsan leesnek, és a befektetők pedig tönkre mennek**.



Nyilván van még valamennyi idő, amíg a soronkövetkező kéretlen levélből megint tájékozódhatunk, milyen részvényt vegyünk gyorsan, melyik híresség is halt meg újfent, de talán **érdemes lenne azon is elgondolkodni**, hogy ahogyan a megbízható programokról előzetesen alaposan tájékozódunk, azokat figyelmesen kiválasztjuk, továbbá ilyeneket nem is töltünk le akárhonnán, hanem csak ismert, ellenőrzött, hiteles helyről - ugyanígy **a hírek világában is élni kellene valamiféle egészséges kontrollnak, kiben és milyen portálokban, forrásokban bízhatunk.**



Talán annak is eljön majd egyszer az ideje, hogy a kéretlen spamet senki nem tekinti érdemi mértékadó hírforrásnak. Addig pedig a "[Kavarja ez vagy nem kavarja](#)" klasszikus kérdésre a helyes Fülíg Jimmys válasz az lehet: "Megint nagyon valószínűen hangzik, amit mond, tehát biztos, hogy hazudik. A valódi kérdés inkább az, hogy időben észreveszem vagy felismerem-e mindezt, és rájövök mi is a rejtett célja az egésznek."

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3194968>

Kommentek:

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

Nincsenek hozzászólások.

Ez itt a Microsoft távoli hozzáférés, vagy mégsem?

2011.09.05. 16:00 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [microsoft](#) [remote](#) [uk](#) [vagy](#) [access](#) [phishing](#) [mégsem](#) [adathalász](#)

Vagy mégsem rovatunk bugyra szemlátomást kifogyhatatlan, mindig akad benne újabb muníció. Ezúttal arra figyeltek fel biztonsági szakemberek, a **Microsoft** nevével és a **távoli hozzáférés lehetőségével visszaélve** bűnözők adathalász támadást indítottak az Egyesült Királyságban.



Távolinak éppen távoli, meg persze hozzáférés is, a kérdés inkább az, tudjuk-e egyáltalán, ki is a hozzáférő, vajon kinek tárjuk önként sarkig a kaput. A dolog egy hívással kezdődik, ahol **a telefonáló magát a Microsoft egyik partnercégének, az E-Pro Solutions munkatársának adja ki magát**, és azt állítja, az MS-től közvetlenül kapta meg ezt a számot, hogy segítsen. **A történet szerint a felhasználó gépe állítólag megfertőződött, de ők majd ezt szívesen orvosolják.** Mutatnak is egy hibaüzenetekkel ékesített könyvtárat mintegy bizonyítékul, majd kezdetét veszi maga a csalási processzus.



A gyanútlan áldozatot ráveszik, hogy [látogasson meg egy előre megadott weboldalt](#), majd aztán ennek segítségével távoli elérést szereznek [a számítógépre](#). Ám a folytatás már nem ilyen olajozott: **az állítólagos mentesítés előtt váratlanul pénzt követelnek azzal, hogy csak ezután történhet meg a fertőzés eltávolítása.** A dolog pikantériája és különlegessége abban áll, hogy **az idáig eljutott történet logikailag már jól nem végződhet a felhasználó szemszögéből**, azaz Murphysen: [a játékban nyerni nem lehet, döntetlent elérni nem lehet, a játékból kiszállni nem lehet.](#)



A naív ügyfél vagy fizet a semmiért, és lássuk be így sem jár jól; vagy ha esetleg megtagadja a fizetést, akkor pedig a távoli kapcsolaton keresztül érheti még számos kellemetlenség. Persze kihúzhatná a netet gyorsan, persze átvizsgálhatná és kigyomlálhatná a gépét a megfelelő biztonsági eszközökkel, de **őszintén szólva ha valaki mindezeket már ilyen frappánsan tudná, az meg nem is hitte volna el ezt az egész [kéretlen hívással érkező support trükközést](#).** A legvalószínűbb tehát, hogy aki ebbe beleesik, az később a folytatásban is baráti, rendszergazdai, support segítségre szorul, **vagy tárcsázhathja a National Fraud authority hotline számát (halló, itt a National Fraud authority, vagy mégse ;-)**



Jegyezzük hát meg kilencezerhatszátnegyvenharmadszor, hogy bár a vírusirtó önmagában hasznos dolog ugyan, de **odafigyelés, óvatos hozzáállás, gyanakvás, biztonságtudatosság nélkül időnként egészen egyszerűen nem elegendő: [social engineering volt, van és lesz.](#)**



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



[Tweet](#)

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3204159>

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.

Génmódosított Zeus botnet

2011.09.07. 12:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [botnet](#) [kártévő](#) [zeus](#) [visszafejtés](#) [eltávolítás](#)

Na jó, a cím dacára nem akarunk GMO-s kukoricákkal, búzákkal és Dolly fedőnevű bárányokkal vetélkedni, ennek ellenére a Zeus botnet új verziójában egy valóban érdekes és egyben kellemetlen változást észleltek az antivírus kutatók.



A napi **temérdek újonnan megjelenő kártévő rengeteg munkát ad a víruslaboroknak**, ezért sok láblógatást nem igazán látni ezeken a munkahelyeken. Ezzel szemben igen sok igyekezet fordítódik arra, hogy minél jobban lehessen automatizálni a nagyszámú egyszerűbb eseteket, az egyedi kézi visszafejtések tanulságaiból pedig lehetőleg minél több generikus felismerési minta születhessen, és - ide kapcsolódik a mai poszt is - **ha valami aprócska hiba vagy extra lehetőség van a kártévő szerkezetében, azt bónuszként a magunk javára fordíthassuk.**



Ahhoz, hogy az új botnet verzió változását jobban megérthessük, nagy vonalakban elég annyit tudni, hogy **miután az antivírus cégek sikeresen visszafejtették a Zeus kártévő titkosító algoritmusát, már képesek voltak arra, hogy ezen információk birtokában és az úgynevezett GetFileAttributesExW API függvény segítségével lekérdezzék az adott bot nevét, pontos verzióját - és itt jön a lényeg - még egy pointer címet is, amellyel teljes visszafejtés nélkül is könnyen el lehetett távolítani a fertőzést.** A gépek mentesítésekor ez véletlen felfedezés mondhatni nagyon jól jött.



Ám minden öröm és boldogság addig tart, amíg ez nem szúr szemet a kártévő fejlesztőknek, és sajnos pontosan ezt történt most. **Eltávolították ugyanis ezt a bizonyos pointer címet, így aztán mostantól már nincs tovább magas labda, ezt az ajándék kiskaput most bezárták a vírusvédelmi szakemberek előtt.** A Trendmicro elemzése szerint az új variáns látszólag célzottan az Egyesült Államokban, Spanyolországban, Brazíliában, Németországban, Belgiumban, Franciaországban, Olaszországban, Írországon és Hongkongban található pénzügyi cégeket irányozta meg.



Ilyen hasznos felismerések egyébként korábban is születtek már, gondoljunk csak a számítógépes állományokat [titkosító és azok visszaállításáért pénzt zsaroló GPCode](#) kártévőre. Az egyik 2008-as variáns esetében Kasperskyék rájöttek, hogy a már elkódolt állományok eredeti állományainak törlése egyszerű delete funkcióval történik, ezért minden „Undelete” segédprogram segíthet azokban az esetekben, ameddig még nem történt felülírás a lemezen. Természetesen idővel aztán itt is jött a következő, fejlettebb változat, amely Murphyvel szólva "gonoszságban és rombolásban újat tudott mutatni", de az biztos, hogy **az ilyen szerencsés apró észrevételek - még ha csak ideiglenesen is lehet élni velük - hasznosak a víruskutatóknak.**



Visszatérve Zeushoz, szóval ha a **búlváros cím nem is igaz teljesen, de biztos jól hangzik ("New Zeus bot could be antivirus-proof")**, azért valóban megnehezítettek a dolgokat. Lehet, hogy a kártévőkészítők mindegyike teljesen maguktól jöttek rá, de az is lehet, hogy valahol valaki eldicsekedett a neten a trükkös kinderspiel mentesítő függvényhívással, és arra reagáltak. Az viszont több, mint valószínű, figyelik és követik az antivírus gyártók minden lépését, és nem félnek használni új ötleteiket munkájuk folyamatos

megnevezítésére.



 Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:



- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3208448>

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.

Emlékezés 9/11-re kattintással

2011.09.10. 22:20 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [911 évforduló](#) [csalás](#) [kattintás](#) [kártevő](#) [kéretlen](#)

Éppen antivírust telepítettünk a Paksi Atomerőműben, mikor az egyik ott dolgozó felénk fordította monitorját a képen egy égő toronnyal. Mivel átverős photoshopolt képeken nőttünk fel, **eleinte nem is hittük el, de aztán mikor az Index, Origó portálokon és az előkapott Junoszty rendkívüli híradásában is ezt lehetett látni**, már éreztük, hogy valami olyan rendkívüli és félelmetes dolog történt, aminek a következményei beláthatatlanok.



Sokszor és sokat beszéltünk már arról, hogy **az évfordulók, ünnepek, valódi és kitalált tragédiák azok az apropók, amit a kártevőterjesztők remek érzékkel kihasználnak**. És nincs ez másként [az éppen tíz esztendeje történt New York-i eseményekkel](#) kapcsolatban sem, **szemlátomást belendült a gépezet, és igyekeznek meglovagolni az érdeklődést**. Nyilván a szeptember 11-e önmagában is minden évben a középpontban van, de **a kerek évforduló** még ezen is tud erősíteni.



[Frissiben regisztrált kétes weboldalak a legkülönbözőbb ötletekkel operálnak](#): van kéretlen levél, amelynek URL-jében érdekes tartalmat kínálnak: "Bin Laden mégis él", "Új ismeretlen részletek a terrorista támadásról" vagy "A rendőrségi nyomozás végeredménye". A próbálkozások aztán innentől már vegyesek, **van amelyik kártevőt terjeszt, van adathalász kísérlet, hamis antivírus oldalra is juthatunk video helyett, de a biztonsági szakemberek már hamis adománygyűjtő oldallal is találkoztak, sőt az állítólagos "eredeti helyszíni ereklék"** árverési piaca is pezseg a csalók hamis tárgyaitól.



Nyilvánvalóan az érdeklődést tovább fokozza, hogy sok megmagyarázhatatlan furcsaság kísérte ezt az egész történetet, emiatt aztán [az összeesküvés elméletek kedvelői is hozzászóltak](#) a maguk véleményét, sőt a [Fahrenheit 9/11 című film is egy elgondolkodtató darab](#) volt Michael Moore-tól. Ennek ellenére a kártevő kampányokat figyelve South Parkosan úgy fogalmazhatunk: az évforduló rossz, mert az évforduló rossz: [ilyenkor ugyanis jelentősen sűrűsödnek a támadási kísérletek](#). És a java, a naptár szerinti évforduló csak most jön még.



Emlékezhettünk, [alig halt meg Amy Whitehouse](#), máris megjelent a nevével kapcsolatos csalás. Karácsony vagy Valentin nap közeledik? **Jönnek a kéretlen linkek állítólagos üdvözlőlapokról, vicces videókról, szenzációkról**. A sor a Haiti földrengéstől kezdve Osamáig töretlen, és **jöjjön a rossz hír: a kéretlen küldözgetésnek az "egy újszülöttnék minden vicc új" elve alapján sosem lesz vége**.



Ami biztos, hogy [nekünk magunknak kell megváltozni](#), nem mindent elhinni, óvatosabbnak lenni, [kéretlen dolgokra nem kattintani](#). A **végére tartogatott jó hír pedig az, hogy mindez tanulható: a saját vagy más kárán**, szóval még választani is lehet.



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



1



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3213142>

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! 2011.09.10. 23:41:46](#)

Ez a Whitehouse direkt volt? :)

Egyébként újfent nem lepődtem meg, az aljas emberek minden apropót kihasználnak.

Restore, Recovery és Repair elementek vadászni

2011.09.13. 12:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [windows](#) [csalás](#) [hamis](#) [rendszerkarbantartó](#) [recovery](#) [repair](#) [restore](#)

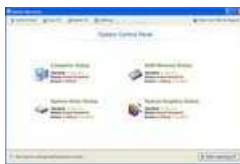
Nem az az igazi újdonság, hogy [az álantivírusok készítői rendre új vízeken is kipróbálják magukat](#), az érdekes inkább az, hogy szemlátomást bejött nekik ez az új vadászterület, és **most már nagyüzemileg ontják a változatos nevű hamis rendszerkarbantartó programokat**. A választott antivírus alkalmazás mellett ezért érdemes alaposan átgondolni azt is, milyen segédprogramban bízunk meg a Windows karbantartásnál.



[A jó név félsiker](#), mondta egyszer egy nagy ember ;-) Ma már rengeteg féle, kitalált és már meglévő termék nevére hasonlítani akaró csaló program terjed a fertőzött weboldalakon keresztül, így a nagyobb, mentesítést segítő tanácsadó oldalak [hozzácsapták a hamis antivírusok mellé az álrendszerkarbantartó programokat is](#).



Az elve analóg a hamis antivírussal: mindenféle bajt és rendellenességet jelzek a naiv felhasználónál felugró ablakban (például a frappáns hangzású "Exception Processing Message 0x0000013"), majd **ha rendbe szeretné tenni a gépet, ahhoz előbb fizetni kell** - ugyebár a semmiért.



Sokasodnak az új nevek [a korábbi Smart Defragmenter, HDD doctor és hasonlók](#) mellett: Windows Restore, Windows Recovery, Windows Repair, Windows XP Recovery, és lehetne folytatni napestig. A megoldás érdekében használjunk naprakész igazi vírusirtót, **ne telepítsünk ismeretlen rendszerkarbantartó programot, pláne nem netezés közben felugró ablakban kérés nélkül megjelenő fizetőset**.

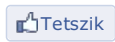


Ám a különféle segédprogramokkal kapcsolatos csalási módok ezzel még nem merültek ki, hiszen **ha például diagnosztikai vagy benchmark programot keresünk, akkor is könnyen belefuthatunk olyan kétes alkalmazásokba, amelyek trójait, kémprogramot, de legalább egy kéréses reklámkomponenst megpróbálnak feltelepíteni a felhasználók gépére**. A megoldás itt is az lehet, hogy előzetesen alaposan utánanézzünk, milyen programot válasszunk erre a célra, például a [magyar fejlesztésű Aida64 alkalmazással](#) elkerülhetjük az ilyen csapdákat.



Magyarán nem csak az antivírusnál, de a rendszerkarbantartó programoknál és **tulajdonképpen bármilyen alkalmazásnál is érvényes, hogy alaposan ellenőrizni kell a programot még telepítés előtt**. Kik a fejlesztők, van-e elérhetőségük, telefonszámuk, postacímük,

telephelyük, nyújtanak-e igazi terméktámogatást, miként vélekednek a programról a neten, és vajon [az alkalmazás nevét begépelve a Google találatai nem mind "How to Remove"-val kezdődnek-e](#). Ha erre is odafigyelünk, az már egy újabb jólírányzott téglát a biztonságtudatosság falában.



4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



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/3222548>

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.

BIOS módosító trójait találtak

2011.09.14. 10:20 | [Csizmazia István \[Rambo\]](#) | [5 komment](#)

Címkék: [award phoenix trójai kártevő bios mbr mebromi](#)

A kártevő módosított kódot telepít az alaplapi BIOS-ba, és olyan utasításokat fűz hozzá, amelyek még a számítógép Boot Up Sequence folyamat alatt hajtódnak végre. A Trojan.Mebrominak nevezett rootkit a Phoenix Technologies által gyártott Award BIOS-okat támadja, és igencsak nehezen lehet tőle megszabadulni.



A BIOS-t támadó kártevők általában nagyon ritkák. Idősebbek és katonaviseltek még emlékezhetnek a [múlt századi CIH vírusra](#), az első jelentések róla 1998 elejéről származnak, az idők során pedig jó néhány változata született. Különlegessége, hogy a Pentium processzorral rendelkező számítógépekben olyan hibát volt képes okozni, amely a hardver javítása nélkül nem orvosolható: **a gép elindulásához szükséges BIOS PROM-ot tette tönkre felülírással.** A legismertebb és legelterjedtebb verzió minden év április 26-án aktivizálódott. Ez a változat azonban csak 1998 közepén terjedt el szélesebb körben, így az első valódi aktivizálódási dátuma 1999. április 26-a lett. Még itthon is adtak ki számítástechnikai laphoz olyan havi CD-mellékletet, amely véletlenül ezzel a vírussal volt fertőzött. A kártevő a nevét a tajvani illetőségű készítőjéről, a kezdőbetűk alapján Chen Ing-Hauról kapta.



Ez a mostani Mebromi azonban ennél fejlettebb, és a korai rendszerindítási szakaszban a BIOS módosításával operál. [A Master Boot Rekord \(MBR\) átírásával még az operációs rendszer betöltése előtt képes fertőzni](#), ezzel pedig a Windows XP, 2003, Vista és Windows7 rendszerek kerülhetnek veszélybe. [A fertőzött BIOS minden esetben betölt egy hook.com nevű fájlt, amely azt ellenőrzi, vajon fertőzött-e az MBR, és szükség esetén újrafertőzi azt.](#)



A mellékelt képen az is jól látszik, hogy [a kereskedelmi forgalomban lévő antivírusok többsége szerencsére már képes detektálni](#), ám érdekes módon éppen a Microsoft programja nem észleli.



Bár [a hírek szerint Mebromi-t ugyan valós környezetben találták \(In The Wild\)](#), de egyelőre csak Kínából jelentettek ilyen fertőzéseket. Ám a mentéssel kapcsolatos lecke mindenestre fel van adva az antivírus fejlesztőknek, ugyanis **ennek nehézségét nyilván fokozza, hogy nem egyszerű olyan univerzális BIOS ellenőrző/mentesítő/helyreállító utilityt írni, amely annyira bombabiztos, hogy a helyreállítással nem okoz bajt, és garantáltan minden egyes gépen működik.** Azt viszont mindenképpen érdemes megemlíteni, hogy elméletileg nemcsak az alaplapi BIOS lehet ilyen célpont, hanem minden olyan eszköz, amelynek a firmware-jét támadni lehet, ez lehet például akár egy router is.



35 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- ["Szósölmédia" és nyaralás](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [25-ször több a mobilos kártevő](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3226228>

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 2011.09.14. 10:53:12](#)

A képen is látszik:

"There is a more up-to-date report (36/43) for this file." És ott már az MS is ismeri.:)



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu>](#) [2011.09.14. 11:05:13](#)

Hűh, jogos az észrevétel, köszi. Szóval az újabb, 2011.09.14.-es VT riport szerint már az MS is észreveszi.

Köszi Cworm :-)

[Med1on 2011.09.15. 00:32:48](#)

A cikk egy részlete - természetesen a forrás megjelölésével - felhasználható más weboldalon?



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu>](#) [2011.09.15. 08:26:17](#)

Szia Med1on!

Üdv a blogon. Természetesen a forrás feltüntetéssel mehet bátran.

[Med1on 2011.09.15. 16:16:28](#)

[@Csizmazia István \[Rambo\]](#): Üdv és köszönöm. :)

Itt az ötödik generációs védelem az ESET-től

2011.09.15. 08:32 | [Csizmazia István \[Rambol\]](#) | [9 komment](#)

Címkék: [security](#) [smart](#) [new](#) [nod32](#) [eset](#) [gyorsabb](#) [5.0](#)

Az ESET bejelentette, hogy [elérhető a NOD32 Antivirus és az ESET Smart Security új változata](#) az otthoni felhasználók számára.



A szoftverek ötödik generációja felhő alapú védelmet is tartalmaz, melynek segítségével **az új kártevők felismerése még gyorsabbá és hatékonyabbá vált.** Mostantól a felhasználók számítógépeire telepített védelmi szoftverek folyamatosan **kapcsolatban állnak a gyártó szervereivel**, és egy új károkozó beazonosítását követően **szinte azonnal frissítik** a védelmüket.



Emellett az ESET belső tesztjei szerint az új verziók ismételt **kézi indítású víruskereséskor 20%-kal gyorsabban teljesítenek az előző generáció tagjainál, és a számítógép gyorsabb indítását is lehetővé teszik.** Az ESET NOD32 Antivirus 5 és az ESET Smart Security 5 egyaránt lehetőséget nyújt a **külső adathordozók vírusvizsgálatának egyéni konfigurálására**, a Smart Security új verziójában pedig fejlődött a szülői felügyelet is, így a szülők a korábbiaknál könnyebben, kategóriák alapján választhatják ki, hogy mely weboldalakhoz kívánják letiltani gyermekeik hozzáférését.



Egyelőre mindkét szoftverből kizárólag **az otthoni felhasználóknak szánt kiadás jelent meg**, a központi menedzsmentet és bővebb konfigurációs lehetőségeket tartalmazó üzleti változatokat 2012 első negyedévében bocsátja ki a gyártó. Az ESET licencpolitikájának köszönhetően **a jelenlegi verziók felhasználói díjmentesen térhetnek át az új változatokra.**



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászáttal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3228743>

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](#).

mateo4 2011.10.08. 10:48:12

Lenne egy kérdésem! Avast! vírusirtó van a gépemen, de sok jót hallottam az ESET új verziójáról és szeretném kipróbálni. Megférnek egymás mellett anélkül, hogy fognák a gépet? Szerinted melyik a jobb? Előre is köszi: mateo4



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.10.08. 20:47:45**

Szia Mateo4!

Én is úgy érzem, ez a mostani 5-ös nagyon jól sikerült. Egyszerre biztos nem tudod tesztelni próbálgatni, mert valósidejű védelemből egy időben csak egy lehet feltelepítve, ez fontos, vagyis egyik leszed, másik feltesz, így működik.

Ahogy utolsó pár teszteredményre emlékszem, mindkettő a kifejezetten gyorsak közül való, az ESET korábbi 3-as és 4-es kicsit lassult, amit most az 5-ösben szépen javítottak.

Igazából én internetsecurity csomagban (vírusirtó, kémirtó, rootkit detektor, spamszűrő, HIPS, szülői felügyelet, tűzfal, stb.) gondolkodnék a helyedben, nem szimpla vírusirtóban, így a Smart Security szerintem megérhet egy próbát, amihez természetesen van 30 napos próbaidőszakos kulcs.

A melyik a jobb kérdéshez pedig ezt az URL-t ajánlom neked, további kellemes hétvégét:
itcafe.hu/tema/melyik_a_legjobb_virusirto_progi/hsz_1-50.html

mateo4 2011.10.09. 10:09:42

Köszi a választ, a cikket elolvastam és sokat segített, ahogy a válaszod is. :) Még egyszer köszi: mateo4

mateo4 2011.10.09. 10:15:53

Bocsi, de van még egy kérdésem: Mi van, ha lejár a 30 napos próbaidő?
Ismét előre is köszi: mateo4



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.10.09. 20:43:57**

Ha lejár, akkor az alábbi lehetőségeid vannak:

- ha Chip vagy PC World olvasó vagy, akkor abban kapsz minden hónapban kódot
- megvásárolod a licencet, és itt vannak különféle kedvezmények is, például ha diák vagy, akkor 50%.

mateo4 2011.10.10. 16:33:34

Ismét köszi, még egy kérdés:

A NOD32 egy technológia?

(amúgy tényleg bocsi, hogy ilyen sokat kérdezek, de nem vagyok szakértője a témának és tényleg örülök, hogy válaszolsz :))



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2011.10.13. 17:33:49**

Hali!

Hát ezt lehet, hogy inkább találos kérdés, vagy valami nyereményjáték keretében kellett volna inkább, de mindegy, ha már így szóba került:-)

a NOD egy mozaik szó, szlovákul annyit jelent: Kórház a Merevlemez Szélén, még a fejlesztés kezdetén az ott ismert és kedvelt tv sorozat apropója adta a progí nevét.

mateo4 2011.10.16. 13:06:08

Helló!

Köszí, nem gondoltam volna, hogy a NOD32 egy mozaikszó. :-)

Még egy pár kérdés:

A 30 napos próbaverzió ideje akkor is fogy, ha nem használod a gépet?

Az ESET egy szlovák cég?



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2011.10.17. 14:23:12

Nem közeli rokonod véletlenül Columbo hadnagy?

Szerintem ha van még további kérdésed, lőj közvetlenül egy mailt nekem, vagy az info KUKAC sicontact PONT hu címre, és bizony mondom, válaszoltatik néked :-)))

Hacktivity 7DB part one

2011.09.20. 13:00 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [hacktivity konferencia millenáris 2011](#)

"Gyerekként azt hisszük, hogy felnőttként már sebezhetetlenek leszünk. De a felnőttség a sebezhetőség elfogadása." **Hacktivity 2011.** beszámoló első rész, első nap délelőtt.



Új helyszínen, a korábbi Dürer kertenél nem kicsit tágasabb helyen, a **Millenárison gyűlt össze a hétvégén** az IT biztonsággal kedvtelésből és hivatásszerűen foglalkozók népes csoportja. Kellemes, tágas, világos, még befértek volna ennél is többen.



A menetrend elég feszített volt, **sok előadás, rövid szünetekkel, sok érdekesség, workshopok**, így aztán volt mivel zsibbasztani az agyakat estére, bár [pihenésképpen például lehetett zárat lockpickelni, ami egy igazi felüdülés.](#)



A korai kezdési időpont sokaknak magasra tette a léceket, overclockolni kellett a kávégépeket, de ennek ellenére - **kissé ijesztő módon** ☐ ☐ ☐ **ezáltal szinte időben kezdődött el az esemény.** A rengeteg illusztris vendég mellett [maga Szomory Dezső is idelátogatott, hátha készségesen megadhatja valamilyen kérdőíven a nevét, lakcímét](#), telefon-, adó-, TB- valamint bankkártya számát PIN kóddal, továbbá a kutya oltási bizonyítványának számát is, ha már, akkor.



A megnyitó után [elsőként Ször Péter állt a dobogóra ezáltal McAfee színeken](#), és természetesen **a vírsokról beszélt.** **2 éves ez a probléma**, többek közt szóba került Hypponen idei pakisztáni látogatása a Brain-t író testvérpárnál, akik [még nevüket és lakcímüket is beleírták annak idején a vírusba](#) és azóta is ugyanott laknak, vezetik a számítógépes boltjukat.



A kártevők száma azóta persze jócskán megnőtt, itt már **egy 70 milliós szám** hangzott el, és persze a korai DOS és Windows fájlokhoz képest már szinte mindenütt jelen vannak, legyen az Windows, Mac, PDF, weboldal, java, bármi. ☐ **iemelte még a rootkites kártevők jelentős veszélyét**, melyekre nyilván az [Intel-McAfee féle Deepsafe](#) is megpróbál majd egyfajta választ adni. Készült egy [külön interjú is Péterrel, amely a Biztonságportálon](#) olvasható.

Ezek után aztán kettévált az előadások szála, az egykori Ganz Villamossági Művek **földszintjén található Pipacs terem** volt az egyik **helyszín, míg az emeleti kisebb Silent terem** a másik, ez utóbbiban kizárólag fejhallgatóval lehetett hallgatni a műsort - innen a név. Sok esetben lehetett tűnődni, hogy húú, most melyik termet válasszam, mert éppen mind a kettő izgalmas lesz, de persze meg is nyugodhatunk, hiszen **mindenről készült videó, szóval lehet pótolni majd az elmulasztott dolgokat**. A tavalyi [2010-es Hacktivity felvételeit pedig itt lehet](#) nézegetni.



Mi ezúttal **Illési Csolt igazságügyi szakértő előadását** néztük meg, ahol különböző jogágak hozzáállásának különbözőségeit vette górcső alá, egyik szemléletes példája éppen **az O. J. Simpson ügy és annak bizonyítékai** voltak. Az emlegetett Simpson ügy ambivalens megítélését jól jellemzi, hogy míg az első büntetőjogi ügyből a **különbő bizonyítékok megkérdőjelezésével, illetve ezek kizárásával** ugyan felmentették, ám később a második polgári peres eljárásban aztán már mégis bűnösnek találták.



Szóba került még, hogy miként kell dolgoznia egy informatikai igazságügyi szakértőnek, **feladata kizárólag a feltett kérdésekre való válaszolás**, és persze ezzel kapcsolatban a szakértővel szembeni esetleges aggály- illetve panaszlehetőségek is terítékre kerültek. Amihez az adott szakértő nem ért, nem illetékes és/vagy nem kérdezték meg tőle, arra elvileg nem válaszolhatna, de **ezeknek a kérdéseknek a kezelése, szabályozása azóta sem kiforrott még teljességgel**.

[Joe McCray érdekes figura volt, lazán kezelte a dolgokat](#), és a szervezők figyelmes odaadását dicséri, hogy mindössze egy slide lapozás után már egy pohár rummal kedveskedtek neki azután, hogy elárulta, mi is a kedvenc itala. **Előadásának szövegvét csak 1-as karikával ajánlják, melynek témája a mobil eszközök pentesztje volt**. Erre nem léteznek még olyan kiforrott módszerek, mint például a PC-k vagy a webalkalmazások esetében.



Manuális módszerek - például iPhone esetében eleve egy jailbreakelt készülék - **no meg virtuális környezetek segíthetik itt a munkát, a nyilvánosságra kerülő sebezhetőségek hivatalos javítása pedig szintén a PC-s világhoz viszonyítva lényegesen lassabb**, körülményesebb, időnként pedig semmilyen. Ám rések és támadások itt is vannak bőven, emiatt aztán ez láthatóan egy folyamatosan és egyre gyorsabban fejlődő terület lesz. Jó lett volna, ha az elméleti áttekintés mellett sikerült volna egy kicsit gyakorlatiasabb részekbe is belefolytani.

Szinte **törzsvendékként köszönthettük Alexander Kornbrüst Racle szakértőt**, aki a délelőtti utolsó előadója volt az ebédszünet előtt. A Red-Database-Security cég alapítója ezúttal arról beszélt, hogy alapos ismeretek birtokában hogyan nyerheti ki egy támadó a jelszavakat. **Az Racle hackelésnek már komoly szakirodalma van**, még az Amazonon is találhatunk könyveket a témáról. Forensics vizsgálatok esetében pedig hasznos módszer, ha időrendi sorrendben szemléljük a log és audit táblák adatait, különös tekintettel **olyan fontos változókra, mint az lcount, melynek értéke jelszavas próbálkozásra**, túl magas (például több tízezres) értéke pedig brute force kísérletre utalhat.





Olyan példát is láthattunk, hogy a jelszavak látszólagos felüldefiníálása (update password set password='mukinyul';commit;) után **hogyan találhatjuk meg mégis az adatbázisban a korábbi eredeti jelszót, sőt akár ezek összes előző változatát**, szóval az előadás színvonala ezúttal sem okozott csalódást.



A mellékelt fotók minőségéért itt kérünk elnézést, kéne már egy komolyabb fényképezőgép, de a jelenlegi öskövílet egyrészt primán kitart [a nagy Tervezett Elavulás összeesküvés](#) dacára, másrészt már több **konóbeli elvesztést is tapasztalt, megtalálták, visszahozták, szeretjük**. Ezenkívül elmondhatjuk, hogy **legalább ezren jöttek el a mostani rendezvényre, és beszámolóikkal nemzetközi szinten is öregbítették a Hacktivity hírnevét a nagyvilágban, még Kínában és Albániában is ismernek** minket. Azt azonban **már az eddigiekből is primán láthatjuk, hogy 10 féle ember van: aki ismeri a bináris számrendszert, és aki nem**.

 Tetszik  7 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kinszenvedés](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3240331>

☐ **ommentek:**

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 7DB part two

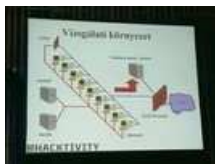
2011.09.21. 10:30 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [hacktivity konferencia millenáris 2011](#)

"Az ember vagy előidézi, vagy megoldja a problémát, különben csak szimpla tereptárgy." **Hacktivity 2011. beszámoló második rész, első nap délután.**



Új helyszínen, a korábbi Dürer kertenél nem kicsit tágasabb helyen, a Millenárison gyűlt össze a hétvégén az IT biztonsággal kedvtelésből és hivatásszerűen foglalkozók népes csoportja. Lássuk mi történt az első nap délutánján. A Silent teremben kezdtük a délutáni sessiont, ahol [Dr Leitold Ferenc és Horváth Botond vázolt fel egy ütőképes koncepciót](#) arra a problémára, hogy lehetne hasonló, sőt egyenesen hajszálpontosan egyforma internetes állapotoknak megfelelő környezetben vizsgálni a különböző antivírus termékeket. A problémát ugyebár az okozza ([mint az közismert](#)), hogy egy adott pillanatban egy weboldalon tapasztalható helyzet - például megpróbál letöltődni valami a gépünkre - **pár perc múlva megváltozhat, eltűnhetnek állományok, vagy akár OS és böngészőkörnyezettől függően különböző válaszokat kaphatunk, illetve egyes esetekben azonos IP cím mellett már sosem kapjuk újra ugyanazt a választ, mint először** - nagyjából végtelen a lehetősége az eseteknek. Viszont ha két vagy több vírusirtót összehasonlítunk, **azonos akciókra történő reakciókat akarunk látni**, hogy értékelhessünk.



Erre lehet megoldás az **úgynevezett Malware Proxy**, melynek segítségével lehetséges eltárolni egy webhely pillanatnyi állapotát, mint egy lenyomatot, és innentől kezdve már egy állandó helyzettel nézhetnek szembe a vírusvédelmek, összehasonlíthatóak lesznek a kártékony környezetre adott válaszaik alapján. A történelmi áttekintésből egyébként az is kiderült, hogy a víruskorszak hajnalához képest (DOS, Win3.1, párezer vírusnak csak a felismerése, negyedéves gyakoriságú adatbázis frissítések floppyn vagy BBS-en) az AV programok összehasonlítása, **tesztelése a könnyűtől az elképesztő bonyolultságú nehézig változott.**

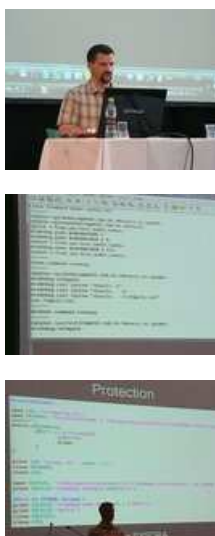
A következő előadást [Ertunga Arsal tartotta, aki az SAP biztonságáról](#) mondott pár keresetlen szót. Ez nagyjából azt jelentette, hogy az SAP biztonsági helyzetét mindenki jónak gondolja, amíg meg nem ismeri azt közelebbről. Ugye itt **csupa nagy értékű szoftverről, még még nagyobb értékű cégszekrekről** beszélünk.





Ertunga a terület szakértőjeként már számos SAP biztonsági hibát jelentett, mostani előadásában ebben a témakörben nálunk talán először demonstrált sebezhetőségeket, példát is mutatott az ABAP Injectionre, beszélt adatbázis rootkitektről, konfigurációs gyengeségekről, és mindenfajta SAP támadási lehetőségről, védekezésről. Tipikusan az az előadás volt, amit érdemes lesz majd videóról újra megnézni.

Az [Oracle témában Tóth László](#) neve mindenkinek ismerős lehet, ő következett ezután szokásos, magabiztos élő demojával.



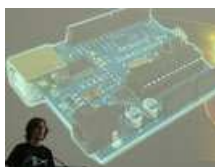
Például a "nem dokumentált" **oradebug parancs** használatával látványosan tudta manipulálni a rendszert, így bizonyítva, hogy az eredetileg hiba felderítő eszköz kreatív és avatott kezekben hacker eszközként is eredményesen vizsgálható.

Az adatbázisok manipulálása után egy kis lazítás következett, kávé, Redbull, és a már **előzőekben emlegetett lockpicking workshop**. Volt itt minden, mi szem-szájnak ingere: postaláda zár, ajtó zár, kínai, olasz és hottentotta lakat, **lehetett próbálkozni a roncsolásmentes kulcsnélküli zárnyitással**.



Fortélyokat és hogyanokat pedig a konferencián előadást is tartó [témagazdáktól, Subecz Ákostól és Zánthó Csabától](#) lehetett ellesni.

Ha esetleg valahol a neten olyan Hacktivity beszámoló jelenik meg, amelyben Georgi Geshev zseniális budapesti előadásáról áradoznak, akkor biztosak lehetünk benne, hogy annak írója nem járt itt személyesen, mert ez a bemutató betegség miatt elmaradt. Így [Veres-Szentkirályi András](#) **következtetett, aki az Arduinóról** tartott élvezetes kiselőadást. Ha röviden össze akarjuk foglalni, mi is az az Arduino, akkor érdemes a Wikipedias leírást elővenni: "Az Arduino interaktív tárgyak készítésére használható, számtalan kapcsolót vagy szenzort bemenetként olvasva, lámpák, motorok és egyéb kimenetek kimeríthetetlen választékát képes vezérelni. **Az áramkör házilag is nagyon könnyen összeállítható, vagy készen megvásárolható; a nyílt forráskódú fejlesztőkörnyezet pedig szabadon letölthető.**" Magyarán [olcsón és könnyen tudunk valamilyen hardveres vezérlést](#) összerakni.



A felsorolt és meg is valósított példák közt láthattuk a HackerSpace "Is there anybody in there" projektjét, valamint az ugyancsak helyütt megvalósított automata virágöntöző rendszert is, amellyel sikeresen igazolta az előadás szlogenjét: "Hacking for Fun". Kedvesinálónak pedig a HackerSpace workshopba invitálta a nagyérdeműt egy kis Weller pákás forrasztásra, amivel bárki megvalósíthatta hasonló álmait és titkos vágyait.

Az ezután következő [Felix Schuster nagyon is élő problémát hozott elő. A fél világ Skype-ot használ](#) a kommunikációhoz, hiszen ez a legismertebb és legszélesebb körben használt ingyenes szolgáltatás hang és video beszélgetéshez az interneten keresztül. Ám egyeseknek fájdalmasan hiányzik ebből egy titkosítási lehetőség. Ezt igyekezett megoldani, és létrehozott egy biztonságos és lehallgatás-biztos Skype hálózaton keresztüli kiegészítést.



A megvalósításnál igyekezett betartani a Skype felhasználói szerződésben foglaltakat (no reverse engineering, blabla), és egy kiegészítő kriptográfiai réteggel oldotta meg a problémát, amelynek demózása közben még a barátai "éles" felhívás próbáját is sikerrel kiállta.



Az előadás után meglestük az Arduionós hardverhackelő csapatot, majd a délután utolsó eseményeként [Léderer Sándor, Földes Ádám, Csörgő László és Bodoky Tamás elemezte ki egy szögletes formájú kerekasztal mellett](#) a Wikileaks-szel kapcsolatos eseményeket, próbálták értékelni, mennyire volt sikeres ez a projekt Assange személye miatt, és mi lesz nélküle.



Szóba kerültek a **hasonló magyar oldalak is (k-monitor.hu, atlatszo.hu)** és ennek kapcsán **etikai kérdések is felmerültek**, aminek kapcsán jól látszott, hogy a közérdek, és a közérdek tájékoztatni akarása szerencsére erősen motiválja a résztvevőket.



A zajos tetszésnyilvánítástól sem mindig tartózkodó nagyérdemű elégedetten vehette tudomásul, hogy **nincs Hacktivity party fejenpörgés nélkül**, és lassan már a Balabites pálinka is az esti program nélkülözhetetlen alapfelszereltségei közé nőtte ki magát. Lehetett hát építeni a kapcsolatokat, lazítani, tágítani a látókört, kötetlenül beszélgetni, sőt később egyes eltévelyedettek még aludni menni sem restelltek. Végül lepihentek az egyesek és a nullák, velük alszik a zümmögés, hogy másnap reggel hajnali 9-kor majd újult erővel folytatódjon a Hacktivity a második nappal.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- ["Szösölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3241810>

Kommentek:

□incsenek hozzászólások.

Hacktivity 7DB part three

2011.09.22. 10:40 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

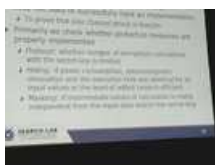
Címkék: [hacktivity konferencia](#) [millenáris 2011](#)

"A világnak több szerény zsenire lenne szüksége. Olyan kevesen maradtunk." **Hacktivity 2011. beszámoló harmadik rész, második nap délelőtt.**



Új helyszínen, a korábbi Dürer kertnél nem kicsit tágasabb helyen, a Millenáris gyűlt össze a hétvégén az IT biztonsággal kedvtelésből és hivatásszerűen foglalkozók népes csoportja. Lássuk mi történt a második nap délelőttjén. Itt előbb [érdeemes idézni egy másik beszámolót](#): "A második nap **kissé csendesebben indult, többen még az előző napi kapcsolatépítést pihenték ki.**"

Ennek tükrében kicsit valóban kisebb létszámban ugyan, de elindult a második nap is, és rögtön megint egy nehéz döntéssel: "Paulik Tamás: Ki lakik a routeremben? A beágyazott eszközök botnetbe szervezésének kivitelezhetőségéről" vagy pedig "[Hornák Zoltán: Crypto-chipek biztonsága – passzív-aktív kombinált támadások](#)". Mi ez utóbbit választottuk a Silent teremben, és egy igen alapos és érdekes előadást láthattunk a szintén törzsvendégnek számító és kissé megfázott Hornák Zoltántól.



Olyan profi trükkök kerültek itt ismertetésre, mint **például az áramfelvételi görbéből meg tudni a titkos kulcsot**. Ennek megfelelően az ilyen titkosító chipek gyártóinak is fel van adva a lecke: olyan módon kell megírniuk az algoritmusukat, hogy a hőfejlődés vagy a sugárzás figyelésével, a végrehajtási idők mérésével ne lehessen megfejteni a crypto-chipekre bízott titkokat. A **passzív-aktív kombinált támadási módszerek (magyarul csak PACA :-)** segítségével, például hiba injektálási módszerekkel - azonban mégis sikeresen lehetett támadni ezeket a folyamatokat.

A következőkben aztán a nagyon várt, és [rettentően profi előadónak bizonyult Raoul Chiesa kiberbiztonsági szakértő](#) lépett a porondra, és igen szemléletesen, szórakoztatón mutatta be, milyen gyengeségek jellemzik az egyes kormányzatokat, milyen incidensek történtek a közelmúltban, amik a kiberhadviselés megjelenésével és mostantól folyamatos jelenlétével befolyásolhatják a történelem menetét. Az olyan kiberfenyegetéseket, mint amit például Észak-Korea szokott hangoztatni, nem minősítette súlyosnak, lévén hogy szerinte az ottani internetes infrastruktúra rendkívül fejletlen.

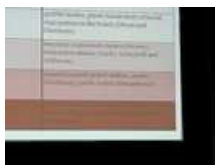




Érdekes színfolt volt az előadásnak az a része, amikor szakértőként **a csíkos nadrágos, sok csillagos tábornokokkal kellett megértetni, milyen megjelenési formái lehetnek a kiberhadviselésnek, végül a hagyományos haditechnikai eszközökkel való párhuzam segítette elérni az Aha-élményt.** Külön [kitért dicsérőleg a korábbi hasonló témájú Kovács László-Krasznay Csaba: Digitális Mohács](#) című előadásra. Az idő rövideje miatt a most már nagy létszámú közönség még megszavazott neki egy tíz perces plusz időtartamot, így szerencsére végignézhettük a teljes prezentációt Stuxnetestül, mindenestül.



A social engineering témakörnek ugrottunk neki ezután, itt [először Bodor Péter vállalkozott arra, hogy a pszichológia és a social engenering fogalmát](#) szakmailag tisztába tegye.



Kicsit nehezen indult a dolog, az első harmada nagyon elvi és teoretikus volt, de szerencsére **később sok konkrét példával, korábbi vizsgálati eredményekkel illusztrálva tudott izgalmas és újszerű dolgokat mutatni**, és a végére már kifejezetten érdekes volt. Izgalmas lenne mindenesetre egyszer egy ilyen pszichológus szakemberrel azt is meghallgatni, milyen szakmai elemzést adna például egy Kevin Mitnickről.

Az elvek után aztán belecsaptunk a gyakorlat lecsójába, mert [Oroszi Eszter nem csupán felolvasta előadását, hanem ahhoz megfelelő praktikus előkészületeket](#) is végzett. Nem volt rest, és meghackelte a Hacktivity, **parókát és kontaklencsét öltött, és a hostesslányok viseletét imitálva, egy Postitből készített hevenyészett "karszalaggal" simán bejutott az eseményre**, ahol aztán tovább kísérletezgetett a jelenlevőkön.





Egyrészt **szétszórt pár** ☐ **SB kulcsot, amin kémprogram volt**, aztán máskor kérdőívekre igyekezett személyes adatokat megszerezni, volt nyeremény játék, ahol egy idegen USB kulcsot kellett/kellett volna a delikvensnek a saját gépébe bedugni (ne mááár, elnézést, de ez itt végtére is egy hacker konferencia, vagy mi). **A szervezők javára írható, hogy az első nap végére a hostessek főnöke sikeresen lefűlelte a kéretlen extra munkaerőt**, aki addigra már a hostessek által kezelt belépő karszalagokat is sikeresen megdézsmálta. Az akció értékelésénél elhangzott, **a résztvevők döntő többsége megfelelően biztonság tudatos volt**, ennek ellenére így is volt pár óvatlan, aki megadta/bedugta/engedte bedugni/bediktálta és hasonló.



Ezzel aztán le is zárult a délelőtt, amelyen természetesen az [ilyenkor elmaradhatatlan](#) ☐ [argame](#) is helyet kapott. Nemsokára a negyedik, befejező résszel jelentkeztünk, már laboráljuk hozzá a fotókat, nagyítás Krokussal, előhívás, fixir és öblítő fürdő - izé ja nem is, hiszen digitális. Ne menjenek sehova, mindjárt kezdünk.



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [A kiknek a Captcha kinszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3241827>

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 7DB part four

2011.09.23. 11:11 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hacktivity konferencia millenáris 2011](#)

"Nem lehet megoldani problémákat ugyanazzal a gondolkodásmóddal, amivel csináltuk őket." **Hacktivity 2011. beszámoló negyedik befejező rész, második nap délután.**



Új helyszínen, a korábbi Dürer kertnél nem kicsit tágasabb helyen, a Millenárison gyűlt össze a hétvégén az IT biztonsággal kedvtelésből és hivatásszerűen foglalkozók népes csoportja. Lássuk mi történt a második nap délutánján. **A délutáni forgatagban [az ESET robotja lendületesen és fáradhatatlanul karatélyozta az ellent](#)** a TV fal monitorain, mi pedig kávézni indultunk, majd a Pipacs terem felé vettük az irányt, ahol **[Balázs Zoltán tartott előadást az IPv6 és a Teredo szerverekkel kapcsolatos](#)** sebezhetőségről.



A lépésről lépésre megvalósított támadás segítségével **előbb local, majd domain adminná lehetett válni**, és igen meglepő volt az a tény is, hogy az IPv6-ot engedélyező gépek elleni támadási lehetőség **már 2001 óta ismert**. A kísérlethez kitűzött célt, miszerint egy Backtracket (alapértelmezett jelszóval) is futtató gépről korábbi pentest dokumentumokat próbál megszerezni, sikeresen abszolválta, ja és Shakespeare rulez!

Utána az emeleten gyülekeztek azok, akik **[Yaniv Miron izraeli kutató előadását](#)** akarták meghallgatni. A jelenleg Dániában élő informatikai biztonsági tanácsadó **a SCADA (Supervisory Control And Data Acquisition) rendszerekről szólva elmondta, sirnivalóan könnyű** ezeket meghekkelni, eredendően gyengék a protokolljaik és sok esetben a telepítéskor is figyelmetlenül járnak el, tovább rontva ezzel a biztonsági helyzetet. De egyúttal rusztikusan üzent is innen annak a betörőnek (szóba hozva annak jó édes anyai ági felmenőjét), aki néhány nappal ezelőtt lakásából kizárólag ezt az előadását tartalmazó CD lemezt és laptopot vitte el.





Saját fejlesztésű DISMAL programjával képes a SCADA eszközök lebénítására, elérve ezzel, hogy az adott egység kizárólag tőle fogadjon utasításokat. A látványos akciót - természetesen az utána következő eredeti állapot visszaállítással együtt - demonstrálta, és elmesélte, **sok esetben a "komoly gond van a biztonsággal"** megállapításnál sokkal hatásosabb érv, ha mindezt így be is mutatja és megérteti az üzemeltetőkkel, mekkora is a veszély.

Itt lehetett volna megintcsak menni a folytatásra egy workshop keretében, mi ezúttal azonban a szélesebb spektrum jegyében a földszintre mentünk, ahol [Michele Orru behatolástesztelő szakember a BeEF, vagyis a Browser Exploitation Framework](#) nevű játékszer segítségével végrehajtott támadási lehetőségeket ismertetett tökéletesen érthető, de fülnek kellemes olaszos angolsággal.



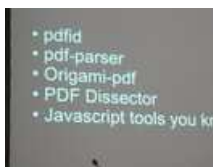
A lehetőségek sajnos szemléltatást zavarbaejtően szélesek, egyszerűen beinjektálható például olyan IFRAME elem, amivel aztán egy JavaScriptben futó keylogger működik. Magáról a [BeEF projektről itt lehet](#) bővebb információkat találni.

A következőkben a szintén veterán [Major Marcell és Zágon Mihály előadása kezdődött, amelyben a webes támadások újdonságait](#) igyekeztek összefoglalni, illetve ezeket bemutatni.



Szóba kerültek a HTML5 kihasználható gyengeségei, de ami nekem talán a legjobban tetszett, az egy **olyan támadási lehetőség volt, amikor egy preparált, rosszindulatú PNG fájl segítségével a böngésző kliens megjelenítéskor rávehető az ebben beágyazott kód azonnali végrehajtására**. Izgalmas volt az is, hogy a WebGL javascript segítségével biztosítja a grafikus hardverre való közvetlen rajzolást és az úgynevezett "shader" kód futtatását magán a GPU-n. Emellett a különböző böngészőkben megvalósított (vagy a Firefox esetében meg nem valósított) **Sandbox megoldásokat is összehasonlították** megemlítve azt az állítólagos lehetőséget, hogy **egy kód a virtualizált homokozó környezetből ki tudjon lépni** - ezt szintén állítólag a Vupen sikeresen megoldotta.

Utolsó körben aztán a [malware analízálás rejtelseiről hallhattuk Kabai András](#)t, aki a végrehajtható EXE fájlok IDA, virtuális környezet és egyéb módszerekkel, segédeszközökkel való elemzését, Processmonitoros és Captureclient segítségével végzett megfigyeléséhez igyekezett kedvet csinálni.



Szóba kerültek természetesen a JavaScriptes kártevők is, ezek **kódösszezavarási kísérleteinek elhárításához is adott tippeket**, mutatott be segédeszközöket vagy programozási trükköket. Értelemszerűen a JavaScriptes támadások nem csupán önmagukban, hanem **PDF állományokba ágyazva is megjelenhetnek, ezért a Portable Document Format típusú fájlok vizsgálata, fejlécük elemzése, a beágyazott elemek visszafejtése is szükséges lehet** a fertőzések elkerülése érdekében. Kihangsúlyozta, a malwarek visszafejtése igen érdekes és tanulságos, nem utolsósorban hasznos ténykedés, ezért minden jelenlevőnek jó szívvel ajánlja a szabad idő hasznos eltöltésének ilyenét formáját.



Szépségében egy remek konferenciát zártunk, kicsit érni kell még a népítéletnek, mit lehetne vagy kellene esetleg másképp. Egy irdatlan gigászi Wall of Sheep is üzemelhetne folyamatosan mindkét napon látástól Mikulásig. Na jó, legyen ez egy pár csillaggal könnyített kijelzéssel lightosan megvalósítva, de aztán amit semmilyen nagyhatalmú sündisznócska panaszkodására sem kapcsoltnak le. Szívesen látnánk több vendéget a környező országok hackerközösségeiből, és egyetlen nagy közös büfés, étkezős, beszélgetős helyszín is talán szerencsésebb a sok kisebb szétszórva található ilyen helyett, de hangsúlyozzuk, **a rendezvény nagyon rendben volt, laza és jó hangulatú, valszeg megyünk jövőre is.**



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az IP él, az IP élt, az IP élni fog](#)
- [Mi a közös bennük? Tőjai, Chrome, kormányzat](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback?id=5>

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 vezet az Autorun vírus

2011.09.26. 11:15 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [adatok](#) [nod32](#) [eset](#) [havi](#) [threatsense](#) [vírusstatisztika](#)

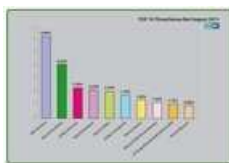
Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit.



Maradt az élboly, az első és második helyezett megőrizte előző havi pozícióját, és az Autorun immár ötödik hónapja áll vezető helyen. Feltétlenül említést érdemel a negyedik helyezett Win32/Dorkbot féreg, amely cserélhető adathordozók segítségével terjed, és tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvethető az irányítás a fertőzött számítógép felett.



A szokásos kémkedő, hátsóajtót nyitó kártevők mellett ebben a hónapban egy igazi adatromboló vírus is jelen van, ez pedig a hetedik helyen található Win32/Autoit féreg, amely 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 feregnek sikerül megfertőznie a rendszert, akkor az összes lokális és hálózati meghajtón megkeresi a futtatható állományokat, és kicseréli őket saját magára.



Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2011. augusztusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 23.89%-áért.



1. INF/Autorun vírus

Elterjedtsége az augusztusi fertőzések között: 6.40%

Előző havi helyezés: 1.

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 az augusztusi fertőzések között: 4.22%

Előző havi helyezés: 2.

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 eljárásán 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/Iframe.B.Gen vírus

Elterjedtsége az augusztusi fertőzések között: 2.38%

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.



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

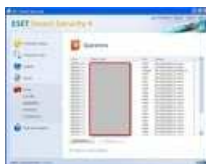


4. Win32/Dorkbot féreg

Elterjedtsége az augusztusi fertőzések között: 2.22%

Előző havi helyezés: 7

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>



5. Win32/Sality vírus

Elterjedtsége az augusztusi fertőzések között: 2.10%

Előző havi helyezés: 3

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



6. HTML/ScrInject.B trójai

Elterjedtsége az augusztusi fertőzések között: 1.79%

Előző havi helyezés: 6.

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/scriinject-b-gen>



7. Win32/Autoit féreg

Elterjedtsége az augusztusi fertőzések között: 1.45%

Előző havi helyezés: 8.

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>



8. Win32/PSW.OnLineGames trójai

Elterjedtsége az augusztusi fertőzések között: 1.23%

Előző havi helyezés: 4.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományait és működését a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatok titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



9. JS/TrojanDownloader.Iframe.NKE trójai

Elterjedtsége az augusztusi fertőzések között: 1.12%

Előző havi helyezés: -

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 az augusztusi fertőzések között: 0.98

Előző havi helyezés: 41

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. 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>



6 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3255734>

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](#).



TrueY • <http://qltura.blog.hu> 2011.09.26. 14:30:27

Nem értem! W7 már nem engedi az autorun-t. Linux-ban meg sosem volt.

Tessen letiltani az XP-ken az autorun-t és passz...

Még nyílnak a völgyben

2011.09.29. 14:40 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [flash](#) [macintosh](#) [adobe](#) [pdf](#) [trójai](#) [kártévő](#) [dyaoyu](#)

Illetve pontosabban a böngészőkben a kéretlen ablakok. Kártevő valóban nincs túl sok, de azért folyamatosan **vannak kisebb trójai próbálkozások Mac vonalon** is, folyik tesztelés, a [korábbi hamis antivírus próbálkozások után](#) most két újabb kísérletről is hírt kaptunk alig egy hét leforgása alatt.



Az egyik esetben egy [hamis Adobe Flash frissítéssel próbálkoztak a trójai terjesztők](#) arra alapozva, hogy nyilván a korábbi [kritikus hibát befolytató új verziót már mindenki nagyon](#) várta. A social engineeringet sem nélkülöző trükk netezés közben **feldob egy ablakot, hogy hoppáré, frissíteni kéne az Adobe Flash-t: "Welcome to the Flash Player Installer"**, és ne várjunk egy percet sem. Mire a felhasználók szokásos pavlovi x százaléka kattint, amire malware települ, ami pedig aztán **személyes adatokat igyekszik kikélni**, majd szanzsén egy távoli szerverre próbál meg továbbítani.



A másik trükk pedig **PDF állományokban terjed**, és erről mindenkinek eszébe juthat a jó öreg, Magyarországon is világhírű Windows módszer: érkezik egy pdf.exe egy Portable Document Format állománytípusra jellemző ikonnal, és már mozognak is a mutatóujjak. Most a Mac esetén jön, kapjuk, ölünkbe hullik [egy sebezhetőséget kihasználó preparált PDF, ami egy valódi kínai nyelvű dokumentum képében jelentkezett](#), és az élet nagy kérdései közül arra keresi a választ: **"Do the Diaoyu Islands belong to Japan?"** magyarul vajon a Diaoyu szigetek Japánhoz tartoznak-e perpillanat vagy sem. A megnyitott PDF belseje azonban egy rosszindulatú kódot is tartalmaz, amely **lefutva hátsóajtót telepít** a fertőzött számítógépre.



Mellesleg mivel a fentemlített Dyaoyu szigetekeken gyaníthatóan bőséges az olaj, valamint a földgázkészlet, továbbá köztudottan egyúttal gazdag halászerületről is van szó, így **ez a kérdés már 1895 óta élénk vita tárgya Kína és Japán közt**, és ha korábban még nem is, de a jövőben elképzelhető, emiatt **több ilyen kártékony PDF hadoszlopot küldenek majd csatába egymásnak ;-)**



Amit valóban érdemes lehet az ilyenek ellen tenni, **figyelni a becsapós trükkökre**, Adobe frissítést csak **őstermelőtől az Adobe lapjáról** letölteni, **kikapcsolni a Safari-ban az "Open safe files after downloading" opciót** (helyette Firefoxot futtatni NoScript-tel hehe :-), és/vagy a gépen **valamilyen biztonsági (antivírus) csomagot használni**, ami **rögtön beszél** az ilyenekre. Nem fogunk meglepődni, ha az ilyen "igazinak látszó" Adobe Flash mellett a korábbi [hamis videók, kodekek módszere is ismét újjáéled](#), és különféle trendi új, például Scarlett Johansson nude video! és hasonló neven feltámad majd hamvaiból.

OS: Platform: Statistics									
Statistics of each platform: 1 day (last 24 hours) (last 24 hours) (last 24 hours)									
Statistics of each platform: 1 day (last 24 hours) (last 24 hours) (last 24 hours)									
Platform	OS	Version	Platform	OS	Version	Platform	OS	Version	Platform
Windows	Windows	Windows	Windows	Windows	Windows	Windows	Windows	Windows	Windows
Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X
Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux
Android	Android	Android	Android	Android	Android	Android	Android	Android	Android
iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone
BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry
Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian
Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone
Android	Android	Android	Android	Android	Android	Android	Android	Android	Android
Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X	Mac OS X
Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux
Android	Android	Android	Android	Android	Android	Android	Android	Android	Android
iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone	iPhone
BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry	BlackBerry
Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian	Symbian
Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone	Windows Phone

A főbb mértékre is már többször kitértünk, ezért jó esetben csak ismételni tudjuk önmagunkat. Aki a PC-hez képest szoroktőrt vesz számítógépet, **annak országtól függetlenül a banki accountja is vélhetően vastagabb, vonzóbb lehet a bűnözők számára**. Valamint [szépen lassan \(slowly and surely\) emelkedik a Mac OS X tortaszelete](#), és gyanítható, **ha ez majd elér egyfajta kritikus limitet** (amiről persze nem tudjuk pontosan mennyi, lehet 10, 15 vagy akár 30% is), és megéri majd ide is kódolni, akkor a kártevő fejlesztő csapat főnöke

egyszer csak azt fogja mondani: *"Figyel ide nekem most Vaszilij, Csing-Li-Kung és Szergej fiam. Ma utan nem eddig mint csak néha, hanem csinál mindig összes kártevő, támadás bele oda neki Mac úgyszintén, és jönni sok pénz. És most kérem én vodkámát!"*

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  1 Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3264652>

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.

Sok kárt okoznak a vírusok

2011.10.03. 11:45 | [Csizmazia István \[Rambo\]](#) | [1 komment](#)

Címkék: [felmérés](#) [kár](#) [support](#) [újratelepítés](#) [vírusok](#)

A magyar internethasználók **felének kellett már újratelepítenie számítógépét vírusfertőzés miatt**, egynegyedük pedig adatokat is veszített el az internetes kártevőknek köszönhetően. Célszerű megoldás lenne, ha olyan vírusirtót használnánk, amihez valódi terméktámogatás jár, azonban a legtöbben sajnálják erre a pénzt.



Az ESET Magyarország és az NRC közös felmérése szerint csaknem kétmillió magyar internethasználónak kellett már legalább egy alkalommal újratelepítenie számítógépét vírus vagy más kártékony program miatt. A legkevésbé a 18-29 éves korosztály törődik a biztonsággal, **a fiatal felhasználók 63%-a telepítette már újra operációs rendszerét vírusfertőzés miatt, és 26%-uk veszített el adatokat.**



A vírusvédelmi rendszereket gyártó ESET szakértője a felmérés eredményei kapcsán arra hívja fel a figyelmet, hogy **nem létezik olyan tökéletes vírusirtó szoftver, ami minden egyes kártevőt biztosan felismer**, éppen ezért fontos, hogy olyan termékre bizzuk gépünk védelmét, melyhez **teljes körű terméktámogatás** jár.



„A vírusirtó cégnek képesnek kell lennie arra, hogy **az esetleges fertőzések 99%-a esetén speciális eszközökkel felderítse és hatástalanítsa a károkozókat, majd adatvesztés nélkül megtisztítsa a számítógépeket**” – emeli ki **Béres Péter**, az ESET vezető IT tanácsadója. A biztonsági szoftverekhez járó terméktámogatás azonban hazánkban még nem megszokott, több gyártó csak e-mailes szupportot biztosít, az ingyenes vírusirtókhoz pedig sokszor nem jár még ez sem. Mindez a magyar felhasználók jelentős részét azonban nem zavarja, ők inkább újratelepítik a gépeiket, és nem törődnek a családi fotók vagy a levelezés elvesztésével.



Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3273982>

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 2011.10.09. 23:10:07

A botnetek és a backdoorok miatt még mindig az újratelepítés adja a legbiztosabb módját a kártevők eltávolításának.
Ha már bejutott valaki a gépre, ott bármit csinálhatott - akár olyan, egyedi programot is telepíthetett, amit egyszerűen semmi nem ismer fel.

Kártékony tartalmak szűrése a Facebook-on

2011.10.05. 11:00 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [privacy facebook megosztás kártékony websense linkszűrés](#)

A Facebook megerősítette a hírt, miszerint megállapodott a Websense céggel, hogy a jövőben a linkeket valós időben fogják átvizsgálni az úgynevezett ThreatSeeker Cloud felhőalapú megoldásával.



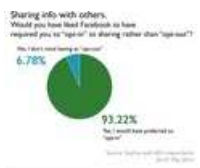
Ez a szűrési folyamat nagyjából úgy képzelhető el, hogy [gyanús vagy kártékony linkek esetében kapunk egy felugró ablakot, miszerint a meglátogatni kívánt URL nem megbízható](#), ezért válasszunk: [visszalépünk az előző oldalra](#), saját felelősségünkre mégis meglátogatjuk a kétes oldalt, vagy bővebb információt szeretnénk kérni az URL-lel kapcsolatban, pontosan miért lett megbízhatatlannak nyilvánítva. Ennek oka lehet vírus fertőzés, adathalász oldal, kártékony vagy trójai program, de lehet kártékony tartalom is, mint például rasszista megnyilvánulások, szélsőséges durvaság, stb.



Az üzemeltetők bíznak a rendszer sikerében, amely annyiban [különbözik a Google linkellenőrzési rendszerétől](#), hogy nem fehér és feketelistákra támaszkodik, hanem valós időben ellenőriz. A Facebookon korábban bevezetett WoT (Web of Trust) szisztéma [ezzel párhuzamosan továbbra is változatlanul megmarad](#).



Összességében elmondhatjuk, jó és rossz történik egyszerre, hiszen ez a szűrés dolog mindenképpen egy áldásos pozitívumnak tekinthető, **nem is értjük, miért nem már korábban vezették be**. Hogy [Atko kolléga idevágó zseniális örökbecsű kommentjét](#) idézzük: "Az uszodában ki van írva: 'mély víz csak úszóknak!' és mellette van úszómester is! Egy közösségi oldal meg olyan, mintha hivatalosan engedélyeznék a strandolást a Niagarában. Aztán ha valaki hamis mentőövvel vagy lyukas csónakkal kereskedik, vonogatják a vállukat és a fürdőzőkre mutogatnak."



Ám az ismét megváltozott kinézet és [minden eddiginél szélesebb körű alapértelmezett megosztási mánia](#) meg egy jókora negatívumnak tűnik, nem is beszélve azokról, [amiket még nem vezettek be, de már tervezik](#). **Szinte a száználmas.hu-ra kívánczok, hogy 600 millió embernek kell egyesével kézzel ilyen idézeteket kiteszegetni esdeklően az üzenőfalára**, ahelyett ahogy maga a nagy Facebook üzemeltetői jobban figyelembe vennék a default megosztásoknál a plebejusok adatvédelmi szempontjait. Sajnos egyáltalán nem látszik közeledni [a sokak által hön áhított cél, az alapértelmezett opt-in](#). Adios privacy!



10 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3279660>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói tartalomnak minősülnek, értük a [szolgáltatás technikái](#) 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>
[2011.10.05. 11:18:31](#)**

Na, szokásomtól eltérően elsőzők is rögtön :-D

Hogy a mai Blikkből idézzünk: "Jorge Csisztu dollármilliomos Beninben, egy afrikai országban tüdőrákban elhalálozott, aki aranykereskedő volt, és nem csekély, 10,5 millió dolláros (vagyis közel 2,5 milliárd forintos) örökséget hagyott a legközelebbi hozzátartozójára" - szólt a Facebook üzenet. Veterán antivirus.blog olvasóknak erre még az arcizma se rezzen (Winettou rulez :-)

Ám a folytatás - ha valóban igaz a dolog - már sokkal lesújtóbb a realitásérzékre nézve: "...folytatta a Csisztu, aki végül 2500 dollárt (vagyis 573 ezer forintot) küldött az ügyvédnek."

Részletek alant:

www.blikk.hu/blikk_aktualis/internetes-csalok-verték-at-csisztut-2066701

650%-kal több kormányzati incidens az USA-ban

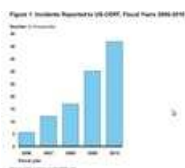
2011.10.07. 10:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [kormányzat usa](#) [incidens](#) [cert](#) [informatikai](#)

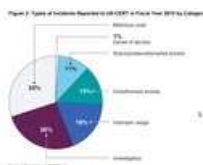
Az Egyesült Államok kormánya szerint öt év alatt emelkedett ilyen szintre a kibertámadások és biztonsági incidensek száma.



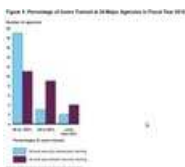
Ismerve a vírusok (vagy inkább számítógépes kártevők) számában évek alatt bekövetkezett meredek evolúciót - amelyre mostanában a 70+ milliós számot szokták használni - aztán a [kínai eredetűnek tartott sorozatos kémprogramos eseteket](#), meg figyelembe véve az ottani törvény által előírt bejelentési kötelezettséget, **a szám abszolút hihehetőnek tűnik, sőt igazság szerint szinte még alacsonynak is látszik.** Nyilván [kiemelt erőfeszítések történnek egy ilyen kulcsterület védelme](#) érdekében, ám a támadások, [az információk jogosulatlan kifürkészése érdekében meg még kiemeltebb :-\)](#) erőfeszítésekről beszélhetünk.



Egy most napvilágot látott [49 oldalas GAO \(Government Accountability Office\) jelentés](#) szerint **a jellemző esetek a jogosulatlan hozzáférés megszerzésétől kezdve a túlterheléses támadásokon át a hozzáférés megszerzésének kísérlete mellett a kártékony kódok felfedezéséig terjednek**, melyeket az US-CERT felé jelentettek, illetve ott vizsgálták ki azokat.



A számszerűsített kimutásból az is kiderül, hogy **a táplálkozási lánc csúcsán a számítógépes kártevők állnak a legnagyobb 30%-os tortaszelettel, de a jogosulatlan hozzáférések mellett olvasható 14% is elég nagy szám ahhoz, hogy sok helyen nyugtalanul érezzék magukat.**



A rendellenes tevékenységek összefoglalója az okok keresése során arra is kitér, hogy **a szakmailag indokolt és kötelezően előírt biztonsági intézkedéseket nem minden esetben tartották be**, és nyilván ez a körülmény is hozzájárulhatott némiképp az incidensek számának növekedéséhez. A szervezet **fokozott biztonsági erőfeszítések megtételét, rendszeres tanfolyamokat és felkészítéseket** lát szükségesnek ahhoz, hogy az ismertetett különféle kormányzati IT gyengepontok a jövőben megszüntetésre kerülhessenek.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/3284454

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.

Antivírusok VS kormányzati trójai

2011.10.10. 15:45 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [r2d2 trójai](#) [ccc](#)

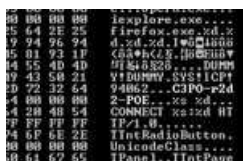
Ez a hétvége sem telt el eseménytelenül, ezúttal a CCC (Chaos Computer Club) publikálta az elemzését arról a megszerzett trójai kártevőről, amelyet állítólag a német kormányzat használ állampolgárai számítógépes forgalmának megfigyelésére.



Az [eredeti CCC elemzés](#) itt található, [Buherátor posztja](#) az eseményekről itt olvasható, továbbá [Mikko Hypponen](#) ugyancsak érdekes írása pedig emitt lelhető fel. Ezek alapján annyit tudunk, **ez egy kémkedő trójai, amely teljes hozzáférést ad a megfertőzött gépekhez, segítségével minden billentyűzeteleítés rögzíthető és elküldhető egy távoli szerverre, de a Skype beszélgetések mentése és képernyőképek menetközbeni készítése is lehetséges általa.**



Ha mindez még nem lenne elég, a CCC elemzése szerint még arra is nyílik lehetőség, hogy az adott számítógép mikrofonját, illetve kameráját távolról bekapcsolva rögzítsenek hangot, videót a felhasználó környezetéből. Bár a C&C szerverek címeit sikerült megtalálni, **sokra mégsem lehet vele menni**, mert a rejtőzködés érdekében ezek egy USA-ban található adatközponti szerverre vannak irányítva, így az alapos vizsgálat, a tulajdonosok adatainak egyszerű kinyerése, vagy egyáltalán bármiféle bizonyítás bírói végzés nélkül meglehetősen nehézkes lehet.



A dolog egyes helyeken máris komoly hisztériát okozott, talán abból kiindulva, ami az F-Secure weboldalán megjelent: *"We have never before analysed a sample that has been suspected to be governmental backdoor. We have also never been asked by any government to avoid detecting their backdoors."* Mostanra már sorra születnek az esetről az egyre újabb cikkek, noha a kormányzatiságot, ha valóban van, egyelőre egyáltalán nem sikerült (és talán nem is lehetséges) bizonyítani.



A hangzatos és bulvárszagú "Can you trust your antivirus solution to protect you against governmental backdoors and 'lawful interception' police Trojans?" kérdések például [arra próbálják meg kihegyezni a kérdést](#), hogy egyes amerikai vírusgyártók állítólag szemet hunynának a kormányzati kártevők esetében.



Ha megnézzük a valóságot, akkor ezzel szemben az látható, nem igazán tapasztalható ilyen félrenézés az észlelésekben, legyen az Avira Antivir, McAfee vagy Norton.



A VirusTotal találatokat vizsgálva jól láthatóan nincsenek erre utaló különbségek, inkább azt látjuk, hogy **lassan minden vendor felébred és gyorsan beresze az adatbázisba a detektálást**, [ezek száma például már a vasárnapi naphoz képest is gyarapodott](#) 17-ről 24-re a 43-ból.



4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

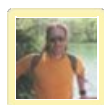
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Ez történik a weben egy perc alatt](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3291699>

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>
2011.10.10. 20:19:06**

Informatív kérdések a megfelelő helyen rovatunkban:

A Titkosügynök-e Ön? kérdésre adandó helyes válaszok:

"Nem, de ha az lennék is ugyanezt kéne válaszoljam."

Ennek fényében: "German officials deny use of Trojan horse program"

www.usatoday.com/tech/news/story/2011-10-10/germany-cyberattack/50718986/1



**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
2011.10.11. 08:04:50**

Egy kis adalék még Remote Forensics Tool tárgykörben, köszü Hypponen:

t.co/ZdON3bmv



Csizmazia István [Rambo] • <http://antivirus.blog.hu>

2011.10.12. 09:18:05

Azt hiszem, erre a bejelentésre vártunk:

"Winfried Seibert, a társaság ügyvédje hétfőn még csak azt jelentette be, hogy vizsgálják az ügyet, mert a cég készített egyes német hatóságoknak lehallgatószoftvert, abban viszont nem teljesen biztosak, hogy az ő termékük jutott a Chaos Computer Club kezébe. Kedden azonban már biztosan állította a cég, hogy a bajor hatóságok által alkalmazott szoftver tőlük származik, és azt még 2007-ben adták el a bajor rendőrségnek. Seibert azt is közölte, hogy hasonló alkalmazásokat holland, osztrák és svájci hatóságok is vásároltak a DigiTasktól."

www.origo.hu/techbazis/szamitogep/20111011-feltuningolhattak-kemprogramjukat-a-nemet-rendorok.html

Lassan jönnek az Androidos kártevők

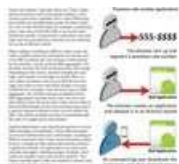
2011.10.12. 13:30 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [trójai android kártevő](#)

Amikor egy platform elterjedtsége eléri egy limitet, széleskörben használják azt és széles körben hozzáférhető a dokumentációja, valamint a bűnözőknek anyagilag is kezd megérni a ráfordított munka, onnantól megugrik az erre a rendszerre készített kártevők száma.



A Symantec [nemrégiben kiadott technikai white paper doksija](#) szerint lassan eljőhet ez a bizonyos határ. Korábban itt a blogon is hírt adtunk már [kémprogramoktól hemzsegő kínai, igaz nem hivatalos Android Marketről](#), valódi Android [Marketen talált kártékony programokról](#), valamint [Androidos botnetről](#), sőt ez a platform sem kerülte el versenytársai sorsát, mikor [a felhasználók GPS adatait kellett titokban lenaplóznia](#).



A mostani cikk igyekszik bemutatni a főbb támadási vektorokat, az összefoglaló szerint sokféle módszer kezd népszerű lenni, kezdve az olyan **klasszikus, emelt díjas hívásokat vagy kémprogramot rejtve tartalmazó kártékony alkalmazásokkal**. Nem csak a készülékek, és az okostelefon használók száma **emelkedik, de annak a bizalmas, személyes, értékes adatmennyiségnek a mértéke is**, amely komolyan inspirálhatja a bűnözőket, különösen pedig **majd akkor, ha a mobil, mint fizetési eszköz később valóban elterjed**.



A felhasználóknak már most is érdemes lehet átgondolni a honnan telepíték, mit telepíték, és mit engedélyezek annak az új alkalmazásnak kezdetű kérdéseket. [Előbb vagy utóbb pedig egy megbízható vírusvédelmi programon](#) is elkezdhetnek gondolkodni. Ha egyszer beindul majd a kártevőáradat, [várhatóan a hamis antivírusok készítői is hálás terepre fognak](#) majd itt találni.



Egyelőre azonban úgy látszik, egyesével lövik fel a különböző támadásokat, kísérleteznek, és valószínűleg eddig nem érhette meg nekik a ráfordítás, talán emiatt aztán egyik támadás sem ismétlődött meg később, illetve folytatódott. Ehhez persze az is hozzátartozik, hogy az ilyen korábban említett emeltdíjas móka elég országspecifikus, és sok dolog korlátozza az ezzel összeszedhető pénzeszköz nagyságát.



Ha azonban **sikerül majd valóban nagyszámú fertőzést megvalósítani, úgy a bevétel / fertőzés arány miatt a jövőben meredeken emelkedhet** az Androidos kártevők száma, és akkor már nem csak külön műkedvelők fognak ilyet a garázsban farigcsálni, hanem a gépműhely csarnokok futószalagjain is beindul majd az ipari méretű termelés. [Ez persze nem egy Windowsos nagyságrendű tömeges áradat lesz, de azért elindulhat valami](#). Egy biztos, [az Android platform sikeressége](#) nem fog ennek a folyamatnak az útjában állni.



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.





Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Ez történik a weben egy perc alatt](#)
- ["Szósölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3297152>

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.

Hatodik hónapja vezet az Autorun vírus

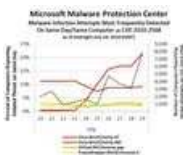
2011.10.14. 09:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

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.



Továbbra is érintetlen az élboly: első az Autorun vírus és második a Conficker féreg. Ebben a hónapban mindössze minimális mozgást lehetett észlelni, tulajdonképpen a lista tagjai nem is változtak meg az előző hónaphoz viszonyítva, inkább csak egyfajta helycsere, átrendeződés történt. Ha a változásokat megnézzük, egyből két helyet is előrelépett a Win32/Ramnit fájlfertőző vírus, amely a HTM illetve HTML fájlokba 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. Míg az előző hónapban a negyvenegyedik helyről lépett a tizedikre, ebben a hónapban ezúttal nyolcadik lett.



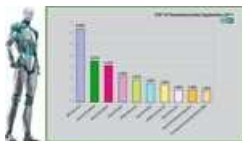
Hasonlóan előre felé araszolt - igaz csak egyet - a Win32/Autoit féreg, amely cserélhető adathordozók segítségével terjed, de olyan variánsa is van, amelyik az MSN üzeneteket használja fel a fertőzés terjesztésére. Súlyos adatvesztést is okozhat, ugyanis ha a féregnek sikerül megfertőznie a rendszert, akkor az összes lokális és hálózati meghajtón megkeresi a futtatható állományokat, és kicseréli őket saját magára. E havi teljesítménye a hatodik helyhez volt elég.



Emiatt az ESET e havi hónapzáró jó tanácsai között kiemelten hangsúlyozza az adatmentés fontosságát, amelyet minden, de különösen az otthoni felhasználóknak érdemes megfigyelni. Míg általában céges környezetben ez jellemzően megoldott valamiféle rendszeres külső adathordozóra vagy felhőbe mentés formájában, addig a magánszemélyek legtöbbször kényelemszeretetből, lustaságból vagy spórolásból elhanyagolják azt, és enyhébb-súlyosabb adatvesztéseket szenvednek el.



Ugyancsak érdekes, hogy Win32/PSW.OnLineGames trójai mennyire állandó szereplője a toplistáknak. A lassan három éve, 2008. december óta jelenlevő Win32/PSW.OnLineGames olyan programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. A kártevőcsalád tevékenysége jellemzően az online játékok jelszavainak begyűjtésére, és a jelszó adatok titokban történő továbbküldésére koncentrálódik. Szeptember havi adatokat összesítő toplistánkon most a kilencedik helyet sikerült megszereznie.



Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2011. szeptemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 24.02%-áért.



1. INF/Autorun vírus

Elterjedtsége a szeptemberi fertőzések között: 6.49%

Előző havi helyezés: 1.

Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozók. 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 szeptemberi fertőzések között: 3.65%

Előző havi helyezés: 2.

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 eljárásán 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>

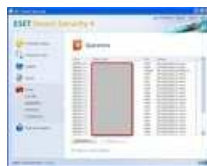


3. Win32/Dorkbot féreg

Elterjedtsége a szeptemberi fertőzések között: 3.23%

Előző havi helyezés: 4

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>



4. Win32/Sality vírus

Elterjedtsége a szeptemberi fertőzések között: 2.29%

Előző havi helyezés: 5

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.



□ővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus_sality_aa_sality_am_sality_ah



5. HTML/Iframe.B.Gen vírus

Elterjedtsége a szeptemberi fertőzések között: 1.97%

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>



6. Win32/Autoit féreg

Elterjedtsége a szeptemberi fertőzések között: 1.65%

Előző havi helyezés: 7

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. HTML/ScrInject.B trójai

Elterjedtsége a szeptemberi fertőzések között: 1.56%

Előző havi helyezés: 6.

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 kísér meg letölteni.



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



8. Win32/Ramnit vírus

Elterjedtsége a szeptemberi fertőzések között: 1.09

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.



□ővebb információ: <http://www.eset.eu/encyclopaedia/win32-ramnit-a-backdoor-ircnite-bwy-w32?lng=en>



9. Win32/PSW.OnLineGames trójai

Elterjedtsége a szeptemberi fertőzések között: 1.09%

Előző havi helyezés: 8.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományait és működését a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatokat titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



10. JS/TrojanDownloader.Iframe.NKE trójai

Elterjedtsége a szeptemberi fertőzések között: 1.00%

Előző havi helyezés: 9

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>



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



• [1 trackback](#)



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés [trackback](#) címe:

<http://antivirus.blog.hu/api/trackback/id/3300658>

Trackbackek, pingbackek:

[Trackback: Könyökléssel a vírusok ellen](#) 2011.10.15. 12:23:33

A Stanford egyetem tudósai szerint ideje felhagyni a kézfogás idejétmúlt, ámde annál károsabb szokásával. Ehelyett sokkal jobb lenne egymást könyökkel üdvözölni, ezáltal jelentősen csökkenthetjük a különböző kórokozók, mint például a rettegett influenz...

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.

Feltört postafiók, észrevétel: nem vette észre

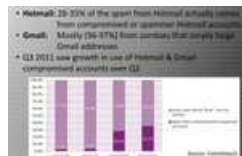
2011.10.17. 15:00 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [felmérés](#) [figyelmetlenség](#) [levelezés](#) [feltörés](#)

Kicsit a régi rendőrviccre hasonlít, ahol az illetőnek a tetőről a fejére esett egy tégl, és a hatósági közeg általi papíralapú jegyzőkönyv kitöltése történik. Eset:? tégl. Neme:? de igen. Észrevétel:? nem vette észre. **Egy most napvilágot látott jelentés szerint a felhasználók tömegei sem veszik észre, ha a levelezési postafiókjukat feltörik.**



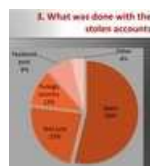
A Commtouch által jegyzett ["State of hacked account" beszélő nevű kutatásból](#) az derül ki, a levelezési feltörést elszenvedett felhasználók 62 százaléka nem is volt a tudatában, hogy egyáltalán veszélybe kerülhet, ahogy azzal sem voltak tisztában, hogy belépési accountjuk hogyan kompromittálódhatott. A megkérdezett felhasználóknak **csak mintegy harmada vette észre magától**, hogy valamilyen rendellenes dolog történt, míg [azok, akiknek úgy szólt barátjuk, vagy ismerősük, hogy "hahó, úgy látszik feltörték postafiókodat", ők 50%-nál is magasabb arányban voltak](#). 15% nyilatkozott úgy, hogy a saját szolgáltatója figyelmeztette a bibire.



Pedig a kutatási eredmények arra is rámutattak, [minden nyolcadik feltörési esetben a támadók megkíséreltek hamis üzeneteket eljuttatni az áldozat ismerőseinek, pénzt kérve tőlük állítólagos külföldi baleset, útlevél elvesztés](#), és hasonló ürügyeket felhasználva. A felmérés **igazolja azt a vélekedést is**, miszerint a támadók egyre célzottabban használják fel a birtokukba jutott eléréseket, mind jobban testreszabják a spamjeiket.



[Az elkövetőkre nézve nincs nagy elrettentő erő, hacsak](#) a keresztnévünk nem Sarah, és egyúttal a vezetéknévünk ráadásul nem Palin, mert [akkor és csak akkor az ilyen gaz postafiók feltörést elkövető illető kiemelten súlyos büntetést](#) kaphat, **egyébként azonban a nem Sarahk esetében történt incidenseknél nagy valószínűséggel az égegyadta világon nem történik semmi**: a felfedezésig az elkövetők tolják ki csövön a nevünkben ész nélkül a reklám spamet, az adathalász leveleket, bármit.



A **"Ha már megtörtént a baj, mit tehetünk kérdésre"** [egyszer már megírtuk a részletekbe menő frappáns választ, így azt most csak belinkeljük](#), itt szépen rendezetten pontokba szedve szerepelnek az okosságok.



A hogyan lehet védekezni már érdekesebb kérdés, nos például a Gmail esetében egy kellemes ficsör, hogy **az utolsó bejelentkező IP címe megőrzésre kerül, így tulajdonképpen elmondható, hogy nehezebb is a bejutás, és hogy hamarabb is észlelhető**. Nyilván [sokat nyom a latban a "megfelelő" jelszó](#), amiről most nem értekezünk hosszasan, csak két kulcselemet emelünk ki a tálból: egyedi, máshol nem használt és erős, vagyis hosszú és vegyesen tartalmaz kis- és nagybetűt, számot, és egyéb furmányos írásjeleket. **Ha netalántán erős elkeseredettségünkben politikusi karriert tervezünk**, úgy lehetőség szerint óvakodjunk a gov.palin@yahoo.com mintájú, esetleg ugyanennek a Freemailes vagy Citromailes változatának használatától.



A rendszeres jelszócsere meg a https alap, aztán lehet gondolkodni még, hogy **lehetőleg semmilyen weboldalon ne használjuk a "maradjak belépve" opciót**. Érdemes hanyagolni az olyan Facebook linkek látogatását, mint az unalomig elcsépett "Hey dude, check this out!!!!!!", vagy "Thought you might like this!!", emellett soha senkinek ne küldjük el a jelszavunkat, bármilyen hivatalosnak látszó kérés is érkezzon erre.



Továbbá ahol van lehetőség a szimpla név-jelszó azonosításon felül telefonos SMS azonosításra is - például a Gmail is már ilyen - ott éljünk ezzel, és használjuk ki az ilyen plusz extra biztonságot nyújtó lehetőségeket.



8 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártyák böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/3309355>

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.

You have 1 lost message on Facebook

2011.10.19. 15:45 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [lost facebook](#) [email](#) [gyógyszerész](#) [message](#) [recover](#)

Egyre emelkedik a közösségi hálókkal kapcsolatos károkozás, ami lehet csalás, kártevők küldése, fertőzött linkek terjesztése, adathalászat, kémprogram, jelszólopás vagy személyiséglopás.



Egy négyszáz kanadai IT szakember megkérdezésére épült felmérés válaszdóí szerint **egy cég életében egyre inkább komoly fenyegetést jelentenek ezek a közösségi elemek. 70 százalékuk ugyan veszélyforrásnak tartja a közösségi hálók használatát**, ám 31% úgy gondolja, a megfelelő és betartott biztonsági szabályozások mellett ezek kivédhetők. A kártevő terjesztők már évek óta rájöttek, hogy adatlopó kódjaik legjobb helye **a közösségi oldalakra beírt üzenetek, kommentek, posztok linkjeiben vannak, ez az üzletág jól teljesít: 800 milliónak a csalásnak bedőlő 5%-a is elképesztően nagy szám**: 40 millió, vagy ahogy John Rambo mondaná: sok katonából sok halott is lesz. Emiatt aztán - [az idei évre vonatkozó tavaly évvégi jóslatoknak](#) maximálisan megfelelően - **51%-kal növekedtek a közösségi médiákkal kapcsolatos támadások**.



Abban a megkérdezettek többsége is egyetértett, múlhatatlanul szükséges, hogy a cégek kezeljék ezt a helyzetet. Ami lehet vírusvédelmi megoldás a végpontokon (79%) vagy javítható a webes forgalom teljes szűrésével (79%), ellenőrzésével, de emellett szükséges lehet a személyazonosság és jogosultság kezelés (76%) megfelelő megvalósítása is, a jó öreg social engineering módszerek elleni oktatással kiegészítve persze. **Amikor azonban munkahelyeket kérdeznak meg arról, van-e nekik olyan cég policy, amely a Facebook, Twitter és egyéb közösségi hálókkal kapcsolatos használatot szabályozza, erről rendelkezik, úgy meglepő módon a vállalatok több, mint egyharmada (36%) egyáltalán nem rendelkezik ilyesmivel.**



Zárásképpen egy mai "hivatalos Facebook" üzenetet mutatunk, ami "Amerikából jött", mesterségének címerével kapcsolatban nem nyilatkozunk. **Szerintük van egy elszalasztott Facebook üzenetünk, amiről kérhetetlen nyílt proletár őszinteséggel be is számolnak** a mellékelt kéretlen emailben csak most, csak nekünk, és egyből megoldást is kínálnak: ímhol végrehajthatunk egy recover folyamatot, amivel visszaszerezhetjük az elvesztettnek hitt báránykát, csak kattintsunk és máris.



A levél kinézete ugyan hú de hivatalos, meg kiköpött Palo Altoi, de ha a szokásos adathalász gyanakvást elővesszük, és [mindössze a link fölé mozgatjuk az egeret, egyből kiderül](#), annak már csak annyi köze van egy hivatalos Facebook üzenethez, [mint Luciano Pavarottinak Fásy Zsülikéhez](#).



A levél minden egyes hivatkozási eleme: a recover, a FAQ, és az "unsubscribe" is egyazon francia URL-re mutat, szóval még arra sem vették a fáradságot, hogy legalább valami mellégépet Fecabook.com vagy hasonló elvarázsolt domain névvel növeljék az esélyeiket. Ami egyben azt is bizonyítja, valószínűleg nincs is szükség rá, enélkül is meg lehet nekik a betevő kattintási ráta.



A kapott link egyébként nem a végállomás, az abban elhelyezett script rögtön átló minket a következő helyszínre, ahol [mosolygós fehérköpenyes bácsik és nénik](#) szolgálják fel nekünk készségesen a kedvező árfekvésű akciók Viagrát.



15 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3314357>

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.

Webkamerás kukkolók III.

2011.10.21. 14:45 | [Csizmazia István \[Rambo\]](#) | [42 komment](#)

Címkék: [flash](#) [hiba](#) [webkamera](#) [macintosh](#) [adobe](#) [mikrofon](#) [kémkedés](#) [player](#) [webkamerás](#) [kukkolók](#)

Az Adobe Flash Player hibáját kihasználva olyan weboldalt lehet létrehozni, amely titokban bekapcsolja a látogatók mikrofonját és webkameráját.



Éppen egy éve történt Philadelphiában, hogy kiderült, [az iskola titokban otthonukban is megfigyelte a diákokat](#) a webkamerás számítógép segítségével. A leleplezés után egy ideig még ugyan tagadtak, de [végül kártérítést fizettek](#) a diákokról illegálisan készült 56000 (!) fotó miatt. Mai hírünk pedig, hogy **az Adobe Flash Player hibáját kihasználva** nagyjából ugyanezt megteheti bárki, vagyis a sebezhetőség a Mac gépeken lehetővé teszi, hogy [támadók rejtve bekapcsolják és kémkedjenek a webkamera és a mikrofon segítségével](#). Az Adobe közben már bejelentette, készül és [hamarosan megjelenik a javító patch](#).



"Egy mester? Tíz mester? Száz mester? Házmester? Nem. Ezeremester tanfolyam nyílik, jelentkezzi!" Ez állt egy cetlin a faliújságon még az általános iskolában, és büszkén jelenthetem, én jelentkeztem. Ami remélhetőleg nem múlt el nyomtalanul, szabadidőmben pedig Öveges professzort néztem a fekete-fehér tévén.



Így hát következzen az általam közkedvelt;-) **időszakos Barkács Pajtás rovat, melynek mostani epizódjában bemutatunk egy egyszerű fapados, de hatékony módszert, amivel filléres költséggel beinthatunk** a zaklató munkaadónak, az ipari kémnek, az iskolai rendszergazdának, önjelölt [iskolai kiberzaklatónak \(cyberbullying\)](#) vagy az állami [R2D2 Nagy Testvérenek](#) - legalábbis ami az [otthonunkban zajló kéretlen hang és fotó/videó felvételt](#) illeti. A szükséges kellékek: egy ötcentis szigetelőszalag darab, és egy szimpla 3.5-es jackdugó, ami akár egy rossz fülesről is levágható.



A kamera úgy működik, hogy kigyullad mellette - elvileg ugye - a piros led, amikor aktiválva lett. Azt már az Élet sokszorosan bebizonyította, érdemes Murphy szerint gondolkodni, miszerint: **"Bízz embertársaiddban, de azért emeld meg a kártyapaklit!"** Nos, a **mellékelt módszerrel fizikailag érhetünk el 100%-os biztos eredményt hang és kép ügyben**. A darab szigetelőszalagot - persze legyen ez inkább ízléses fekete, mi pusztán az illusztráció kedvéért választottuk a ronda zöld-sárgát - ahogy a boldog békeidőkben az autópályamatricát, felragasztás előtt párszor simítsunk a farmerünk térdéhez, így könnyebben lejön, ha kell, és nem hagy annyi ragasztófoltot sem. A kamerás részt letakarva ezek után semmilyen alkalmazás nem fog kéretlen képet, videofelvételt készíteni, ha pedig mégis használni akarjuk, akkor könnyen le lehet venni.



A levágott jackdugó mehet a mikrofonbemenetbe, ennek persze csak és kizárólag akkor van hatása meg értelme, ha van beépített mikrofon is, amit a dugó felülbírálna egy új bemeneti eszközzel, ami ugye itt a csupasz drótnál nincsen.



Végezetül a hétvége előtt [ritka, de jó szokásunk szerint egy kis színes, de teljesen ontópik olvasnivalót ajánlunk, kedvenc Szentmihályi Szabó Péterünktől](#), még kedvencebb "101 mini sci-fi" című kötetéből, amely **bár számos olvasónk születése előtt, még a múlt századi 1988-ban jelent meg, sok jövőbe látó, érdekes gondolatot (pl. Huawei, szabadalmi pereskedések, túl kitérülő Facebook, stb.) találunk benne.** Copyleft by innen, köszönettel, idézet ON:

"Kémtelevízió

A Nikai cég reklámáron dobta piacra 2011-ben az új háromdimenziós tévéjét, alig harminc rublárért. A Nikai tri-di olyan olcsó volt, hogy az irigységtől sárga versenytársak eldobható tévének csúfolták, és a dömpingár miatt különböző pereket indítottak a Nikai ellen. De egyetlen pert sem vesztett a Nikai, sőt büszkén vállalta az eldobhatóságot, mert a Nikai tri-dit nem lehetett szétszedni, s így javítani sem, viszont ha két éven belül elromlott, a vevő ingyen kapott egy újat. Harminc rublárért a bolondnak is megérte ez a vásár. Három éven belül a Nikai letarolta a piacot, csak a nagyon gazdagok és a nagyon szegények ragaszkodtak a hagyományos készülékekhez.

A Nikai cég pedig folyvást gyarapodott, és kiterjesztette birodalmát a hírközlésre és a magas politikára is. A legtöbb hírügynökség és újság Nikai-érdekltség lett tíz éven belül, és mindenki csak sejteni vélte, hogy a Világállam helyi kormányai csak addig nem buknak meg, amíg szabad utat engednek a Nikai cégnek.

Akik pedig valamilyen módon megpróbálták fellépni a cég ellen, kellemetlen helyzetbe kerültek előbb-utóbb. Olyan csinos botrányba keveredtek, magánéletük olyan kinos epizódjai láttak napvilágot, hogy szűkülve kértek bocsánatot a cégtől, és vonultak vissza, minél messzebb az emberek tekintetétől.

Ám egy túl kíváncsi tévészerelő mégis szétszedte az eldobható Nikai tri-dit, és megdöbbenve tapasztalta, hogy a képernyő mögött egy parányi videokamera van elhelyezve, mely pontosan közvetíti a képernyő előtt ülők minden szavát és mozdulatát. Egy független tridi állomás világgá röptette a hirt, és a Nikai konszern hiába tagadott és zsarolt körömszakadtáig, minden kiderült. A Nikai cég olcsó készülékei univerzális, bármikor bekapcsolható családi kémekként működtek, s milliárdokat érő információkat nyújtottak..."



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3319658>

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](#).

winston01 2011.10.21. 16:20:53

Hm, nem rossz, csak hogy a valóságban a "kíváncsi tévészerelő" már a bemutató példányt szétszedi.

[lifelike 2011.10.21. 1□:□1:55](#)

ip címem honnan fogja tudni?



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu> 2011.10.21. 16:43:57](#)

Szia Winston01!

Hát ugye ez már egy 23 éves sci-fi, manapság már egy Gizmodo a megjelenés napján szétkapja.

De ha mondjuk egy UPC boxot nézel, ami nem a te tulajdonod, az már érdekesebb, különösen ha majd egyszer bevezetik vele a TV/PC politikai távvezérlést.

[Madarsky 2011.10.21. 16:45:10](#)

@lifelike: nem kell tudnia. Egy weboldalt lehet létrehozni, amin van egy vicces flash alkalmazás. Amikor elmész a weboldalra, te magad kapcsolod be a kamerát és a mikrofont, amivel aztán a weboldal ki tudja micsinál. Nem csak úgy lövöldöznek ezzel valakik vaktában, hanem csinálnak egy csapdát az arra járóknak.

[Madarsky 2011.10.21. 16:46:28](#)

@Madarsky: mármint úgy értem hogy azzal kapcsolod be, hogy elmész arra az oldalra, hogy megnyitod a weboldalt.

[Laciii 2011.10.21. 17:12:17](#)

Azért remélem raktál oda egy kis papírfecnit ahol a kamera van és nem ragasztóztad össze.

[Laciii 2011.10.21. 17:14:45](#)

@lifelike:

Onnan, hogy az iskola honlapjára rakják a flasht ahova belépsz szépen a kedves neveddel ügyintézni.

[ezanevemeskesz 2011.10.21. 17:59:35](#)

zseniális, a kamerát már azóta leragasztottam, amióta megvan a laptop, ez nagyjából 3,4 év

[eax_ 2011.10.21. 18:01:58](#)

"A levágott jackdugó mehet a mikrofonbemenetbe"

Ez nem feltétlenül elég.

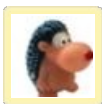


[cso zsi • <http://www.ingyen-jatekok.com/> <http://www.demonoid.me/> 2011.10.21. 19:48:14](#)

@Csizmazia István [Rambo]: Manapság? Apám 30-40 éve minden egyes új rádió és magnó hazahozatalakor megkért, hogy legalább egy hétig ne babráljam a belsejét. Pedig tényleg csak érdeklődési szint volt, látni kellett, "mi nyávog a macskában". A dörzs, és szíjhajtásokról sokmindent megtanultam azokból.

Nem volt bennük kamera. :)))

És évekig működtek az összerakás után is.



dr. phil. ün ツ <http://sunews.blog.com> **2011.10.21. 20:24:52**

A kamerát úgy is ki lehet kapcsolni, ha kivágod az ablakon.
A mikrofont vízzel öntözve elvileg örökre elnémul.
Ha kib@szod a laptopot a susnyásba, akkor az ip-címedet se tudják meg soha!



ColT • <http://kilatasgaleria.blog.hu/> **2011.10.21. 20:27:08**

Fájdalmasan egyszerű, grat :D
Amúgy asztali gépnél meg kihúzd/elfordítod a webkamerát.

klarky • <http://kreport.blog.hu/> **2011.10.21. 20:49:33**

Ezt 2x is elolvastam, mert nem hittem el. Te komolyan posztot írtál abból, hogy kell letakarni a kamerát? Az index meg komolyan kirakta címlapra?

Az eszem áll meg... Még hogy piros led villan fel... Ki kell ábrándítsalak, az én gépemen semmi nem villog, ha megy a kamera. Leragasztani? Minek? Veszél egy darab papírt, ketté hajtod és ráarakod. Ha meg nem kell a takarás, leveszed...

Aki ezt magától nem tudja, azt a nettől is el kell tiltani, sőt, gondnokság alá kell helyezni. Én mióta az eszem tudom letakarom a kamerát, jóval az előtt is ezt tettem, h ez a vírus kiderült.

Paranoia? Lehet, de a hírek szerint nem volt alaptalan...



TrueY • <http://qltura.blog.hu> **2011.10.21. 20:52:21**

@cs0 zsi: :) Jaja! A Matáv is akkor követte el a legnagyobb hibát, amikor a Schönherz koleszbe felszerelte az első kártyás telefonokat. Hetekig laptop-okkal ültek előtte a tanulni vágyó villamosmérnök palánták.

Szentpétervárott le is szerelték őket, mert szinte senki sem telefonált bolti kártyával.

Seravy **2011.10.21. 21:41:01**

Nekem se kamerám, se mikorofonom. 100% biztonságos megoldás kémkedők ellen.

hungi. **2011.10.21. 22:49:33**

Szövegértelmezés látom nem megy sokaknak:

" Mai hírünk pedig, hogy az Adobe Flash Player hibáját kihasználva nagyjából ugyanezt megteheti bárki, vagyis a sebezhetőség a Mac gépeken lehetővé teszi, hogy támadók rejtve bekapcsolják és kémkedjenek a webkamera és a mikrofon segítségével."

Megnézem kinek van MacOSx-es gépe otthon...

lifelike: ha már fut az a flash, haza tud telefonálni az adataiddal (meg persze a videóstream-eddel is).

Peetee **2011.10.21. 23:28:13**

Nincs webkamerám, ilyen egyszerű!
Egyébként meg nézhetnek, pulcsiban ülök a gép előtt, henete 5*2órát...szevasz.



Androsz **2011.10.22. 00:43:15**

Szentmihályi Szabó Pétertől 1983-ban jelent meg A tökéletes változat című kisregény (Kozmosz Fantasztikus Könyvek), amely több Világmodellt is vázol, a távoli jövőben élő radikális gondolkodó elméleteiként. Van ezek között olyan, amelyet ma olvasva alig értjük, hogy a mester ezt már akkor hogyan láthatta előre. Mivel ma nyakig benne vagyunk abban a modellben,

amely akkor a szocialista Magyarországon teljesen ismeretlen volt. Ma nem látszik a dolog nagy felfedezésnek, de a leírás 28 évvel ezelőtről származik. Most is érdemes lenne kérni tőle egy előrejelzést a húsz évvel ezutánra.



bunkó • <http://bunko.blog.hu> 2011.10.22. 00:45:57

Ha belegondolok, hogy mennyit kerestem havarnak (politikus) mire olyan laptopot tudtam venni neki, amelyben se kamera se mikrofon nincs beleépítve - adtam hozzá webkamerát, ha akarja, bedugja.

...mondjuk fogadni mernék, hogy nem azt használja többit, hanem az államtól ingyen kapott, beépített mikrofonos-kamerást...



bunkó • <http://bunko.blog.hu> 2011.10.22. 00:53:39

@big-boss: "Megnézem kinek van MacOSx-es gépe otthon..."

Ez a mostani cikk a Mac-es hibáról szól.

Windows alatt ugyanilyen flash kémkedési lehetőséget kb a tavalyi hírek között olvashatsz.

...meg a következő években még néhányszor, mivel maga a flash úgy ahogy van egy zárt kódú biztonságtechnikai életveszély-halom...

musi 2011.10.22. 01:01:33

@big-boss: "Megnézem kinek van MacOSx-es gépe otthon" :DDD LOL Nincs senkinek hallod... Még nem láttunk olyat soha.

lehuto 2011.10.22. 04:17:20

Jobbat mondok: én olyan életet élek, amit leshetnek. Akinek az a kaland, hogy az én életemet meg adataimat figyeli, az már tényleg származik. Mindenesetre jó szórakozást hozzá. Pffff.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.10.22. 07:30:53

Üdv, köszöri a rengeteg kommentet :-)

A mostani hiba igaz, hogy Mac-en van, de semmiképpen nem akartam ezt kihangsúlyozni, hiszen ez ahogy Bunkó említette, volt, van, lesz Windows alatt is tömegével, és összességében a Mac még jobban áll a Windowshoz képest. Ami a Mac fronton a lényeg, trójai ott is van, és vigyázni meg mindenhol kell.

@eax_ :

"a levágott jackdugó, Ez nem feltétlenül elég."

Ha már kaptál száz gépet, rádiót, egyebet, látni, hogy ez egy machanikus cucc, ami leválaszt, amint bedugsz új cuccot.

Legalábbis én így tudom, de ha tudsz részleteket, érdekelne.

@Cso zsi:

Igazad van abban, hogy a történet idealisztikus abból a szempontból, hogy évekig zajlik. Amikor a hanglezstúdióban dolgoztam, a technikusok között sok olyan volt, ami azonnal szétkapott mindent, hogy lássa, hogy tanuljon, mert kíváncsi volt.

@Klarky:

Egy újszülöttnek minden vicc új, ezek alapján például egy túlélő blogban is leírható, hogyan olt el egy tüzet víz nélkül biztonságosan földdel. Aki ismeri, azt kommentelheti: nem hiszem el, hogy ezt írja, ezt mindenki ismeri. Nos, ahogy a philadelphiai esetet láthatod, nem vette észre senki, azon buktak le, hogy a diri azért adott intót valakinek, mert otthon csinált valamit. Enélkül évekig kukkoltak volna. Ha egy diák ezt elolvassa, és pavlovi reflexből leragaszt, és ezzel védi magát, már nem dolgoztam hiába.

@TrueY:

A kíváncsi hozzáértők elől nincs orvosság, ezzel egyetértek. Régen volt, hogy az IC-ket lecsiszolták, kiöntötték műgyantával, stb. Ajánlom olvasni valónak ezt:

antivirus.blog.hu/2011/09/22/hackactivity_7db_part_threeewrgf

Ahol Hornák Zoltán: Crypto-chipek biztonsága címmel azért jól látszott, a szakértő elől nehezebb eldugni bármit, mint a klaszikus elavult "Security by obscurity" elv alapján.

@Androsz:

Igen, egyetértek, tudna még okos tanácsokat mondani. Talán még volt is valamilyen kormányzati tanácsadó. Az azért szintén érdekes, hogy ha BÁRMILYEN állást keresel, több körös vallatás, képesség felmérés van, szétszednek, de ha politikusnak

mész, akkor arra AZONNAL alkalmas vagy :-)) Lehetne nekik is felvételi, nem olyanra gondolok, hogy mikor volt a mohácsi vész, de mondjuk világtörténelem az jöhetne, és még a Sim City-ben seem tud végig vinni egy elégedett prosperáló város felépítését, akkor vizslát.

@Bunkó:

A kormányzati gépekben - legalábbis Amrikában - kb. 2008 óta kötelezően beleteszik a GPS-t, ezért tudja például Jack Bauer megtalálni a CTU-ban

@Lehuto:

Veled ezúttal nem értek egyet. Szerintem a magánemberek esetében jól megdőlt az a korábbi, közkeletű vélekedés, hogy "én csak egy hétköznapi ember vagyok, nincs semmi rejtegetni való a gépemen" Már alaptól helytelen a provacy-hoz való ilyen hozzáállás, senkire nem tartozik a magánéletünk részletei, de aztán jöttek a botnetek, kémprogramok, és ellopják a logint, nevedben levelet küldhetnek az ismerőseidnek, küldj pénzt. Ellopják a banki accountot, amit aztán árulhatnak a neten, illegális (warez, porno, terrorista) anyagokat tölthetnek a gépedre, amiért aztán te felelhetsz. Már a képek ellopása is hasznos, lehet, hogy most átlagember vagy, de majd 10-20 év múlva indulni akarsz a polgármester választáson, és akkor kiteszik a sugárban hányós, melegfesztyálós, náci egyenruhás, egyéb képeidet, és máris nem leszel polgármester. A magánélet védelme szerintem mindenkinek fontos, és sokszor nem kézenfekvő a veszély, de létezik ilyen, például Londonban a betörők már a Google térképen nézik, hány autó áll a ház előtt, hova érdemes betörni, de az idióta minden percben tudósítok a Facebookon, melyik utcában járok éppen szokás is veszélyes ugyanilyen okból, lásd: pleaserobme.com/



Rosszindulatú Vászka • <http://globalicum.wordpress.com>
2011.10.22. 07:55:41

MacGyver óta tudjuk, hogy szígszalaggal szinte minden kiélezett élethelyzetre tudunk megoldást :)

Én ezt a trükköt már évek óta ismerem. No nem azért, mert annyira sok eszem van, hanem a Mamikántól lestem el. Rendszeresen hív, hogy elromlott a TV-je, mert nem tud csatornát váltani ill. és vagy ki-be kapcsolni. Ugyanis bántja a szemét az a soi piros fény meg szám a beltéri meg a TV elején és rendszeresen leragasztja vagy letakarja.

Más.

Az az iskolás megfigyelési ügy nem vett-e olyan fordulatot, hogy a tanár pedofil kukkoló-e (ha nem szakmai blog volna, ezt most kifejteném bővebben szívesen :)?



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2011.10.22. 08:10:06

Szia Rosszindulatú Vászka!

Ez a Tv-s leragasztás jó, a nagy kérdés, ha mi öregek leszük, ilyen technikai fejlődés mellett most a topon érezzük magunkat, de fogjuk-e érteni majd mi történik öregén?

Az iskolás megfigyelési ügy azon alapul, hogy a Mac-ben - nagyon helyesen - van ilyen ellopás elleni cucc, ha a tolvaj bekapcsolja a lopott gépet, akkor be lehet azonosítani, lehet képet csinálni róla - és ez kétségtelenül hasznos. Ám az iskolában a rendszergazdák emellett be nem jelentett módon, illegálisan Istent játszottak, ellenőrizgettek akkor is, ha nem volt lopás, illetve el akarták dönteni, mi a megfelelő magatartás otthon, amihez semmi közük. Képzeld magad egy szülő helyébe, hogy a gyerekedet egy idegen kukkolja.

Pedofil szál ebben az esetben tudtommal nem volt, felmentették őket, az FBI szerint "nem tudatosan" sértettek jogot. Ám visszanyúlva Léhőti kolléga felvetéséhez, az én csak egy hétköznapi ember vagyok, csak bátran buzerálják a gépemet: ha spamet küldenek a gépedről, meg DDoS-olják a Fehér Házat, vagy mondjuk pedofil képeket töltenek rá, nagyon durva ügymenet is lehet ez. Voltak Amerikában tanár, ahol a diákok bosszúból töltöttek fel illet neki, és több évig tartó hercehurca, állásvesztés, feleség otthagya, kiközösítés, és talán valami szakértő esetleg segít neki. De volt az a tanáros eset is, ahol egy kártevő fertőzte meg a gépét, letartóztatás, válás, állásvesztés, kiközösítés, több éves provedúra, míg egy forensices kimutatta, a kártevő percnként 40 pedofil oldalra látogatott, ami egyértelműen NEM SZOKÁSOS EMBERI használatot mutat, így végül felmentették. Hogy aztán mit kezd az életével, nem tudni.

Viszont a kártevő szerzők is olvasnak híreket, és mostantól neked és nekem olyan pedofiles kártevőt fognak feltölteni, amit öt percnként megy egy oldalra, így mehetünk majd a kóterba ;-)



Rosszindulatú Vászka • <http://globalicum.wordpress.com>
2011.10.22. 08:27:38

[□ Csizmazia István \[Rambo\]: Üdv!](#)

Mamikánk ügyében még annyit, hogy ha másképp nézem a dolgot, akkor meg a lehető legegyszerűbben, saját erőforrásból, az eszközök károsítása, másosítása és megbontása nélkül megoldotta a problémáját :)

A sztori vége egyébként az volt, hogy miután a hibajelenséget detektáltam, a zavart elhárítottam és mutattam neki hogy tud kapcsolgatni, azt felelte? hadjad fiam, úgyis csak azt az egyet nézem mindig.

Tanulság azon kívül, hogy ahogy te is megjegyezted, vélhetően mi sem leszünk jobbak, talán annyi, hogy ami nekem hiba, másnak nem feltétlenül.

A pedofil szálban meg inkább arra gondoltam - feltételezve a jóhiszeműséget és a jogalkotó ill. szervek ügyében többször tapasztalt "köfejtiséget" (ld. a Huckabee Finn rasszista listára tételét), hogy életszerű az elképzelés, hogy a diák fehérneműben csetel vagy szörföl, innen kezdve a megfigyelése ügyében megáll a pedofil gyanu, ami amerikában súlyos vád és elég egy egzintencia megtöréséhez.



[Rosszindulatú Vászka](http://globalicum.wordpress.com) • <http://globalicum.wordpress.com> **2011.10.22. 08:30:03**

Monnyakle :(

Egy rosszindulatú hejesírásvírus megfertőzött :(

Donor 2011.10.22. 09:08:55

Manapság már nem mechanikus kapcsoló szakítja meg a mikrofont.

Nekem is olyan, hogy bedugom, kiírja a windows hogy jack csatlakozó bedugást érzékel, szerinte az egy mikrofon és hogy elfogadom, vagy más eszköznek használja?

Ha elfogadom onnantól kezdve külső mikrofon.

Mondjuk ez a hangkártya driverből megy, szóval nem hiszem hogy a flash minden egyes hangkártya esetén bele tudna buzerálni :)

A másik, hogy a notim kamerája fizikailag egybe van építve egy LED-el. Ha villanyt kap, a LED világít. Ha kikapcsolom a kamerát, nincs tápfesz, a LED elalszik. Bukott le már szoftver ennek az egyszerű megoldásnak köszönhetően.

Mondjuk épületes látvány lehet az arcom, amint az ágyban gyűrött tokával bambulom az emaileket, meg a facebookot :D Ha nem használom meg úgy is le van csukva a monitor.

hungi. 2011.10.22. 09:43:14

Ennyi erővel a trójai/spyware/botnet programok is lehetne félni, az ellen meg nem segít semmilyen szigszalag...



shitgun 2011.10.22. 09:58:10

HELPHHELP! A 101 mini sci-fi-t nem lehet letölteni valahonnan??? Évek óta keresem, az enyémet anno megette a kutya, és nagyon szeretném újra birtokolni! Aki tud linket esetleg, löje már ide nekem!



shitgun 2011.10.22. 10:13:38

@Rosszindulatú Vászka:

1. Nekem nem segített, béna vagyok:(
2. A legalitás nem kizárt, nem tudom, élnek-e még a jogok, illetve megvolt eredetiben, tehát kifizettem, tehát nincs lel kifurka. Nem tudom egyébként, hogy a könyv a zenéhez vagy a szoftverhez húz-e, egyik ugyanis legál, a másik nem.
3. Köszkösz!



[Rosszindulatú Vászka](http://globalicum.wordpress.com) • <http://globalicum.wordpress.com> **2011.10.22. 10:21:11**

@shitgun: a szerzői jogok még élnek.

Te a papíralapúval a digitális formátumot nem fizetted ki, pont úgy, ahogy a vinyl birtoklása sem jogosít fel az MP3 vagy CD "lopására".

A magáncélú letöltés szűrkezőna, mert Magyarországon nem kriminalizálható. A torrentezés már más ügy.

Egyébként meg canadahun, ott lelne csudákat. Persze én nem és ellenzem!

Summa summárom, ezért vélhetően mind a ketten Pokolra kerülünk :)

[□űzgolyó 2011.10.22. 10:29:20](#)

Ez a Nikai történet egy film szinopszisa? Mert ilyen tuti nem történt.

[dobzse.laci 2011.10.22. 11:12:54](#)

[@Csizmazia István \[Rambo\]:](#)

ahogy @Donor is írta, ez manapság már nem így megy.

A bemeneten impedanciát mér és úgy dönti el, hogy az mire jó.

Pl. néhány mobilnál egy db mini USB van, de arról megy a headset is.

Az impedanciából dönti el, hogy adatot vagy audiót küldjön rá.

Viszont, ha a jack végére egy membránjától kiherélt, vagy akusztikusan eldugított mikront raksz, akkor sanszos, hogy kivédted a dolgot.

[becsoccsent 2011.10.22. 11:40:19](#)

a flashblocker nem jo?



[bunkó • http://bunko.blog.hu 2011.10.22. 12:50:15](#)

Semmi olyan biztonsági dologban nem szabad teljesen megbízni, ami szoftveresen felülbíráható.

Kamera/mikrofon/bluetooth/wifi/stb - ezeket az egységeket vagy FIZIKAILAG működésképtelené tudod tenni (lásd pl: szigszalag), vagy csupán reménykedhetsz, hogy amit szoftveresen letiltottál, azt valaki más nem fogja szoftveresen visszakapcsolni...

Engem pl érdekelne olyan laptop, amelyiken a wifi kapcsolóval (és NEM nyomógommbal) letiltható.

[dobzse.laci 2011.10.22. 13:10:52](#)

[@bunkó:](#) Sajnos általában a tolókapcsoló sem a wifi tápellátását szünteti meg :(

Múltkor javítottam egyet (Asus F5x), akármilyen bemenetként veszi, szoftveresen felülbíráható...

Stick-kel vagy express-card-dal meg kinek van kedve szütytögni?

Tuti beakad valamibe és kitörik az egész, ha szerencséd van az alaplaptól :D

[Gaspar Gil y Pollas • http://www.kulturtapas.com 2011.10.22. 13:13:28](#)

Azért ez elég kemény. Egyre kevesebb bizodalmmam van a 21. századhoz...

üdv

www.kulturtapas.com



[Celtic 2011.10.22. 17:05:47](#)

[@becsoccsent:](#) Deja. Vagy a

killall -9 plugin-container. A procit is kimeli.

[Trucka • http://tutinoti.blog.hu 2011.10.23. 21:06:10](#)

leragasztod, mikibe meg forró gyantát csöpögtetsz

becsocsent 2011.10.24. 06:55:45

[@Celtic](#): a linuxos korszakom legemlekezetesebb szava a kikillelni. de jól is működött! :D



Celtic 2011.10.31. 09:41:14

[@becsocsent](#): Nyilván működik Windows alatt is, csak ott nem tudom a parancssort.

1.

a) CTRL-ALT-DEL: taskmanager indítása

b) Start menu/Futtatás (XP) vagy Keresés (vagy hogyhíjjak), beírni: taskmgr.exe

2. Megkeresni a plugin-container.exe-t és kilöni

Nem bonyolult, csak leírni. Sokkal egyszerűbb a fenti parancs, hatránya, hogy hozzanemertonek betűzni kell a telefonba....

És tessék: Osama után Kaddhafi

2011.10.24. 14:45 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [video](#) [halál](#) [trójai](#) [ceo](#) [gaddafi](#) [kadhafi](#) [keresőtalálat](#)

"Tessék, tessék, hölgyeim és uraim, Tisztelt nagyérdemű közönség, csak tessék tessék! Itt látható a világhírű diktátor, a popzenész, az utolérhetetlen keresett terrorista vezető, itt haldoklik a nevezetes híresség, elsőrangú közeli videofelvétel, csak tessék, tessék!" Érdekes módon sokakat nem elrettent vagy elgondolkodtat ez a fajta vándorcirkuszi visszás mentalitás, hanem éppen hogy vonz, és kattintásra ösztönöz.



Felejtéstudományi megbízottunk jóvoltából ismét megerősíthetjük azt a közkeletű bölcsséget, miszerint **"azok, akik nem tanulnak a múltból, arra ítéltetnek, hogy megismételjék azt"**. Hát most majd jól kiderül, ki hogy is áll a leckéjével.



[Több mint, két esztendeje már, hogy Osama Bin Laden](#) kapcsolatos kéretlen üzenet érkezett a postaládákba. *"Figyelem! Olvasd el, fontos!!!!!! Az elkövetkezendő napokban E-mail útján képeket küldhetnek, melyen Osama Bin-Laden vagy felakasztva látható, vagy elfogása látható."* Nos ezúttal sem ültek a babérjaikon a kártevőterjesztők, már **gőzerővel zajlik a Kadhafi ezredessel kapcsolatos Google keresési találatok mérgezése kártékony linkekkel**.



Az első jelentések Portugáliából és Spanyolországból származnak, vagyis **ez a kör a spanyol nyelvterületet vette célba**, de a folyamat biztosan nem áll meg itt, ha külön magyar nem is lesz, az angol nyelvterületnek már biztosan reszelik a kódot. Szóval a keresések között feltűnik egy látszólag ismert brazil média linkje (Buenos dias:-), és **azt ígéri, egy videót fogunk látni majd Kaddhafi haláláról**. Ez is [milyen már, hogy mindenki a másik halálát akarja látni a neten](#), node ne morogjunk, inkább nézzük, [hova vezet mindez](#).



Nos, nem a beígért videóhoz, hanem **a felhasználó tudta nélkül átirányítják a böngészőt egy dél-koreai weboldalra, ahonnan a Win32/Qhost nevű banki jelszólopó trójai család egyik tagja fertőzi meg a számítógépet**. Nyilvánvaló, hogy az elfogásakor még élő, de aztán [ismeretlen és rejtélyes körülmények között gyorsan elhalálozó diktátor esete nagyon is alkalmas egy kártevős kampányhoz](#), hiszen már alaptól is mindenki kíváncsi, ám **ezúttal a titok övezte végkifejlet erre is rátesz egy lapáttal**.



Kíváncsiak leszünk, [mi lesz majd Fidel Castro halálakor, milyen emailek, Facebookos, és egyéb csatornák fognak csak most, csak nekünk valamilyen halálos videót beígérni](#), mindenesetre annyi tanulságot le lehet vonni, hogy érdemes óvatosabban internetezni, legyen naprakész biztonsági internet security csomag telepítve a gépünkre, legyen NoScript böngészőben, legyen valamilyen feketelistás linkszűrő plugin, ne kattintsunk mindenre, továbbá éljen és virágozzék a brit tudósok szerint is a legmagasabb alkoholtartalmú étel: [a falra hányt borsó](#).



Mellesleg a [múltkor emlegetett hamis Facebook értesítőtől](#) jött azóta pár újabb, volt az előző kísérlettel hajsza! pontosan egyező is, de jött már új típusú tárgysorral is, szóval nem árt tudni, láthatóan rácuppantak a trükkre a kártevőterjesztők.



2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



• [2 trackback](#)

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3326226>

Trackbackek, pingbackek:

[Trackback: Kadhafi fia él?](#) 2011.10.24. 16:13:01

Az új idöket ünneplik Líbiában, miután az Átmeneti Nemzeti Tanács hivatalosan is lezárta a Kadhafi-rezsim korszakát. Szudáni sajtóhírek ugyanakkor arról szólnak: a lelött líbiai vezető korábban halottnak hitt fia él.

[Trackback: Zsarnoki festészet: Kadhafi festményei](#) 2011.11.04. 19:46:14

Régóta beszélnek Kadhafi festészetéről, de képek nélkül haszontalan beszélni róla. Íme néhány festmény, amit a sajtójelentések neki tulajdonítanak. A képek többsége szomorkás hangulatú. A kritikusok szerint viszont annyira rondák, mint maga Kadhafi....

Kommentek:

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

Nincsenek hozzászólások.

Fúú, mit találtam rólad a neten!

2011.10.26. 12:40 | [Csizmazia István \[Rambo\]](#) | 2 komment

Címkék: google csalás twitter adathalász

Ez a fiú eleinte egy vicces képet jelentett, amire - állítólag - az önzetlen levélíró ismerősünk hívja fel a figyelmünket.



A kérértlen üzenethez mellékelt egy képet is, amin [az alábbi üzenet olvasható: "Found a funny picture of you \[LINK\]"](#). Itt megint a magyar nyelv megment minket sok mindentől, mert eléggé életszerűtlen, hogy Kovács úgy adja Takács tudtára, hogy milyen képet talált róla a neten, hogy szokásától eltérően nem magyarul emaillez neki, hanem helyette angolul kommunikál vele a Twitteren át. Igaz, ha egy külhoni ismerősünk nevében érkezik mindez, azzal már valóban növekszik a csábítási és kattintási esély (Mit láthatott, amit mi nem?)



Am még így is, ha a mellékelt képekre nézünk, valljuk be őszintén, **veterán antivirus.blog olvasók körében mindez csak egy hervatag ajkbiggyesztést érhet, hiszen a csupa kétes ".ru" végződésű domain már elegendő ahhoz, hogy undorral és nagyon helyesen visszautasítsuk a kattintást.** Ha belegondolunk, miért pont egy panmatrac.ru;-) vagy valami hasonló oldalon írnának rólunk dehonesztálóan - legalább egy vonzóbb nevű és .com végződésű lenne az Istenadta, az nem lenne annyira árulkodó, és nem lógna ki ennyire a csalás lólába.



A módszer továbbfejlesztett változatánál szintén egy ismerősünktől kapjuk az alábbi kéretlen figyelmeztető üzenetet, melyszerint kedvesen tudtunkra adja, hogy egy számunkra kellemetlen blogot fedezett fel, a séma kísértetiesen hasonló, mint a fent: "I saw a real bad blog about you, you see this? [LINK]"



[Am sztahanovista módszerekkel lehet még erről a rókáról további bőrköket is lehúzni](#), ehhez pedig mindössze a következőt kell írni: "**so i googled your name and found some really funny stuff about you lol its archived here** [LINK]", magyarul Fúú, rákerestem a nevedre a Gugliban, és ott aztán apám hú de micsoda dolgokat sikerült találni, itt vannak mind lementve!" Hát nagyjából itt tartunk most, **ha esetleg valaki meggondolatlanul mégis belesétált a kelepcébe, az cseréljen mihamarabb Twitter jelszót**, az 12345, abc és a kutya56 helyett [valóban erős jelszavakért például itt is lehet keresgél](#)ni.



Ha valaki egyazon jelszót több helyszínen is használt volna - amellett, hogy sújtsa őt dolgozó népünk jogos megvetése ;-) - az **számíthat rá, hogy a gmailjétől kezdve a facebookig bezárólag hamar rápróbálnak minden accountjára**, így a további családok elkerülése érdekében a változtatás ezeken a helyeken is mielőbb szükségessé válik, mostantól egyedi erős jelszó formájában. **Kötelező szakmai olvasmányok lehetnek** a tárgykörben [Noszty fiú esete Sarah Palinnal](#) valamint a [Légy jó te büdös jelszó mindhalálig](#) című korábbi opuszok.



A műves **Twitter** adathalász hasonmás oldal ötlete egyébiránt nem újdonság, hiszen már idén nyáron is zörögtek az orsók, zizegtek a damilok, [akkor a jó öreg "Osama Bin Laden éli" kezdetű](#) csali himbálódzott az adathalászok horgán. **Nehéz** persze örökvénvű és

egyetemesen tanácsot adni arra nézve, milyen ismerőstől és/vagy idegentől kapott érdekesnek ígérkező tartalomra lehet, illetve nem szabad kattintani. Ehelyett inkább arra érdemes fókuszálni, hogy ahová személyes név-jelszó accoounttal lépünk be, ott **mindig** ellenőrizzük le, valóban a megfelelő weboldalon járunk-e - URL, IP cím helyességének ellenőrzése például ShowIP kiterjesztés használatával, ahol csak lehet, legyen HTTPS, fusson valamilyen böngészési tanácsadó (például NetCraft, WOT), mely **kiegészítő** feketelista alapján figyelmeztet, ha gyanús vagy leplezett adathalász oldalra tévednénk, illet egyébként a jobb antivírusok is tudnak. Ja és persze sokat használunk magunknak már pusztán azzal is, ha nem hiszünk el rögtön mindent.



13 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3330926>

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](#).



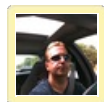
[szmoker \(Homo Trollicus\) 2011.10.26. 16:59:41](#)

"Ez a fúú eleinte egy vicces képet jelentett"

Azt hittem ez Mr. Furkó szavajárása volt vala - "Fúú, de jó vagy!"

spforever.uw.hu/Iskolai_alkalmazottak.html

Viccesnek épp vicces :)



[BenkovicsTomi 2011.10.28. 17:50:09](#)

Én nagyon szeretem az ilyen feladókat is:

noreply <noreply[kukac]facebookbeecham[pont]com>

A legszebb, hogy olyan címre jön a levél, amit még véletlenül sem használok a FB-n.

Szerencsére az ilyeneket a legtöbb levelező program kiszűri elsőre.

iTunes, youTunes

2011.11.02. 17:00 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [apple](#) [itunes](#) [phishing](#) [adathalász](#)

A [Facebook oldalas trükközések](#), valamint [Twitter csalások után](#) most az Apple következett a sorban, ezúttal az "Account Info Change" tárgysorral rendelkező, és igen élethűen kinéző ügyes levélnek határozottan jó esélyei vannak a táplálékláncon.



Az iTunesbeli account adataink változásáról értesítő kéretlen üzenet küldői szemlátomást nagy gondossággal jártak el, minden részletre igyekeztek ügyelni, így a levél feltüntetett feladója sem Lakatos Winettou, [hanem "do_not_reply@itunes.com" lett](#), igaz a levél smtp.com-on keresztül elküldése valamilyen Gmails accountot sejtet.



Bár a valódi Apple levelek inkább az "id.apple.com" vagy az "InsideApple.Apple.com" címet használják, de egyfelől ez még így is sokaknak hitelesnek látszhat, másfelől a jó adathalász is holtig tanul, mindig vannak továbbcsiszolható részletek.



Kinézetre aztán már nem igazán találni kifogásolni valót, jó csalinak bizonyul a levél, azonban [a végállomás az Apple és az iTunes helyett egy ingyenes tárhelyre felpakolt adathalász oldal](#). Az biztos, hogy az ilyen költség- és ráfordításmentes csalási módszer nagyon népszerű, mert a felelőtlenül rossz helyen begépett személyes (pl. név, lakcím) és bankkártya adatokkal könnyű visszaélni.



A világhírű mouse hover módszer segítségével mindazonáltal a felhasználók túlélési esélyei mégis javíthatók, és remélhetőleg azért erre csak kevesen kattintottak rá. Összefoglalva jól felismerhető az a tendencia, hogy spamek az elavult "Replica Rolex" és "Enlarge yo Penis" módszerek helyett egyre inkább a legitim, valóságos és neves cégek, szolgáltatások valóságos leveleit lemásolva, azokat hamisítva terítik hamis gyógyszeres és egyéb kártékny kódokat tartalmazó weboldalakra irányító linkekkel felvértezett kéretlen leveleiket.



Ennek fényében a felhasználóknak hozzáállás terén is egyre inkább észnél kell lenni, például hogy a kéretlen leveleket hány fokok szögben dobják a kukába :-)

Tetszik Regisztrálg, 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](#)
- [Ez történik a weben egy perc alatt](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3348235>

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.

Már csak harmadik a Conficker féreg

2011.11.04. 10:05 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

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.



Elindult végre a Conficker féreg háttérbe szorulása, bár ez pillanatnyilag csak egy enyhe fokozatú, második helyről a harmadikra való mozgást jelent. Helyét a Win32/Dorkbot féreg foglalta el, amely cserélhető adathordozók segítségével terjed, és mivel tartalmaz egy hátsóajtó komponenst is, emiatt távolról átvehető az irányítás a fertőzött számítógép felett.



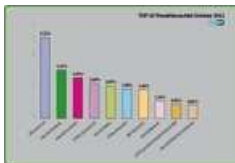
Szinte érthetetlen módon továbbra is az Autorun vezeti a mezőnyt immár hetedik hónapja. Az idén [végre a Microsoft is próbált hatékonyan segíteni a helyzeten februári célzott frissítésével](#), vagyis egyértelműen a felhasználóknál van ez ügyben a labda, nem idejében vagy egyáltalán nem is frissítenek. Igaz, azt is el kell ismerni, hogy az ellenoldalon, a kártevő készítőik is igyekeznek minél jobban és minél tovább kiaknázni az Autorunnal kapcsolatos lehetőségeket új kártevő verziókkal, aminek ékes példája, hogy nem csak a korábbi Conficker féreg, hanem [például a hírhedt Zeus botnet egyik jelenlegi fertőzési rutinja is ezt a sebezhetőséget igyekszik kihasználni](#).



Viszonylag nagyot rukkolt előre a korábbi hetedik helyezett HTML/ScrInject trójai, amely ezúttal az előkelő negyedik lett. Fertőzése során egy üres (c:\windows\blank.html) állományt jelenít meg a gép böngészőjében, és hátsó ajtót nyit a megtámadott rendszeren, melyen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Az ESET e havi [hónapzáró összefoglalójából a havi statisztika mellett](#) még az is kiderült, éppen az ESET víruslaboratórium kutatói figyeltek fel egy új OS X-es kártevőre. A Tsunami nevű IRC csatornán át vezérelhető backdoor [egy 2002-es, tehát egy kilenc évvel korábbi Linuxos kártevő átirásából, portolásából](#) keletkezett, és segítségével a megfertőzött Macintosh gépekről távoli DDoS támadásokat lehet indítani. A kutatók úgy gondolják, a régi-új trójai program fertőzése egyelőre nem jelent átfogó veszélyt, inkább csak az OS X platform kószolgatása, tesztelése zajlik a háttérben.



Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2011. októberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 21.90%-áért.



1. INF/Autorun vírus

Elterjedtsége az októberi fertőzések között: 5.21%

Előző havi helyezés: 1.

Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozónak. 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/Dorkbot féreg

Elterjedtsége az októberi fertőzések között: 3.12%

Előző havi helyezés: 3

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>



3. Win32/Conficker féreg

Elterjedtsége az októberi fertőzések között: 2.63%

Előző havi helyezés: 2.

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 eljárshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárson 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: 2.24%

Előző havi helyezés: 7.

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>

5. Win32/Sality vírus

Elterjedtsége az októberi fertőzések között: 2.07%

Előző havi helyezés: 4

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

6. HTML/Iframe.B.Gen vírus

Elterjedtsége az októberi fertőzések között: 1.89%

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.



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

7. Win32/Autoit féreg

Elterjedtsége az októberi fertőzések között: 1.84%

Előző havi helyezés: 6

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>

8. Win32/Ramnit vírus

Elterjedtsége az októberi fertőzések között: 1.12

Előző havi helyezés: 8

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.



☐ővebb információ: <http://www.eset.eu/encyclopaedia/win32-ramnit-a-backdoor-ircnite-bwy-w32?lng=en>



9. JS/TrojanDownloader.Iframe.NKE trójai

Elterjedtsége az októberi fertőzések között: 0.91%

Előző havi helyezés: 10

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/PSW.OnLineGames trójai

Elterjedtsége az októberi fertőzések között: 0.87%

Előző havi helyezés: 9.

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponensei is vannak, melyek segítségével igyekeznek állományait és működésüket a fertőzött számítógépen leplezni, eltüntetni. A kártevőcsalád ténykedése jellemzően az online játékok jelszavainak ellopására, majd a jelszóadatok titokban történő továbbküldésére fókuszál. A bűnözők ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21psw-onlinegames>



Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Információkai biztonság az egészségügyben](#)
- [Ez történik a weben egy perc alatt](#)
- [Dropbox csálival terjedtek a kémprogramok](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3351583>

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](#).

[mateo4 2011.11.06. 20:27:34](#)

Hát persze, ha egy vírus sokáig előkelő helyen van a vírustoplistákon, akkor előbb-utóbb a felhasználók is megtanulnak ellene védekezni és visszaszorul. Szerintem ez történik a Confickerrel is. Remélem, hogy az Autorunnal is ez fog majd történni.

Csináld magad fapados Autorun féreg

2011.11.07. 13:05 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [php password féreg jelszólopó](#)

Éppen most tettük közzé az **október havi vírusstatisztikát**, és ebben elméltünk arról is, miért **vezethet már hetedik hónapja az Autorun**. Ha a választ nem is fejtettük meg, megint találtunk valamit, ami még rákapaszkodhatott a mérleg serpenyőjére, és talán növelte valamiképp az ezzel kapcsolatos fertőzések számát.



Az [ESET víruslaborjában figyeltek fel egy PHP nyelven készült kártevőre](#), amely a megtevesztés többféle eszközével felvértézve próbál meg adatokat eltulajdonítani az áldozatok gépéről. Kezdjük azzal, hogy szokatlan, hogy egy kártevőt ne alacsony szintű, hanem "mezei" szkript nyelven írjanak, erre maximum pár darab PoC, azaz Proof of Concept kód készült: lám, na ugye, hát ilyet is lehet, megmutattuk, nesze. Esetünkben a **PHP kódot a Bambalam PHP Exe Compiler segítségével hozták EXE**, azaz Windows alatti bináris futtatható formátumúra.



A megtevesztésre nem véletlenül céloztunk, ugyanis abból több kilónyi található benne, kezdésnek mindjárt a kicsozott üzenet, amely **cseh nyelven írja az alábbiakat: "(C) Copyright 1985-2001 Microsoft Corp. Inicializálás... Ez a művelet néhány percet vesz igénybe. Kérem várjon ..."**. Egy rejtőzködő és adatlopó kártevő nyilván nem azt fogja kiírni, én egy vírus vagyok, egy MS üzenet pedig ártatlannak és hivatalosnak látszik.



Vegyük észre, hogy egy vadonatúj kártevőben milyen okosan és rafináltan használnak "Copyright 1985-2001" szöveget, **erősítve az ártatlanság látszatát, ez már régóta a Windows része, nem egy friss kód**. A fertőzés folyamán létrehozott Autorun.inf pedig többek közt **olyan neveket is alkalmaz, mint setup.exe vagy például install.exe**.



A fapados jelzőt pedig az magyarázza, hogy különösebb programozói kunsztok helyett az **olyan alapparancsok kimeneteinek fájlba irányításával nyerik ki a kikémlt információt, mint net user, ipconfig, netstat, arp, tasklist vagy regedit**. A begyűjtött információk **elég széles kört ölelnek fel**, többek közt ICQ és egyéb IM kliens adatok és üzenetek, böngészőkliensek (IE, Mozilla Firefox, Opera, Chrome) mentett jelszavai, levelezőkliensek (Outlook, Outlook Express, Mozilla Thunderbird) mentett jelszavai, Total Commander régi változatában clear textben mentett FTP jelszavai, Windows hitelesítési információk, a Windows Address Book címjegyzék tartalma, a Windows User Account részletei, hálózati címek, nyitott kapcsolatok, a futó processzek és szervizek listája, a környezeti változók, a felhasználó összes könyvtára és állománya, a legutóbb megnyitott dokumentumok listája, a Registry teljes tartalma, valamint a Windows MS Office termékulcsok adatai.



Az összeharácsolt adatokat aztán a **80-as porton HTTP POST módon küldözgetik ki egy .gz típusú tömörített állományban**. A NOD32 és ESS detektálja a PHP férget, Win32/Autorun.PSW.Agent.E néven érkezik rá a riasztás. Látható, hogy kifinomult és különösen szofisztikált víruskód nélkül is lehet LEGO elemek mintájára összeállítani működőképes kártevőt. Emellett **tanulság lehet még, hogy nem csak zoknit és alsónadrágot kell több-kevesebb rendszerességgel cserélni, hanem jelszót is ;-)** **Jelszólopás gyanú esetén pedig nem a meglévő account begépelése szükséges esetleg további ismeretlen indíttatású "lopásellenőrző" weboldalon**, hanem valóban erős, egyedi új jelszó választása Speedy Gonzalest meghazudtoló gyorsasággal.





4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



0



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["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/3360512>

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 számítógépes védekezés 4 arany szabálya

2011.11.09. 17:10 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [jelszó](#) [számítógép mentés](#) [vírusvédelem](#) [óvatosság](#)

Mit tegyünk, ha négy pontban kellene összefoglalni azokat a legfontosabb dolgokat, amikkel a támadásokat, vírusfertőzéseket megelőzhetjük? Az "ismétlés a tudás jó édes anyukája" jegyében jöjjenek a tippek, amiből három a magyar igazság, és egy a ráadás.



1. A vírus- és kémprogramvédelmi programok azért vannak, hogy használjuk őket.

Tűzfalal kiegészítve, vagy még inkább komplett Internet Security csomagként pontosan az a feladata, hogy a már ismert, vagy ismeretlen, de gyanús viselkedésű programokat távol tartsa a számítógépünkől. Az persze igaz, hogy nincs 100%-os védelem, de még így is nagy szolgálatot tesz a védelmi program.

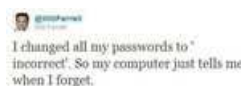


Szokott még ezzel kapcsolatban egy olyan hiedelem lenni, hogy ha van vírusirtó telepítve, akkor letudtunk minden feladatot. Ez nem igaz, ezt ki kell egészítse a biztonsági javító frissítések, úgynevezett patchek naprakész telepítése, különben sebezhető marad a rendszer. Nyilván az is fontos, milyen védelmi programot választunk, ebben pedig AMTSO elveknek megfelelő tesztek eredményei segíthetnek, és [semmiképpen nem felugró ablakban kéretlenül ajánlkozó ismeretlen, hamis antivírusok](#).



2. Használjunk erős jelszavakat

A "kellően erős" és a "könnyen megjegyezhető" nagy valószínűséggel nem közeli rokonok, ám [ennek ellenére érdemes megtenni ezeket az erőfeszítéseket, és valamilyen nehezen kitalálható](#) (nem kutya, macska, gyerek neve, születési dátuma), nem túl rövidke (legalább >8), vegyes karaktereket (kisbetű, nagybetű, szám, valamint extra jeleket +, -, %, stb.) is tartalmazó jelszó a kellően erős, aminek ahhoz, hogy megfelelően betöltse szerepét, még további kívánalmaknak kell megfelelnie.



Ne tudja rajtunk kívül más, ne legyen ki postitelve a monitor szélére, és ne használjuk sehol máshol, magyarul minden egyes helyen külön bejáratú másik egyedi jelszót használjunk. A jelszót gyanú esetén azonnal, míg incidens nélkül is valamilyen rendszerességgel (havonta, negyedév, félév) változtassuk meg.

3. Saját adatok rendszeres mentése külső adathordozóra

Bármilyen szoftvert megvehetünk újra, de [a saját munkánkat, saját dokumentumainkat, elveszett családi fotóinkat nem kaphatjuk meg senkitől és sehonnan](#). Az adatok elvesztésének oka különböző lehet: felhasználói hiba, hardver meghibásodás, vagy számítógépes kártevő, ám az eredményt tekintve ugyanaz: [ha van mentés, és van mit újratelepíteni, mentésből helyreállítani, akkor jó, ha nincs ilyen, akkor megáll az élet, vagy pótolhatatlan veszteségeket szenvedünk el](#).



A gyakoriság ebben az esetben a felhasználás módjától függ, munkavégzés esetén napi részmentés indokolt, havi teljes, inkrementális mentéssel kiegészítve, míg egy csak játékra és szórakozásra használt otthoni számítógépnél elég lehet a negyedéves vagy akár a semmilyen is. Lehetőségek itt is tágak, ma már felhőben is tárolhatunk mentéseket, de a külső adathordozók árai is elérték azt a szintet, hogy mindenki által elérhető legyen egy külső HDD vagy egy méretes USB kulcs.



4. Legyünk biztonság tudatosak és óvatosak

Ide tartozik már az is, milyen programokat telepítünk, hogyan választunk megbízható alkalmazásokat. Mindent telepíteni, minden [kéretlen linkre, üzenetre, tartalomra, levélre kattintani](#) felelőtlenség és veszélyes. Ilyen üzenetek érkezhettek nem csak ismeretlen feladótól, hanem közvetlen ismerőstől is, ám ez sem oka arra, hogy gondolkodás nélkül mindent elhiggyünk.



Az óvatos telepítés nem csak a kéretlen hamis vírusokat jelentheti, hanem [újabbban már Windows rendszerkarbantartó programok](#) között is vannak scarewarek, trójai pedig tulajdonképpen bármi lehet, akár egy Adobe telepítőnek látszó fájl egy rosszindulatú weboldalon. Igyekezzünk alaposan utánanézni, ha valamilyen programot keresünk, a biztonságos letöltéshez pedig a gyártó közvetlen weboldala a legfelelőbb.



Ha névvel és jelszóval jelentkezünk be egy oldalra, tegyük ezt lehetőség szerint titkosítva (HTTPS-en keresztül), ingyenes wifi elérésnél ne lépünk be sehova, otthoni vezeték-nélküli routerünket pedig mind a setup beállítási, mind a webes adatok forgalmi részénél lássuk el erős jelszóval.



23 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adatahalászáttal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3366079>

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.

Social Engineering olimpia

2011.11.14. 14:35 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [facebook átverés](#) [15 másodperc](#) [98%](#)

Megszokhattuk már, hogy a sportteljesítmények az évek folyamán - a szerfelett ritka kivételektől eltekintve, mint [például Mike Powell 895 cm-es távolugró világrekordja](#) - **állandóan javulnak**, atlétáink **faragják a másodperceket, harapják a centiket rendületlenül**. Mai példánkban is tanúi lehetünk a képességek effajta folyamatos javulásának, hiszen kettő egész (zwei comma null) másodperccel jobb eredmény abszolválását mi másnak is hívhatnánk?



Kezdjük ott, hogy egy nagyon is találó névvel jelent meg idén januárban egy posztunk, melyben arról elmélgedtünk ["De igen, többször is, és ugyanabba a folyóba"](#) címmel, hogy vajon mi okozhatja valójában, hogy **folyamatosan mindig rengeteg áldozata van a csalásoknak**. Amiatt lehet, hogy minden vicc új minden újszülöttnak, vagy esetleg az az oka, hogy a figyelmetlenségükből nem tanulnak a felhasználók, akiknek pedig legalább a saját kárukon azért illene.



Biztos, hogy nem az alábbi szalagcímmel fognak majd beszámolni a médiában erről a "régi-új" csalásról: **"Mivel már mindenki alaposan megtanulta a leckét 'Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót' esetből, mire vigyázzon, így a mostani indigóval készült '98 Percent Of People Cant Watch This Video For More Than 15 Seconds' csalásnak már egyetlen biztonság tudatos ember sem dől be világszerte, így végül a csalók visszavonultak, jelenleg képeslapok és díszműáruk terjesztésével töltik egyhangú napjaikat."**



Ám sajnos nem így van, ehelyett az látszik valóságos forgatókönyvnek, hogy mégis terjed a fenti link. [Aki a "CLICK LINK TO WATCH VIDEO & SEE HOW LONG YOU CAN LAST!!" URL-re rákattint](#), azzal a beígért video helyett ismerőseinek elküldi, megosztja velük ezt az idióta linket, **bónuszként időnként esetleg feljön neki még egy "Complete a 30-second test below to prove you are a human" ablak is, valóban emberek vagyunk-e**. Talán mert egy Deep Blue sakkozó robot, vagy R2D2 már alaptól nem is kattintana rá;-)



Szóval csak akinek az a történelmi momentum, hogy bár **nem lát semmilyen videót, de ezenközben szénné spammeli az összes ismerősét** kimondhatatlanul és fájdalmasan hiányzik az életéből, kizárólag az kattintson rá.



Mit is mondhatnánk zárásként? Talán azt, **ha legközelebb valaki azzal kap Facebook üzenetet, hogy 'Az emberek 98 százaléka nem tudja 12 másodpercnél tovább nézni ezt a videót', kattintás előtt/helyett esetleg jusson eszébe ez a mai blogbejegyzés**. Amúgy meg érdemes lehet olvasgatni még [egy hosszabb összefoglalót is 2011 legjelentősebb facebookos átveréseiről](#).

Tetszik 2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)

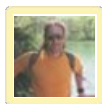
- [Kártékony böngésző kiegészítők jönnek](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3379552>

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>
[2011.11.16. 08:10:48](#)**

Itt az ESET-es srácok YouTube videója ugyanerről a csalásról:
www.youtube.com/watch?v=fGkNi8w87OY

Fizess a semmiért, újratöltve hanyadszor is?

2011.11.16. 14:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [facebook](#) [csalás](#) [support](#) [átutalás](#) [hideghívás](#)

Lehetne az is az alcímünk, hogy a "Száraz tónak nedves partján nem létező Microsoft partner kuruttyol" mondatban vajon melyik a kakukktojás. Hogy aztán a süket ember végülis meghallgatja-e vagy sem, azt csak sejteni lehet, tudni viszont, hogy **kialakult egy újfajta irányzat, melyben kéretlenül jelentkező csalók állítólagos számítástechnikai támogatásra hivatkozva nem létező hibákat javítva úgymond "segítenek", majd ezért banki átutalás formájában fizetséget kérnek.**



A Facebookon is terjedt a kéretlen technikai segítségnyújtás, amikor is a korábban Microsoft partnercég kamu bejegyzésekkel próbált meg Dell, Linksys vagy általános supportot nyújtani. Emellett a tisztes [állampolgárok kéretlen hideg hívásokkal való zaklatása is egy ősi spammer szokás](#), ez a módszer is szerepelt a repertoárjukban. **Az állítólagos segítségnyújtás során olyan létező, de egyáltalán nem veszélyes jelenségre hívták fel a figyelmet, amit "segítenek" elhárítani távoli eléréssel belépve a gépünkre.**



"Ha valami nem romlott el, azt nem kell megjavítani" - tartja az amerikai közmondás, és igazat kell adjunk neki. Emellett pedig **ismeretlen, kéretlen supporthívást, üzenetet, levelet kezeljünk kellő óvatossággal** - például előbb igyunk egy feketekávé-t kevéske tejjel, és csak aztán ignoráljuk, töröljük ki, etc. Könnyen belátható, hogy egy kitalált, nem létező szervíz is könnyedén tud magának Facebook oldalt nyitni, akár lájkokat és kamu köszönetnyilvánításokat is gyűjthet, de ez még egyáltalán nem ok arra, hogy mindezt el is higgyünk.



A leírt eseteknél aztán látható, az ügyintéző gáláns kérése után sokan kattintottak a bediktált linkre, ezzel tették be a fejüket az oroszlán szájába: távoli elérésre hatalmazták fel az öt perce még ismeretleneket. [A Guardian információi szerint évi 2 millió GBP-t szakítanak a hamis supporthívásokkal](#) üzletelő csalók - ez a jó magyar forintba átszámítva úgy 742 millió, abszolút nem kispálya.



Az esetről [egy korábbi, 2002-es maci ikonos jdbgmrg.exe hoax jutott az eszünkbe](#), ahol szintén nem volt igazi javítani való, sőt az tett rosszat magának, aki elhitte az álhírt, és naivan kitörölte az ártatlan rendszerállományt. **Ha egyszer valóban számítógépes javításra szorulunk**, azt ne a facebook lájkok alapján tegyük, hanem a **szakszerűség, megbízhatóság és a fizikai távolság aranyháromszög kompromisszumából kijövő szakszervízbe** helyezzük inkább a bizalmunkat, mindezt persze alaposan előre leinformálva.



Ha már Facebook, akkor [a Reuters is beszámolt arról, hogy a pornográf linkek már a spájzban, illetve a Facebookon vannak](#). Valószínűleg kevesen szeretnék, ha [nevükben ilyen tartalmakat küldözgetne valaki az összes ismerősüknek](#). Érdemes hát résen lenni, ehhez persze az is kellene, hogy ha kapunk egy ["Az emberek 110 százaléka nem tudja mínusz 635 másodpercnél tovább nézni ezt a videót"](#), ne kattintsunk rá egyből pavlovi reflexből egysejtű módjára. **Vannak persze ennél univerzálisabb és konkrétabb jótanácsaink is**, ezek következzenek most.

Tartsuk frissen rendszerünket - az operációs rendszer mellett minden alkalmazói programunkat, beleértve az olyan sűrűn támadott elemeket is, mint az Adobe Flash, Adobe Reader, Java, böngésző kliens, stb.

Gondolkozzunk, mielőtt bármire is kattintanánk. Az egy mondatos linkmellékeltes kéretlen üzenetek döntő többsége kártevő terjesztésre, adathalászatra, csalásra, kéretlen reklámok megjelenítésére jó csak.

Legyen mindenhol egyedi és erős jelszavunk, amit időnként csak úgy is változtassunk meg. Ha pedig gyanús események, betörés, kompromittálódás történik, akkor pedig azonnali jelszócsere javasolt.



Ne bankoljunk, levelezzünk, ne vegyünk igénybe név-jelszó párossal igénybe vehető szolgáltatásokat nyitott wifinél. Ha mégis, akkor használjunk VPN-t, ha ez nincs, akkor legalább https-en keresztül kommunikáljunk. Például a Gmail esetében így nem csak a belépés, hanem a bejelentkezés teljes időtartama alatt SSL kapcsolatban tudunk maradni, ám ezt viszont nem minden weboldal biztosítja. Erről a témáról egyébként [Randy Abrams irt egy jó kis összefoglalót még a FireSheep-es mozgalmas időkben](#), de jó részt ma is aktuális.

Fusson naprakész internetbiztonsági szoftver (antivírus, kémprogramirtó, tűzfal) a gépünkön. Akár a kártékony kód viselkedése, akár a kártékony URL jó eséllyel fennakadhat a szűrőjén, így ezzel, és az előző pontokkal együtt elmondhatjuk, mindent a tőlünk elvárható legnagyobb gondossággal megtettünk biztonságunk érdekében.

 Tetszik  19 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3386808>

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.

Ki menti meg Ryan facebookozót?

2011.11.18. 13:40 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [spam](#) [javascript](#) [facebook](#) [porno](#) [xss](#) [optin](#) [optout](#)

Egyes vélemények szerint a napokban zajló Facebookos támadás az eddigi legdurvább volt: [a felhasználók nevében küldött üzenetekben végigsöprő pornográf képek, videós linkek ijesztők és gusztustalonok](#) voltak sokak számára, míg valljuk be, emellett [az alig egy hónapja beharangozott kártékony tartalomszűrés](#) után az üzemeltetők hosszas tehetetlensége is elég kiábrándító.



Ma az idézetek napja van, lesz több is, a mottónk pedig nagyjából valami ilyesmi: **"Trying to solve the world's data security problems is like a doctor trying to solve death."** Most pedig olvassunk bele **a 16-i FB közleménybe**, [amelyet az incidens után adtak ki](#):

"Protecting the people who use Facebook from spam and malicious content is a top priority for us, and we are always working to improve our systems to isolate and remove material that violates our terms. Recently, we experienced a coordinated spam attack that exploited a browser vulnerability. Our efforts have drastically limited the damage caused by this attack, and we are now in the process of investigating to identify those responsible." Vagyis ebben a Facebook azt állítja, **a felhasználók védelme a spamtól és a kártevőktől elsődleges szempontjuk**, és a probléma miatt a böngészőkliensek sebezhetősége okolható.



Direkt benéztünk, még simán lehetett találni tegnap este is ilyen subjecteket az üzenőfalakon. Itt persze azt is meg kell vallani, az áldozatoknak is meg kellett dolgozni azért, hogy elhiggye, hogy megossza, kellett hozzá sokat kattintgatni.

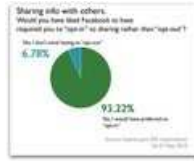


Igaz, **a videó megnézése előtti lájkolásra kattintva tegnap este a rendszer már nem engedélyezte azt**, de azt már nem tudni, vajon amiatt, hogy csak szimplán írtak rá egy szignatúrát, ami ezt blokkolja.





Az már ugye egy másik kérdés, egyáltalán miért engedélyezett az, hogy [előbb kell valamit lájkolni, hogy utána megnézhessük, miért nem szűnik ez meg generálisan, miért ilyen naivak a felhasználók](#). Gondolhatjuk azt is, csődöt mondott a kártékony linkek szűrése is, mert **mi más lenne ennek a feladata, mint hogy egy ilyen helyzetben még a kezdeti szakaszban jelezzon az üzemeltetőknek, és meggátolja a komolyabb világszintű kitörést.**

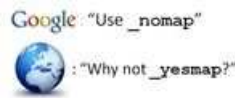


És mi Reynoldsok miért is osztunk meg mindent? Jelenítjük, [mert alaphelyzetben ez az alapértelmezett](#). Nyilván **ennek a megváltozása bár segítene a biztonsági helyzeten, de a biznissz szempontjából viszont kevésbé lenne jó az üzemeltetőknek**, akik így például mondhatják a hirdetőknak: [ide gyertek, itt napi 900 millió kapcsolati információ keletkezik](#).

Az alapértelmezés szerinti **optin - vagyis csak azt osztom meg, amit én akarok, amit én magam engedélyeztem, alpból pedig semmit - esetében ez a szám nyilvánvalóan sokkal kisebb lenne**. A kérdés az, hogy eljut-e egyáltalán és mikor arra a szintre a Facebook biztonság, amivel a jelenleginél sokkal hatékonyabban lehetne megvédeni az átlagfelhasználókat, akik nem számítógépes szakemberek, csak használják a gépüket, a közösségi oldalukat, mint egy mosógépet vagy egy kávéfőzőt. Ahol a mosógépgyártónak meg a kávéfőzőgyártónak van valamekkora felelőssége, ott a közösségi oldalt üzemeltetőknek látszólag nincs, **pedig a statisztikák szerint [az USA-ban a 12 éves gyerekek fele rendszeres](#) Facebook használó.**



Annak idején a Microsoftnak is évekbe tellett, mire eljutott oda, hogy [az Office csomagban a makróvírus helyzet miatt](#) a kikapcsolt makró legyen az alapértelmezett, vagy [a nagysikerű Autorun alaphelyzetben mostanra már tiltva legyen](#). Meglátjuk, [sikerül-e esetleg az FTC-nek itt is nyomást gyakorolnia a jelenlegi alapértelmezett optout](#) - minden megosztok, amit nem tiltok le a sok és bonyolult beállítások között - [gyakorlat megváltoztatása érdekében](#). Talán megbocsátják az olvasók, ha ebben mi az emberi természet ismeretében pesszimistán látjuk a jövőt.



[Egy teljesen másik ügyben, a "véletlen" wifi feltérképezésekkel kapcsolatban](#) az a Google javaslata, hogy **aki nem akar bekerülni az adatgyűjtésbe, az biggyessze a SSID neve mögé a "_nomap" szócskát** (miért nem rögtön "_nosnoop"?). **Ez a megoldás kb. olyan, mint amikor a bank kötelezve van arra, hogy a megváltozott szerződési feltételekről tájékoztassa az ügyfeleket, amire mit tesz? Levelet ír nekik? Frászt, kitesz egy papírt a saját banki falújságjára, és hip-hop, tájékoztatás kipipálva.** Mert hány wifi router tulajdonos fog majd erről értesülni, hány fogja ezek közül meg is érteni és lesz képes változtatni, miközben hányan nem is fognak tudni erről az egésztől és akkor áldozatok maradnak. **A mellékelt kép jól tükrözi a mi véleményünket is, a hetet zárni pedig pedig egy szomorkás hangulatú Clueley idézettel fogjuk: "When will the day come when access to our data is considered to be an assault unless it's a consensual act? Not today."**



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3391845>

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](#).



[gothmog 2011.11.19. 12:36:21](#)

Kattintani könnyű. Gondó'kodni nehéz.

[NextGeneration 2011.11.21. 07:50:22](#)

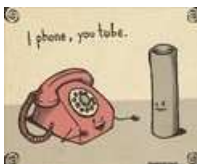
Azért az ssid-s részt egy kicsit keménynek tartom. Amúgy is broadcastolják az ssid-t, így az legalább hasznos is a köznek.

Email a YouTube-tól. Vagy mégsem?

2011.11.21. 14:25 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam youtube vagy phishing mégsem](#)

Kaptunk már korábban "[hivatalos](#)" levelet a Facebooktól, miszerint olvasatlan üzenetünk van. Majd [kaptunk a Twittertől, hogy fent van rólunk](#) pár funny pics. Aztán [végül az iTunes is küldött egy kis account infót](#). Vagy mégsem rovatunkban akkor most folytatjuk ezt a korábban megkezdett sort: **ezúttal a YouTube tájékoztat bennünket szomorúan: nem sikerült elküldeni korábbi üzenetünket, és mellesleg meg is haladtuk az egy napra engedélyezett levélküldési kvótánkat.**



Ezt egy hivatalos YouTube logó és egy valóban a YouTube oldalra mutató link is igyekszik bennünk megerősíteni. Bár egyáltalán nem emlékszünk arra, hogy korábban egyáltalán próbálkoztunk volna levélírással, mindig öröm és megtiszteltetés, ha az üzemeltető személyes levelével érdemesít minket kitüntetett figyelmére;-) Vagy mégsem?



Szinte nem is kéne már mondani, de mint az kiválóan látható is, **a második link, amely erre a bizonyos nekünk szóló üzenetről szólna, már egy egészen máshová mutató URL-je van.** Úriember ilyenre nem kattint, és segítheti még a védekezést többek közt valamilyen spamszűrő is, amely például már nálunk is felcímkézte ezt a küldeményt.



Dolgozik, illetve **kiegészítő formájában választható** a Thunderbird alatt is olyan, a gyanús üzenetek szűrésére szolgáló mechanizmus, amely például remekül figyelmeztet. **A hivatkozott linken mi már nem találtunk semmilyen hasznos vagy káros tartalmat**, maga a weboldal sem üzemelt éppen, hogy mi volt itt, az is csak a cache-ből látszik, így ezt a részét a dolognak nem tudtuk vizsgálni.



Láthatóan a létező, sok felhasználót kiszolgáló szolgáltatások a kiszemelt feladói ezeknek az újabb spameknek, adathalász kísérleteknek. Vagyis megint csak arra a tanulságra juthatunk, **mindenkinek meg kell tanulnia, hogyan különböztesse meg az igazi szolgáltatói üzeneteket a valótlantól**, ne higgyünk el mindent, és legfőképp figyelmesen kattintgassunk [ne csak a Patrick Chantól](#), hanem **a világ bármely tájáról érkezett kéretlen levelek esetében is.**



 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  2  Tweet

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [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/3400977>

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.

Tippek személyiséglopás ellen

2011.11.23. 13:00 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

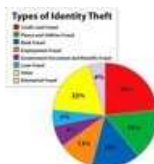
Címkék: [tippek](#) [identity theft](#) [védekezés](#) [személyiséglopás](#)

Incidensekről már számoltunk be korábban is néhány alkalommal, akkor jobbra [az érdekesebb eseteket emeltük ki](#). Most úgy gondoltuk, ideje **pár szóban a védekezés hogyan-járól** is megemlékezni.



Közelednek az ünnepek, jön az online vásárlások célegyenesé, [nézzünk hát pár ökölszabályt, tudnivalót, érdekességet, hogy elkerüljük](#) a személyes adataink illetéktelen kezébe kerülését.

Ha **vásárolunk az interneten, akkor ezt ne nyilvános wifin** kövessük el. Nem minden weboldal képes https-es belépésre, [és még ennél is kevesebb tart a kilépés végéig folyamatosan titkosított kapcsolatban](#).



Ha bankkártyával fizetünk, **takarjuk le a kezünket a PIN kód megadásakor**. Ezt se kifigyelni, se lefotózni, videóra venni ne lehessen könnyedén. **Haladócsoporthoz paranoidok előnyben részesíthetik a fémgombos billentyűzetet a műanyaggal szemben**, ott ugyanis [kevésbé lehet hőkamerás módszerrel leolvasni a begépelés utáni](#) másodpercekben.

Vigyázzunk a hivatalosnak látszó kéretlen emailekkel, küldje ezt akárki. Az rendben van, hogy védekezünk különféle programokkal, de az emberi tényező akkor is fontos, nekünk is óvatosságnak kell lenni. Ha csak egy csöpp **kétség van, ne válaszoljunk, például személyes adatok email-es bekérése nem szokványos eljárás**. Itt a jelszavunk kb. ez lehet: ["Cybersecurity is everyone's job, not just that of the CIO or security specialist"](#)



Amikor a legjobb vételre vadászunk, azért ne csak és kizárólag az ár döntsön, hanem a megbízhatóság is játsszon bele az összhangzatba. Nyilván a lopott vagy hamis áruk orgazdájánál nincs numerikusan alacsonyabb ár, de [senki nem akar egy zsák krumplit kapni előre átutalt pénze fejében mondjuk noteszgép helyett](#). **A bankkártya adat - elektronikus fizetésnél ugye a háromjegyű ellenőrző kóddal együtt - egy azonnal megterhelhető forintsítható személyes információ, amit csalóknak biztosan nem akarunk megadni**. Ahogy a kötelező biztosítás átkötésnél is keressük ugyan az alacsony ajánlatot, de nem minden áron. A korábban sosem hallott ismeretlen Első Magyar Ungabunga és Macska Johnny Biztosító Bt. ajánlatára nem csapunk le azonnal, hanem inkább másik létező, legitim, elérhető, irodákkal is rendelkező, valamennyire ismert céget választunk, aki még így is jobb árat mond a korábbiánál. Ez **akkor lehet érdekes, ha bármi esemény történik, és biztosan tudunk majd hova fordulni**.



Folyamatosan kísérjük figyelemmel számlánkat, egyenlegünket. Ha érthetetlen, ismeretlen tranzakciók jelennek meg, **akár kis összegről is, haladéktalanul lépünk kapcsolatba a bankunkkal**. Például szokás a lopott bankkártyákat úgy ellenőrizni, hogy 20 eurocentet átutalnak a Vöröskeresztnek. Ha sikerül, működőképesnek jelölik a kártya adatot, így többet lehet majd érte kérni a feketepiacon mint a kipróbálatlanért.



Minden internetes helyszínen használjunk egyedi és erős jelszót. Ezt a témát nem győzzük elégszer hangsúlyozni, mert a feltörések

jelentős részében nem ultra bonyolult varázskártevő a felelős, hanem [a fantáziátlan és vérprimitív jelszóválasztási szokások egyfajta mixtura pectoralis a felhasználói lustasággal](#).

Mind a számítógép operációs rendszerét, mint pedig az alkalmazói programjainkat - különös tekintettel az internetes böngészőre - [tartsuk frissen, a megjelenő biztonsági javításokat futtassuk mihamarabb](#), hogy a sebezhetőségek útját ezzel is bezárjuk.



És persze **a naprakész vírusirtót se felejtjük ki** a fenti sorból, hiszen a kártékony kódokat, URL-eket szintén segítenek észlelni, ellenőrizni, blokkolni.



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3405631>

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.

Hálaadás itt, iTunes ajándékutalvány ott

2011.11.25. 13:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [itunes](#) [csalás](#) [trójai](#) [utalvány](#) [backdoor](#) [kémprogram](#) [hálaadás](#)

[November negyedik csütörtöke](#) idén sem kerülhette el sorsát, és élelmes csalók felhasználták az alkalmat, hogy hamis iTunes Store ajándékutalványokkal trükközzenek.



A kéretlen e-mailben érkező "iTunes Gift Certificate" tárgyú üzenet egy fájl melléklettel érkezik, amiben állítólag az egyedi azonosító kód van. Ez okos gondolat a kártevőterjesztők részéről, ezért már sokan kattinthatnak az 50 dolláros ajándékot ígérő [EXE-ben érkező kártevőre](#), nehogy a hálaadás ünnepét követő vásárolgatási világnapot - az úgynevezett Black Fridayt - a végén még véletlenül lekéssék.



Ezzel a szokásos beárazást is követik, a [mai árfolyamon számolt, nagyjából 11,809.- forintnak megfelelő összeg](#) nem túl nagy ahhoz, hogy elriasszon és gyanúsán hihetetlen legyen, de a jelek szerint elég nagy ahhoz, hogy már vásárlásra csábítson.



Ha bár a feladó látszólag hivatalos, ez még a nevében is ott fityeg: "official@itunes.apple.com", mégsem lesz belőle kedvezményes árfekvésű vásárlás, csak fekete péntek, esetleg fekete szombat vagy vasárnap - kinek mikor fertőzi meg a backdoor a számítógépét. [Nem ez az első iTunesos csalás](#), és nyilvánvalóan nem is ez az utolsó. A vonzó termékek tökéletesen lettek kiválasztva, hiszen a felmérések szerint [az amerikai gyerekek 44%-a pontosan Apple-cuccokat szeretne](#) kapni karácsonyra.



Sok víznek kell még a Missourin lefolyni ahhoz, hogy a kéretlen ZIP, EXE mellékletes "pénzt kapok ajándékba ingyen" e-mail módszer kevésbé homályosítsa el a felhasználói tisztánlátást a kuponok országban. Azt viszont földrajzi elhelyezkedéstől függetlenül mindenesetre érdemes kiemelni, hogy a közelgő karácsonyi ünnepek miatt még rengeteg hasonló "akció", és [megannyi tündibündi elektronikus üdvözlőlap](#) várható, ezért nem árt résen lenni.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [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/3410467>

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.

Ne telepítsd a Christmas Tree App-ot!

2011.11.28. 15:25 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [hoax](#) [facebook](#) [christmas](#) [üzenet](#) [tree](#) [app](#) [trojan](#)

Ahogy David Harley fogalmaz: **egy jó hoax sosem hal ki**. Ami egyszer már bejárta Európát, az változatlan vagy modernizált formában rendre visszatér, új áldozatokat keresve. Most éppen ismét **arra intenek minket, hogy bár Advent már a kertek alatt, nehozz telepítsük a Christmas Tree App-ot a Facebookon**.



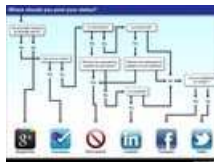
Szinte biztosan állíthatjuk, a "tudd meg ki nézegeti legtöbbet az adatlapodat" csalás sosem fog kihalni, ám az ilyen oszlopos tagok mellett vannak tisztességes idénymunkások is, **akik állandó alkalmazotti státusz híján csak a megfelelő időszakra várnak, hogy ismét előbújhassanak rejtekükből**. Három napnyira decembertől **el is jött ez a most a "WARNING!!!!!!.....DO NOT USE THE Christmas tree app. on Facebook" számára**. Ígérjük, nem fogjuk telepíteni, mert nincs ilyen, ám a **nemvalós álhír** tömeges és felesleges **továbbküldözgetése már elérhet olyan szintre**, hogy a napi Facebook **üzenetforgalom jelentős hányadát elérje**.



Mit tegyünk, ha ezt látjuk egy levélben vagy egy üzenetben: "Please re-post and let your friends know". **Ehhez kukkantsunk bele egy 1998-as "Lánclevelek küldőinek tanfolyama" című örökzöld Grin mesébe**. Szinte azt mondhatjuk, **a jelentős mennyiségű eltelt idő dacára mit sem vesztek ezek az információk a fényükből**, legfeljebb azóta kevesebb számú klasszikus emailt és több facebook üzenetet kapunk kézhez. Nem löjük le a poént azok előtt, **akik eléggé el nem ítélték módon esetleg nem ismerik ezt a klasszikus műveltség alapját képező művet**, az időtálló lényegét azonban mintegy doktor Bubóként kiemeljük: **Gondolkozzunk el minden ilyen üzeneteken, mielőtt bármit is tennénk**.



Ha valamilyen rejtélyes okból kifolyólag mégis abszolút hitelesnek és nyilvánvalóan hihetőnek tartanánk a *"ha továbbküldöd 13 ismerősödnél 3 napon belül akkor téged nagy szerencse fog érni"* kezdetű szöveget, **legalább az üzenet címére, tartalmára keressünk rá mégis az interneten, hátha** egy visszajáró lélek szorgalmával kísértő csaló levélről van szó. Ezzel megspóroljuk ismerőseink szükségtelen megspamelését és erkölcsi tekintélyünk sem csorbul általa.



Elképesztő módon az álhírek tényleg nem halnak ki véglegesen, **rövidebb-hosszabb szünetekkel rendre újra előbukkannak**. Ismerősöktől befutott például hétvégén **az a 2006 óta terjedő levél**, melyben azt állítják, hogy **ha erőszakkal kényszerítenének bennünket pénzfelvételre ATM-ből, akkor állítólag nincs más teendőnk, mint szándékosan fordított sorrendben begépelni a PIN-kódunkat**, ezzel máris értesítjük a rendőrséget. **Rossz hír, de nem**, ez egyáltalán nincs így, fordított sorrendű, négyzetgyököt vont vagy logaritmusra emelt - rövid szóhasználatlaltal csak helytelen - kód esetén nem jön a rendőrség, csak egy gépi üzenet, hogy hibás a bevitt PIN-kód.



Röviden összefoglalva, ha valaki ilyesfajta értesítést kap, amelyben a "küldd tovább minden ismerősödnek" panel is szerepel, ne higgye el, ne kattintson, ne továbbítsa, ne bombázza meg vele barátait. Ellenben ahogy egy Elvirán kikeressük a menetrendből a vonatunkat, kétség esetén Googlizzuk ki az adott csalást, és 99.99% eséllyel meg is találjuk azokat az angol Hoax Slayer vagy [a magyar nyelvű Urban Legends oldalakon](#). Ahol sok érdekes hasonló csalási esetet is találunk, szóval ha valaki szeret olvasgatni, kihagyhatatlan, és szerfelett tanulságos.



Ha pedig igazi csalásba botlunk, **jelenthetjük közvetlenül a Facebook üzemeltetőknek, amikor pedig bármilyen Facebook alkalmazást vizsgálunk, tartsuk észben, hogy ezek telepítése vagy használata hozzáférhet személyes adatainkhoz, barátaink listájához, ezért csakis olyat telepítsünk, amiben teljes mértékben megbízunk.**

 Tetszik  95 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 4  Tweet

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Ez történik a weben egy perc alatt](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3418493>

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.

No More Mr. Nice Guy

2011.11.30. 13:30 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [adatvédelem](#) [privacy](#) [facebook](#) [ftc](#)

Énekelte Alice Cooper a hetvenes években a Billion Dollar Babies című bakelit albumon, amire ma már csak idősebbek és katonaviseltek emlékezhetnek. Bár ez a felvétel [még fellelhető például a Youtube rejtett bugyraiban](#), megtekintését azonban Southparkosan fogalmazva **semmilyen korosztálynak nem ajánljuk;-)** Apropos mindennek pedig az, hogy hihetetlen módon **sikerült fogást venni a Facebook elfajzott adatvédelmi gyakorlatán**, amire eddig szűkkeblűen mindig úgy tekintettünk, mint eleve reménytelen és soha meg nem valósuló célra. Egészen tegnapig.



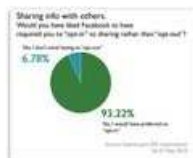
A helyzet röviden: alapértelmezetten mindent megosztunk, nekünk kell letiltani, amit nem akarunk, ehhez [nehezen kezelhető és bonyolult biztonsági beállításokat kell használni](#), a felület és/vagy a felhasználói szerződés változásakor pedig korábbi beállításaink előzetes figyelmeztetés nélkül meg is változhatnak. Idézzünk pár [fontosabb tételt a teljesség igénye nélkül az FTC panaszlistájáról](#).



- 2009. decemberében a Facebook megváltoztatta a honlapját, így bizonyos információk, például a barátok listája - nyilvánosságra kerülhetett. Nem figyelmeztették erre a felhasználókat, hogy ilyen változás jön, és nem is kértek ehhez előzetes jóváhagyást.

- a Facebook korábban azt hangoztatta, a telepített applikációk "csak annyi felhasználói adathoz férnek hozzá, amennyi a működésükhöz elengedhetetlenül szükséges". Ezzel szemben tény, hogy az alkalmazások elérhetik szinte minden felhasználó személyes adatait, bár a működésükhöz ezek egyáltalán nem szükségesek.

- A Facebook azt állította, a felhasználók korlátozhatják az adatmegosztást a "Friends Only", azaz csak ismerősöknek beállítással. Ezzel szemben tény, hogy third party alkalmazások ehhez mégis hozzáférhetnek.



- A Facebook azt állította, a "Verified Apps" címkével ellátott programokban bízhatunk, az biztonsági szempontból ellenőrzött és hiteles. Ezzel szemben tény, hogy ez mégsem volt így.

- A Facebook azt állította, nem osztja meg hirdetőkké az adatainkat. Ezzel szemben tény, hogy megtette, és nem is egyszer.



Nem soroljuk tovább, egy szó, mint száz - az FTC, azaz a U.S. Federal Trade Commission döntése alapján mostantól [látszólag megvan, ki mentheti meg Ryan facebookozót](#). Ha mindez megvalósul, akkor [a jövőben nem adhatják el többé titokban és orvul hirdetőknél a személyes adatainkat, az vet végét az idióta applikációk ámokfutásának](#), akinek [ez a feladata: maga az üzemeltető](#), és nem fordul elő többet, hogy a felhasználói beállítások váratlan megváltozása ismét tömegesen kellemetlen helyzetben hozza a felhasználókat.



Megszűnhet hát végre a kaotika, [melynek jellemzésére anno Atko kolléga a következőt](#) írta: "Az uszodában ki van írva: 'mely víz csak úszóknak!' és mellette van úszómester is! Egy közösségi oldal meg olyan, mintha hivatalosan engedélyezné a strandolást a Niagarában. Aztán ha valaki hamis mentőövvel vagy lyukas csónakkal kereskedik, vonogatják a vállukat és a firdőzőkre mutogatnak."



Egy ősi Murphy törvény szerint a politikusok (állítólag) tudnak logikusan és helyesen is dönteni, de csak ha előtte már minden egyéb lehetőséget is kimerítettek. Most **úgy tűnik, vége lehet a korábbi felelőtlen tobzódásnak, és kedvenc mondatunkkal zárjuk a mai posztot:** "Facebook is prevented from misrepresenting users' privacy or security; is required to get "express consent" before altering users' privacy preferences; must prevent access to deleted account material after 30 days; will agree to establish and maintain a privacy program; **and will submit to a bi-annual privacy review for the next 20 years"**. Megyek koccintani Clueley-val ;-)



118 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Ez történik a weben egy perc alatt](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3425363>

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](#).



TrueY • <http://qltura.blog.hu> 2011.12.01. 14:32:00

Ez pénzről és nem a privacy-ról szól! Naná, hogy kiadja az emberek adatait! Így jár, aki gyalog...

Új Facebook féreg terjed

2011.12.01. 18:43 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [facebook](#) [malware](#) [koktél](#) [peter](#) [féreg](#) [kruse](#) [cockail](#)

Ilyen címmel manapság már nem is érdemes posztot írni, Index címlapra talán csak valamiféle "Óriási szenzáció, ma nem terjedt semmilyen féreg a Facebookon" szalagcím predesztinálhatna. Hacsak az illető kártevőnek nincs valami különleges tulajdonsága. Nos akkor szerencsére rendben vagyunk, mert van neki.



Dán kutatók észlelték először azt a Facebookon terjedő férget, amely [az adott felhasználó nevében bejelentkezve spam üzeneteket küld a barátoknak, ismerősöknek](#). A továbbított üzenet mindössze egy URL-t tartalmaz, amely egy izraeli szerverre mutató link.



Erre a linkre kattintva a felhasználók a mellékelt képet látják, ami **látszólag egy képernyővédő (screensaver)**. Letöltése és futtatása **azonban nem javasolt, mert kártékony kódot tartalmaz**. A kártevőt Visual Basic 6.0 segítségével készítették, és az elemzések szerint számos visszafejtés elleni trükköt tartalmaz, például érzékeli az elemzéskor használt virtuális környezeteket, mint amilyen a VMware, Sandboxie vagy a VirtualBox. És itt következik a beharangozóban emlegetett érdekesség: **az elemzés szerint a kártevő még egy sereg további kártékony kódot hoz létre a fertőzött gépen, vagy ahogy Peter Kruse biztonsági szakértő fogalmaz: egy komplett malware koktélt igyekszik elhelyezni**. Ezek között leginkább az adatlopó Zeus trójai lehet a legismertebb és egyben a legveszélyesebb.



Bár [a VirusTotal riportja szerint eleinte nem volt teljes a mezőny felismerése](#), David Harley blogjában rámutatott, [az ESET programja már a kezdeti időszakban is sikeresen detektálta azt a proaktív felismerés segítségével](#) Win32/Injector.LML néven. Mostanra pedig a konkrét minta elemzése végeztével Win32/TrojanDownloader.Small.PFD néven került bele a NOD32 vírusadatbázisba.



Ennek is lehet örülni, de ami még ugyanilyen fontos lehet a jövőben, hogy a **semmilyen kísérő szöveget, hanem csak csupasz linket tartalmazó üzeneteket soha ne nyissuk meg**. De ugyanerre az óvatosságra van szükség akkor is, ha a kéréten üzenetben "Hey dude, check this out", "98 Percent of People Cant Watch This Video" és hasonló tipikus beugrató szöveget lehet olvasni. **Letöltéseinket - még a képernyővédőt is - kizárólag megbízható helyről intézzük**, és magunk közt szólva egy kéréten üzenetben, kísérőszövegnélküli URL-ben érkezett screensaver semmilyen szempontból nem tekinthető megbízható forrásnak, ezért legyünk tehát mindig gyanakvóak, alaposak és óvatosak.

Tetszik 817 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Ez történik a weben egy perc alatt](#)
- [Küldj pénzt! - Az elvesztett poggyász sztori](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/3429643

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.

Anyu, hogy lett Apuból egy zombi?

2011.12.05. 14:20 | [Csizmazia István \[Rambol\]](#) | [4 komment](#)

Címkék: [zombi](#) [botnet](#) [botmaster](#) [infografika](#)

Rendhagyó módon ma az "egy kép többet mond ezer szónál" szlogen jegyében **egy infografikát** mutatunk be egy olyan témáról, amit korábban [ezernél is több szóban már sokszor tollhegyre tűztünk](#): **hogyan fertőzik meg a számítógépünket és hogyan leszünk egy botnet része.**



Következzen hát akkor az ígért infografika, ha kedvelt lesz, akkor esetleg csinálunk majd talán máskor is hasonlót.



Tetszik 12 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3438774>

Kommentek:

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



**[A Hannibal Lektúr-attitúd](http://hannibal.blog.hu/) • <http://hannibal.blog.hu/>
[2011.12.05. 14:33:02](#)**

klassz



[Robina](#) [2011.12.06. 09:30:28](#)

Nekem tetszik :)

[cworm](#) [2011.12.06. 16:47:52](#)

Ez az anya-gyerek párbeszéd helyenként elég sületlenségeket tartalmaz. Pl mi az, hogy a zombik sok pénzt tudnak keresni? És hogy ezért van sok belőlük? Nem a zombik keresik a pénzt, hanem a "bot mester". Azt is megkérdezi a gyerek, hogy akkor apu írja a szemétleveleket? De nincs rá válasz (mondjuk gondolom mindenki tudja, hogy nem, de akkor is, ebben a beszélgetésben többször is ignorálják egymás mondanivalóját a szereplők). Honnan jön a Superman Hacker és mit jelent?



**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
[2011.12.07. 10:10:59](#)**

Szia Cworm!

Nyilván mi már mosolygunk az ilyeneken, de remélhetőleg sok átlagfelhasználónak az ilyen szájbarágósdí meg jól célbajuttatja az üzenetet, hiszen végül is ők a potenciális kattintók.

Hát mivel hozott anyagból folyt a munka, még így is azt mondom, hogy jobb lett, mint az eredeti ;-)

www.infographicsarchive.com/tech-and-gadgets/how-my-pc-became-a-zombie/

Ki innen letöltesz, hagyj fel minden reménnyel!

2011.12.07. 10:40 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [reklám](#) [letöltés](#) [cnet](#) [trójai](#) [nmap](#) [wrapper](#) [optout](#)

Vagy valami hasonló lehetne a szlogenje mostani történetünknek, amely arra a szálra igyekszik egy újabb gyöngyöt felfűzni, amelyen [már több ízben boncolgattuk a főállású letöltési oldalak hibáit, hiányosságait, mulasztásait](#). Ezúttal már kicsit többről van szó: **maga a Cnet csomagol mindenféle kétes, nehezen kikapcsolható kérértlen reklám és trójai tartalmakat az egyébként tiszta szoftverekhez.**



Ha van, aki számítógépes létére esetleg [nem tudja mi az nmap](#), az megvilágosodása érdekében sürgősen [vonuljon el a nagyvilágtól, kilenc éven át meditáljon egy barlang falával szemben ülve és közben hallgassa a hangyák beszédét](#) ;-)



Szóval az nmap fejlesztője, Fjodor mester vette észre, hogy [a Cnetes letöltésekkel valami gubanc van, saját programját onnan letöltve "esemény van", beletomogolnak valamiket, amit nem kéne](#). Erről többek közt Clueley blogjában is olvashattunk, **mindenféle Startnow Toolbar, Babylon Toolbar és egyéb nemkívánatos hulladékok települnek, ha valaki nem elég szemfüles, hogy az alapértelmezett "Igen, kérem, sőt követelem telepíteni ide nekem a sok trágárt" mellől kivége a pipát.**



A "halál vagy ungabunga" kérdésre nem véletlenül mondják a viccben, hogy "akkor inkább a halál", mert senki sem szereti, ha erre "na jó, de előtte egy kis ungabunga" a válasz. Ebben a helyzetben ugye **az is egy kellemetlen mellékhatás, hogy a sok haszontalan toolbar láttán az emberek mindezt a letöltött szoftverrel - a példánkban az nmap-pel - kötik össze, és ennek a renomóját rontja, [máskor nem fogja letölteni, mert nem akar szeméthalmazt látni](#) a hagyományos böngésző ablak helyett.**



Idősebbek és katonaviseltek még emlékezhetnek, amikor a békebeli C64 játékok elindítása nem közvetlenül a játékot futtatta, hanem előtte még egy rakás kitömörítő és kérértlen képernyőüzenetet kellett kivárni, végignyomkodni (Cracked Anno Domini by SatanSoft, greetz ennek, sucks amannak), a kurzor bal-felső villogása és a karakterek pörgése mellett, hogy aztán a felejthetetlen "Sándor ima uvek novo programme" üzenetről ne is beszéljünk. Ilyet pedig nem akar senki, a baaableves legyen baaableves, ez a tiszta helyzet.



Csak egy apró mellékszál, valószínűleg most is [sikerül majd sok embert kattintásra bírni, ha várhatóan majd beindul a "mindenki ingyenes CarrierIQ detector programot kínál" biznisz](#). Már nem a Rolex óra, nem a Viagra, hanem **várhatóan ez lesz a jó csali, és jönnek majd seregestül a spamek, adathalász cuccok, trójaiak, kártevők.**



Visszatérve nem csak az okostelefonos, hanem a PC-s, vagy inkább **minden típusú letöltésre: előbb-utóbb mindenkinek meg kell tanulni, hogy alkalmazást letölteni közvetlenül a gyártótól, fejlesztőtől, appstoreból, etc. a legmegbízhatóbb.** Ha már további partnerek partnereinek partnerei aggregálják sokadiziglen a tartalmakat, akkor vagy nem kell onnan letölteni, **vagy jóval nagyobb figyelem szükséges mind a vírusellenőrzésnél, mind pedig az elolvasás nélkül kapkodva elvégzett next-next-finish nevű nemzeti sport esetén.**



3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3445021>

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.

Egy adathalász támadás anatómiája

2011.12.09. 15:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [eset adathalászat infografika](#)

Folytatjuk előzőleg [megkezdett infografikás sorozatunkat](#), mai epizódunkban azt mutatjuk be, milyen egy [klasszikus adathalász akció](#) forgatókönyve, milyen fő- és mellékhatással járhat egy ilyen a felhasználó adataira nézve.



Bár az eltelt pár napban - érthetetlen módon - nem telt meg a postaládánk további infografikákat követelő olvasói levelek garmadjával ;-), pár apró biztatást, szórványos tetszésnyilvánítást azért sikerült kiérdemelnünk, így hát az **abszolút alkalmi jellegű folytatás** ösvényére lépünk. Ha valaki az előző rész alapján tévesen azt gondolta volna, az ESET-nek nincs ilyesmije, vastagon tévedett. Egész rövid keresgélés után **az édesvízi adathalászat rejtelseiről szóló** tetszetős illusztrált szájbarágóra bukkantunk, ezt mutatjuk be ma. De a jövőben tudatosan **igyekszünk majd az ESET összes hasonló anyagát is egybegyűjteni**, mert nekünk tetszenek az ilyen szemléletes, közérthető tematikus összefoglalók, illetve demonstrative hasznosnak gondoljuk. Ahogy Öveges professzor fogalmazta: **"nincsenek nehéz és könnyű dolgok, csak megértettek és meg nem értettek vannak"**, és talán az ilyen ábrák is segíthetnek ebben.



Ha valaki sajátkezűleg is közelebbi barátságot akar kötni az infografikákkal, annak az alábbi [Bluewheelmedias összefoglaló](#) segíthet, melynek végén még egy hosszú listát is kapunk a **használatos segédeszközök tekintetében**. Ha pedig megkérdezzük orvosunkat, gyógyszerészünket, az egyik potenciális jelölt lehet a [multiplatformos, azaz Windows, Mac és Linux alatt egyaránt elérhető vektoros Inkscape szoftver, amely ráadásul nyíltforráskódú és ingyenes](#) is.



Nem zárható ki, hogy néha majd saját kútöböl is eszkábálunk össze ilyeneket, és ezt a blogolvasók nyugodtan vehetik fenyegetésnek! ;-)
Addig is bátran - akár témakör szerint is - lehet turkálni a [korábbi infografikák archívumában](#), illetve akinek kedve van, szabad próbálkozni az ismertetett készítő eszközökkel.



8 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/3450499

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.

Szavazz rám!

2011.12.12. 15:30 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [indián facebook előre adathalász lájk](#)

Válassz meg, jobban jársz velem! Indián-e vagy? Szabad-e lájkolni, amíg nem tudjuk, kire tesszük? - ez a központi kérdés áll a figyelem homlokterében. Szerintünk: semmiképpen."



Ha nincs arcod, használd az enyémet" - mondja az Európa Kiadó, illetve "Én úgy vagyok szép, ahogy az neked jó" - ismétlődik a panel [az örökbecsű "Szavazz rám" című számban](#), és a hiszékenységgel együtt úgy tűnik mindkét oldalon túl sok szabad ideje van. **A csalóknak telik sok szép csalit építeni, az unatkozó számítógépfelhasználóknak pedig megtudni az indián nevüket, kielégíteni a kíváncsiságukat, hátha éppen ők lesznek azok, akik 17 helyett 18 másodpercig tudnak nézni egy inkriminált videót.**



Be kell látni, egyszerűen **nem járható az az egybites út sem, ami arra korlátozódik, hogy csak ha egy konkrét weboldalon kiírják : "Ember! Ne kattints az indián névre", "Hé! Ne kattints a cowboy névre", akkor vigyázok csak és kizárólag**, ám ha valami még nem szerepel ezen a figyelmeztetés listán, akkor viszont kattintgatom a sablonosan ismétlődő régi-újakat gondolkodás nélkül.



A gyanakvásnak, az óvatosságnak mindenki fejében ott a helye a "minden marhaságra rákattintok" rendező elv helyett. Ma úgy látszik Demotiválás és Európa Kiadás napot tartunk egyszerre, így további ontopik zenei idézet következik: ["Veszélyes vagy magadra, de ez csak a szokás hatalma, senki nincs veled, se ellened, félre érted a helyzetet".](#)



Jó lenne, ha mi a továbbiakban nem értenénk félre a helyzetet, és nem lennénk veszélyesek magunkra. Egyik kommentelőnk találó szavai lehetnének az iránymutatók ebben a kérdésben mindenki számára: **"már nem kattintok sehol sem, ahol előbb lájkoltatni akarnak és csak utána adni a tartalmat. A LÁJK-om fontos nekem, nem szórom el csak úgy a világba".**



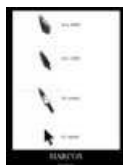
Ha kicsit körbenézünk, [mit írtak erről az indián neves dologról](#), a magyarinfo oldalról érdemes beidézni a válogatott főlényeket: **"A Facebookon terjedő Mi az indián neved? alkalmazás, egy ügyesen álcázott adathalász eszköz. Ha megnyomod a belegyezés gombot az alkalmazás futtatására egy ékszerüzlet hozzájuthat személyes adataidhoz, és csatlakoznod kellett a Facebook oldalához, promócióhoz kötötte az alkalmazását. Így lett egy egyszerű ékszer üzletnek 730 ezer rajongója a facebookon, és lett ezzel Magyarország legnagyobb cége a Facebookon."**



Az ellenvélemények szerint azonban: "Viszont ha nagyra nő ez a hiszti, Magyarországon ellehetetlenül a közösségi marketing, a vállalkozások még hamarabb tönkremennek, és az ország előbb csődöl be. Nos ezzel fizetünk a hisztis média reakciókért." □ **i ebben a látatlan, vabank rendszerben magunk részéről nem hiszünk, ha a "nem tudom ki, nem tudom mire használja az adataimat, és nem tudom mit fog nekem mutatni, de én előtte azért jól lájkoljam őt", hát részünkről no never, és absolutely no way.**



Abban sem hiszünk, hogy a magyarországi gazdasági felvirágzás és a közösségi marketing fényes jövője és életben maradása ezen a becsapós, zsákbamacska szisztémájú előrelájkolás rendszerén állna vagy bukna. Szerintünk remek ellenpélda erre az ESET facebook.com/biztonsag oldala, ahol előbb mindenki megnézheti, miről van itt nagyba szó, aztán ha elolvasta, végignézte és tetszik neki, amit lát, akkor ezután lájkolja őket, ha akarja, ha hasznosnak gondolja.



És ha logikai eszmefuttatásként a "mi volt előbb: tyúk vagy tojás" problematikát nézzük, abban mi a magunk részéről a tojásra voksolunk: lásd dinók, akik ugye tojásból keltek ki ;-) Azonban ha ugyanez a gondolat kísérlet úgy vetődik fel, **"mi legyen előbb: lájk vagy megismerés", ebben a rendíthetetlen ólomkatona álhatatosságával úgy gondoljuk, látatlanban senkinek semmit sehova.** Mindenkinek meg kellene tanulnia már ezt a leckét, mert minden lájk mellé továbbra sem lehet külön közlekedési rendőrt állítani...



Mindazonáltal kíváncsiak lennénk, hányan lépnének előbb házasságra egy lefátyolozott idegennel - mondjuk a fenti kevésbé foglalkoztatott bébiszitterek közül, és majd csak utána kukkantanának a fátyol mögé, ki is lett életük párja, míg a halál el nem választ. Szóval visszatérve a **Facebook lájk logikus sorrendjére mondhatjuk: 1. előbb megnézem, mi az; 2. aztán vagy tetszik vagy sem, utána szabadon döntöm el - ez lenne a normális.**



409 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

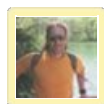
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3457209>

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>
[2011.12.12. 18:40:15](#)

Hát szomorúan látom, az eseményről hírt adó cikkekben egyedül maradtam a negatív véleményemmel, így akkor mosz beidézek egy-két érdekesebb kommentet.

www.origo.hu/techbazis/20111212-indian-neveket-kinal-a-legnepszerubb-magyar-facebookos-alkalmazas.html

"Az egyetlen különbség a Túró Rudi és az ékszerbolt facebookos jelenléte között, hogy míg az édességért rajongók közvetlenül a Rudi oldalán nyomták meg a lájkgombot, addig az ékszerrajongók csak az indián nevüket akarták megtudni"

onlinemarketing.blog.hu/2011/12/11/pukkadjatok_meg#comments

"Azzal nehéz vitatkozni, hogy a Facebookon az alkalmazások egyre átbaszósabbak. Ez a mostani hullám (ami talán az utazom.com-mal kezdődött) nekem egy új mélység. Ha a hőbörgő szakmánál te csak a likemaksimalizálók céhére gondoltál, akkor rendben, én értettem félre, hogy kit értesz szakma alatt.

...

Ez nem marketing, ez ügyeskedés."

Én azzal értek egyet, amit DeeJayy mond:

'miért nem jó ez a kampány? De hiszen leírtad:

"Igen, az emberi hiszékenységet használták ki, de ez maximum etikátlan."

"Lássuk be: a marketing nem az erkölcsösség és a finomkodás terepe."

Nekem ennyi bőven elég. Black Hat Marketing, szevasz. '

[vágtaázó halottkém 2011.12.17. 11:36:11](#)

Az emberek barmok.

Indiánok a Facebookon

2011.12.13. 18:15 | [Csizmazia István \[Rambol\]](#) | [20 komment](#)

Címkék: [indián facebook család előre láthatatlanban lájk](#)

Széles skálán mozogtak a reakciók a ["Mi az indián neved?" alkalmazás kapcsán](#). Sokan, és sokféle véleményt megfogalmaztak ezzel kapcsolatban, [a skálán az évszázad "legjobb marketing fogásától"](#) egészen a ["mocskos átverésig" terjedtek a hozzászólások a különböző fórumokon](#).



Érkeztek hozzánk is ezzel az indiános esettel kapcsolatban kérdések, észrevételek földön, vízen, levegőben, a tegnapiak dacára ezért járjuk most körbe ismételten ezeket a dolgokat.



Az ESET facebook.com/biztonsag oldalán mindenfajta Facebookos jelenségről, veszélyről rendszeresen beszámolunk, igyekszünk figyelmeztetni, erre is felhívtuk a figyelmet, és így fogunk tenni a jövőben is. Egy cikket linkeltünk be és abból idéztünk, így **attól fogva mindenki már az előzmények, tapasztalatok ismeretében szabadon eldönthette, megnézi-e az indián nevét a mellékhatások ismeretében**, csatlakozik-e. Mi biztos szívesebben döntenénk el így, ha pontosan ismerjük a kockázatokat és mellékhatásokat, mintha nem mondják meg előre.



Máskor sem, és ennél az indiános dolognál szintén abszolút nem számított, hogy magyar, angol, svéd vagy hottentotta cég készítette, hanem csak az, hogy ígért valamit (indián név), és ezt bár tényleg odaadta, de **emellett más is történt, csak a névre kíváncsi egyszerű felhasználó egyben a cég rajongójává is vált**, ezt ki is posztolta az üzenőfalára az ismerőseinek anélkül, hogy az "akarsz-e a xy ékszerbolt rajongója lenni" kérdést látta volna, arra igent felelt volna.



De vegyük úgy most egy pillanatra, hogy ez ne legyen probléma. Az alapvető gond ezzel, és minden más hasonlóval, ahol rejtett dolgokat **ELŐRE LÁJKOLNI KELL**, ahhoz, hogy egyáltalán megtudd, mi is az. Ez helytelen, és **a felhasználók biztonsága szempontjából veszélyes módszer, a kártékony linkek terjesztőinek tipikus eljárása**. Ha valakinek a szülei vagy a gyereke kíváncsi lenne a horoszkópjára, vagy mit kap idén karácsonyra, és kattintana egy előre lájkra, majd másnap azt látná, hogy ezzel tudtán kívül például a svéd nekrofilok társaságának kedvelője lett, emiatt ismerősei kinevetik, zaklatják - azt mondanánk, na ki tette ezt vele, megrángatjuk a grabancát.



A helyes ítéletet nagyban segíti, ha beleképzeljük magunkat a másik fél helyzetébe, és nem teszünk vele olyat, amit nem szeretnénk, ha velünk tennének. Hogy a fenti dolog meg is történhet, arra [itt egy példa, amikor is jó szándékú adománygyűjtői csoporthoz csatlakozók éppen erre ébredtek](#) a Facebookon egy reggel. És itt [egy teljesen másik antivirus cég véleménye a clickjacking-nek](#) nevezett módszerről. Ez azért veszélyes, mert tipikusan **csak a lájk után tudhatjuk meg, mire is lájkoltunk pontosan**.



Ebben az indiános történetben is tényleg lehet, hogy az ékszerészek jó szándékúak voltak, ezt készséggel elhisszük. **A felhasználóknak azonban mindenképpen tanulság lehet, érdemes-e egy vicces játék miatt hozzáférést engedni személyes adataikhoz és elérhetőségükhöz, engedélyt adni ahhoz, hogy a nevükben posztoljanak az üzenőfalukra.** Hogy egyébként mit lehet ilyenkor látni az átengedett adatainkból, azt [a BESOCIAL volt olyan kedves, és bemutatta egy konkrét alkalmazáson keresztül](#), ezt minden olvasónak jó szívvel ajánljuk figyelmébe.



Szintén az ő keze munkájukat dicséri a "[Hogyan rejts el szinte bármit magadról és másokról a Facebookon?](#)" című összefoglaló, hogy ne váljon az üzenőfalunk rémálommá az Elm utcában. De emellett ugye közismert, hogy **a nemkívánatos alkalmazások egyszerűen ki is törölhetőek az engedélyezett alkalmazások listájából.**



Mindenesetre a fő kérdésben továbbra is kitarunk a véleményünk mellett, **a látatlanban előre lájkolás egy olyan gyanús módszer, amitől az óvatos felhasználóknak mindenképpen érdemes tartózkodnia** - ez a mi álláspontunk, megszólalásunk, figyelmeztetésünk lényege. Válgon a vérünk, hogy **saját biztonságunk érdekében, ha csak a legkisebb kétségünk van, inkább ne kattintsunk.**



428 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



5

Tweet

• [1 trackback](#)



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3460924>

Trackbackek, pingbackek:

[Trackback: Válságos üzletindítás](#) 2011.12.14. 06:50:24

Válságos üzletindítás avagy lehet-e „biztosra” menni ma? Az üzlet szempontjából, mindig van bizonytalan időszak, bizonytalansági tényező. Egy nehéz gazdaság

Kommentek:

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



Konrad • <http://onlinemarketing.blog.hu> 2011.12.13.
21:12:22

Az oldal Like-olása semmilyen kockázattal nem jár, sőt, egy kattintással semmivé tehető. Az alkalmazás Like-olása valóban jár kockázatokkal, de arra ott a jelzés, mi történhet. És a Facebook elég jól beállítható, hogy nagy baj ne történjen. Ráadásul később az alkalmazással való kapcsolat is megszüntethető, itt se érzem a problémát.

Amit írtok, alapvetően igaz egy ismeretlen platformon, de a Facebook nem fenyeget se vírus, se adatlopás tekintetében (ha csak nem vagyunk annak tevőleges résztvevői a saját hülyeségünkkel). Pontosabban nem jobban, mint bármely weboldal, ami cookiet rak le. Szerintem.



rockseiaXLL • [http://nemfasza.blog.hu/ 2011.12.13. 22:31:34](http://nemfasza.blog.hu/2011.12.13.22:31:34)

nemfasza.blog.hu/2011/12/08/a_grazi_apolt_facebook_lapja

is 2011.12.14. 00:18:58

@Konrad: akkor küldenék neked két operajegyet adott dátumra. közben side-effectben az előadás alatt kirabolom a házad, de az operajegyet ígertem, és azt be is tartottam. összességében jól szórakoztál, ugye?



Konrad • [http://onlinemarketing.blog.hu 2011.12.14. 00:25:02](http://onlinemarketing.blog.hu/2011.12.14.00:25:02)

@is: Kifejezetten rossz példa. Feltételezi, hogy visszaéltek az átadott jogokkal, holott nem történt ilyen. Vagy igen? Tudtok valamit?

Ez egy álpara, elhiszem, hogy tanítani kell az embereket - sőt, ezzel egyet is értek -, de ebben az esetben azt hiszem jobbára információ hiány és félreértés miatt történik a riogatás.



DR.version • [http://m-12.blog.hu 2011.12.14. 01:11:05](http://m-12.blog.hu/2011.12.14.01:11:05)

jelöljétek meg spamkent, majd akkor talán a facebook kitiltja őket orokra

Komáromi Teréz Atya 2011.12.14. 04:21:52

@Konrad:

Bocs, most alpári leszek:

Minden cégnek a k..va anyját, amelyik tudtomon kívül reklámfelületet akar belőlem csinálni az ismerőseim felé. Nem elég, hogy a tv is nyomja az ízléstelen mocskos hazugságokat, már engem is erre akarnak kihasználni?

A facebook biztonsági beállításait meg hagyjuk. Valószínűleg azért cseszegeti az FTC, mert annyira jófej.

Komáromi Teréz Atya 2011.12.14. 05:55:30

@Komáromi Teréz Atya:

Meh, ez talán erős, volt, szerkeszt gomb meg nincs...



Csizmazia István [Rambo] • [http://antivirus.blog.hu 2011.12.14. 06:34:12](http://antivirus.blog.hu/2011.12.14.06:34:12)

Szia Atya!

Semmi gond, sok pontozás meg sok igazság volt abban amit írtál, és vannak időnként erős érzelmeink, szóval no problemo :-)

Az FTC-vel kapcsolatban majd azért arra is kíváncsi leszek, mennyire tartják be a dolgokat. Sok csoda tud ott a tengeren túlton történni, például egyik napról a másikra leáll az MS szétदारabolása, és hasonló. Félő, hogy két évente lesz egy plebsnek szánt ejnyebejnye, és minden marad a régiben.

Figyel Castro 2011.12.14. 08:17:41

@Komáromi Teréz Atya: Mielőtt megnevezhetné mindenki az indián, cigány, hottentotta, stb nevét, kap egy üzenetet, hogy a

cucc mikhez akar hozzáférni. Aki igent nyom, az innentől magára... Mondjuk az emberi hülyeség határtalan, amikor cigány nézi meg, hogy mi a cigány neve, mellesleg informatikus az illető, no comment...



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2011.12.14. 08:53:43

Blöki kolléga éppen a szívemből beszél a másik topikban, ezért idézni szeretnék:
onlinemarketing.blog.hu/2011/12/13/at_foglak_dobni_a_palankon_igen

"Viszont szerintem az a normális, hogy az alkalmazás már a likeolás előtt is (és utána is folyamatosan) kiírja, hogy mi fog történni, pl:

"A kvíz kitöltése után kapsz egy oklevelet/akármit ... Ez a kép a Facebook üzenőfalodon is megjelenik ismerőseid számára. Amennyiben ezt nem szeretnéd kérlek ne használd az alkalmazást!"

Ezek után nincs probléma és egyértelmű, hogy mi fog történni. "



Konrad • <http://onlinemarketing.blog.hu> 2011.12.14. 09:17:09

[@Komáromi Teréz Atya](#): Igen, és? Nem kell rákattintani, akkor nem fognak reklámnak használni. Miért, mit gondoltál, ingyen csinál valaki egy ilyen alkalmazást, csak úgy, passzióból?

Motyóbábi 2011.12.14. 09:57:05

Ha érkezik egy idétlen alkalmazásra felkérés (márpedig ugye a facebookon nemigen létezik normális alkalmazás... na meg nem is ezért van az oldal), azonnal letiltom. Nem kattintok rá, nem nézem meg, csak nyomom a mellőzést, majd a végleges tiltást. Ilyen egyszerű. Így aztán nincs tele az oldalam pálmákkal, meg kecskékkal, mint az elején, amiket valakitől kaptam, de miért is?

Csak katt a tiltásra, és nincs min rágódni.

(az indián nevem meg nem érdekel) :))

lupus78 2011.12.14. 10:01:44

Azt nem értem, hogy a Facebook miért nem törli és tiltja ki az ilyen appok üzemeltetőit azonnal? Nem nagy kérdés számukra, hogy valaki visszaélt az APIval... miért engedik a kamu lájkok gyűjtését... szánalmas

mim 2011.12.14. 10:11:10

Eccerű. Létrehozol egy kamu user-t. Pl. Gaamer Sündor. És egy külön böngészőn keresztül lépsz be, ha ilyenekkel akarsz foglalkozni.

Ezzel megkíméled ismerőseid és magadat is.

Persze a marketingesek (nincs adat és valós terjesztés) és a FB (hamis adatok) veszítenek rajta, de ezzel a kockázattal úgy is számoltak.



serwer 2011.12.14. 10:22:11

Amíg az emberek többsége hülye a facebook-hoz és egyáltalán az internethez, addig ezek a "marketing-fogások" a nethez értők kisebbsége által elkövetett lehúzások, megtévesztések és csalások.

Tudom hogy melósabb és nehezebb a célzott közönséget megtalálni, de hogy jobban fizet, az biztos.

Ráadásul a szánalmas magyar piacon a lájkolók 99 százaléka 0Ft-ot ér, így a hirdető 0Ft-ot keres.

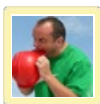
Egy valaki jár jól, a marketinges, ő mindenképpen számláz a hirdetőjének.

De hát ő meg egy "bűnöző". ;-)



seahawks 2011.12.14. 11:11:00

baszó bölény



Frady Endre • <http://fradyendre.blogspot.hu/> 2011.12.14. 11:34:46

JOHNTALANSÁG

Törzsfők neve ritkán János,
Mert az nem túl indiános.

/részlet a Kétsörösök c. cikluskámból/

fradyendre.blogspot.com/2011/08/ketsorosok.html
:)

is 2011.12.14. 11:54

@Konrad: azért vagy marketinges, mert az adataim reklámra felhasználása, (!)anélkül, hogy ezt explicite előre közölték volna(!), neked pozitív dolog, azaz nem visszaélés. csak szólok, hogy rajtad (marketingeseken) kívül ezt mindenki másképp látja. ha előre közölték volna, hogy egy reklámért az oldaladra cserébe megkapod az indián neved, az teljesen rendben van.

nem kell ingyen adni, csak meg kell mondani pontosan az árát. no hidden costs, please. és továbbra is áll a hasonlatom az operajeggyel.

Komáromi Teréz Atya 2011.12.14. 13:24:37

@Konrad:

Az egyik South Parkban Steve Jobs rávaratta Kyle száját egy japán csávó seggére, mivel nem olvasta el az EULA-t. Akkor ezt a valóságban is meg lehetne tenni, ha a törvény nem tiltja?

mim 2011.12.14. 17:08:16

@Komáromi Teréz Atya: Persze, hogy nem. De egy rakás dolgot tényleg megtehetnek, ha elfogadod a feltételeket. Amit igazán veszélyesnek tartok, az az EULA utólagos módosítása. Pl fél éve használsz egy programot, amit rendesen kifizettél és el is fogadtad az akkor érvényes feltételeket. Aztán hirtelen azzal a fedő szöveggel, hogy folyamatos támogatást kapsz és vele frissítéseket is, az arcodba nyomnak egy frissített EULA-t, amit már nem lennél hajlandó elfogadni. Ekkor innentől a szövegezés alapján ezzel "lemond" az "előfizető" (user-nek: "vásárló") a termék használatáról.

Németországban egyébként van jelenleg hatályos jogszabály ami ezt blokkolja, de más országban nem egyáltalán nem jellemző.

Pedig ez egy terjedő trend.

Még mindig az Autorun a kártevők kedvence

2011.12.15. 11:40 | [Csizmazia István \[Rambol\]](#) | [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.



Érdekes egy hónap ez, a toplista első és hátsó fertályában minden maradt változatlan, egyedül a középmezőnyben érzékelhető kisebb átrendeződés. Ennek részeként a Conficker féreg a korábbi harmadik helyett immár csak az ötödik. És bár a Conficker féreg folyamatosan csúszik egyre hátrébb, sajnos ugyanezt nem mondhatjuk el az Autorun vírusról, ugyanis továbbra is az első helyen parádézik immár nyolcadik hónapja.



Pedig az Autorun trónfosztásához tulajdonképpen minden adott lenne, hiszen a Microsoft már 2011. februárjában kiadta azt a frissítést, amely végül alapértelmezetten letiltja ezt a veszélyes funkciót. Emellett a naprakész vírusirtók is detektálják, illetve igen hasznos funkcióval bővült az új 5-ös sorozatú NOD32, illetve Smart Security is, amely mostantól a csatlakoztatott külső adathordozók még hatékonyabb vizsgálatát, azonnali ellenőrzését biztosítja. Ha decemberben sem változik meg ez a helyzet, nem frissítenek operációs rendszert a felhasználók, alighanem még 2012-ben is találkozunk majd vele.



Maradt második helyezett a Win32/Dorkbot féreg, amelyről eddig viszonylag keveset beszéltünk, pedig elég alattomos kémprogram. Azt kell tudni róla, hogy szintén cserélhető adathordozók segítségével terjed, és tartalmaz még egy hátsóajtó komponenst is. Ennek segítségével távolról átvethető az irányítás a fertőzött számítógép felett, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd megkísérli ezeket a támadóknak egy távoli gépre elküldeni.

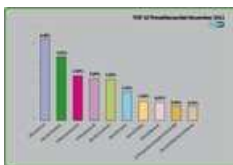


Az ESET e havi hónapzáró összefoglalójából a havi statisztika mellett hasznos tanácsokat kapunk a vírusvédelmi szakértőktől a Karácsony előtti online bevásárlások biztonságosabbá tételéhez, melyek hatékonyan segíthetnek elkerülni adataink, jelszavaink, pénzünk illetéktelen kezekbe kerülését. [Az összeállítást magyarul is elolvashatjuk az antivirus.blog weboldal posztjai között](#) az alábbi linken.



Ezenkívül említésre került az a tény is, hogy a Facebookon sajnos egyre gyakoribbak a csalások, a kártékony kódokat tartalmazó kéréten üzenetek. Egy viszonylag új módszer, hogy kéréten üzenetben, levélben, sőt néha még telefonon is műszaki segítségnyújtást ajánlanak fel Dell, Linksys vagy általános számítástechnikai supportra hivatkozva, ám ha valaki ezt gyanútlanul elfogadja, póru járhat. [A kérétenül jelentkező csalók ugyanis nem létező hibákat - hasonlóan a hamis vírusok álfertőzéseihez - "javítanak ki"](#), megadott linkre való rákattintásra próbálják rávenni a gyanútlan felhasználót, aki ilyenkor távirányított kémprogramot telepít a saját gépére. Nem csak az ártó szándék a felháborító ebben, hanem ráadásul ezért banki átutalás formájában még vaskos fizetséget is kérnek.

Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebookos kártevőkről, a közösségi oldalt érintő mindenfajta megtevesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.



Vírustoplista - 2011. november

Az ESET több millió felhasználó visszajelzésein alapuló **statisztikai rendszere szerint 2011. novemberében a következő 10 károkozó** terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 19.02%-áért.



1. INF/Autorun vírus

Elterjedtsége a novemberi fertőzések között: 4.38%

Előző havi helyezés: 1.

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>

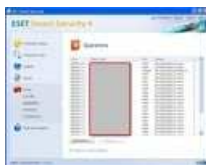


2. Win32/Dorkbot féreg

Elterjedtsége a novemberi fertőzések között: 3.43%

Előző havi helyezés: 2.

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>



3. HTML/ScrInject.B trójai

Elterjedtsége a novemberi fertőzések között: 2.40%

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>



4. HTML/Iframe.B.Gen vírus

Elterjedtsége a novemberi fertőzések között: 2.24%

Előző havi helyezés: 6.

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. Win32/Conficker féreg

Elterjedtsége a novemberi fertőzések között: 2.20%

Előző havi helyezés: 3.

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 eljárásán 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/Autoit féreg

Elterjedtsége a novemberi fertőzések között: 1.53%

Előző havi helyezés: 6.

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 novemberi fertőzések között: 1.03%

Előző havi helyezés: 5.

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.



A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/3□63366

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.

Magyar adathalász levél - én így szeretlek

2011.12.19. 15:50 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [spam galopp adathalász jacks magyarnyelvű](#)

[Patrick Chan nyelvzszenijét megszegyenítő](#) stílussal érkezett **Mr. Jacks Galopp** venezuelai úriember úgynevezett "magyar nyelvű" **adathalász levele postaládánkba**, amely ugyan 18 millió angol fonttal kecsegtet, de végigolvasva őszintén szólva sokkal inkább készlet sírva röhögésre, semmint személyes adataink pedáns begépelésére.



Így közeledve az év vége felé meg kell állapítsuk, **egy ilyen szürke fátyolos napon igenis megérdemlünk néha egy ilyen kéretlen levelet, bár a nyelvezetet látva** a szilveszteri időzítés nyilvánvalóan stílszerűbb lett volna. A levélhez nincs mit hozzáfűzni, az úgy kerek ahogy van. A helyesíráson felül kissé kiábrándító még, hogy **a címzettnél a körlevelekre jellemző "undisclosed-recipients" szerepel**, ez enyhén csökkentheti a figyelmes olvasó örökösödésben való hatékony reménykedési faktorát.



"Jó napot.

Én vagyok Mr. Jackie Vágta a Harlesden, Észak-Nyugat-Londonban, itt Angliában. Dolgozom NatWest Bank London. Tiszteletben kell tartani, és kapcsolatban írok Önnek a saját irodai és szeretnék javasolni Önnek, hogy üzleti lesz óriási előnye, hogy mind a ketten. Az én osztály, hogy a Private Banking Manager (Greater London Regional Office), felfedeztem egy elhagyatott összege 18.500.000 £ GBP (Tizennyolc millió £ 500,000) egy fiók tartozik egyik Külföldi vásárlóink Dr. Erin Jacobson, aki meghalt Egész családjával a Montana repülőgép-szerencsétlenségben március 23, 2009, útban egy csoporthoz ég vakáció.

A választás a kapcsolatot akkor volt, felkeltette a földrajzi adottságai, ahol élsz, különös érzékenysége miatt az ügylet, és a titoktartási itt. Most a bank várt bármely rokonok, hogy jöjjön fel a követelés, de senki sem tette ezt. Én személy szerint pervesztes lett megtalálását a rokonok már két éve, igyekszem az Ön hozzájárul ahhoz, hogy jelen van, mint a legközelebbi hozzátartozó / kedvezményezett az elhunyt úgy, hogy a bevételt e számla értéke 18.500.000 £ GBP fizethető meg.

Ez kerül folyósításra, vagy megosztani ez az arány, 60%-én és 40% az Ön számára. Én biztosított minden szükséges jogi dokumentumokat lehet használni biztonsági másolatot készíteni ezt az állítást mi a köze. Minden, amit kell, hogy töltsse ki a neveket a dokumentumokhoz és legalizálja azt a bíróság itt kell bizonyítania Ön, mint a törvényes kedvezményezett.

Minden, amit igényelnek most a becsületes együttműködést, titoktartás és a bizalom ahhoz, hogy lássuk, az ügylet révén. Biztos vagyok benne, hogy ez alatt hajtják végre a törvényes előírás, amely megvédi a felhasználót a megsértése a törvény.

Kérjük, adja meg nekem a következő: mint már öt napon keresztül futnak. Ez nagyon sürgős PLEASE.

1. Teljes név
2. A telefonszám
3. A Kapcsolat cím.

Miután ment keresztül módszeres keresést, úgy döntöttem, hogy Önt abban a reményben, hogy megtalálja ezt a javaslatot érdekes. Kérjük, a visszaigazoló e az üzenetet, és jelzi az érdeklődést, én ellátják Önt a megfelelő információkkal. Törekednek arra, hogy tudassa velem a döntést, nem pedig hogy engem vár. Hívj, vagy írv után megkapta a mail vagy hívj a Tel: +447024011974,

Üdvözlettel,

Mr. Jacks Galopp.

*****AVISO LEGAL*****

Este mensaje es privado y confidencial, está dirigido exclusivamente al uso del correo institucional. Si usted ha recibido este mensaje por error, debe abstenerse de distribuirlo, copiarlo o usarlo en cualquier sentido. "



Hogy jó hírt is mondjunk, még sokáig védettek leszünk, ha [az adathalászati levelekben az automatikus fordítások addig is tudják tartani](#)

[ezt a jelentősen kiemelkedő színvonalat](#). A klasszikus vicc szerint, a "hogyan készül a mákos pacal" kérdésre az a helyes válasz, hogy véletlenül összeragadt két lap a szakácskönyvben. Kicsit ennek analógiájára itt a **legsuperebb rész talán az, mikor a levélküldő még saját vezetéki nevét is lefordította a programmal**, így keletkezett aztán az "Én vagyok Mr. Jackie Vágta a Harlesden" kezdetű örökbecsű mondat. **Őszintén reméljük, erre [a hamis levélre sem Csisztu Zsuzsa](#), sem senki más nem fog válaszolni "sürgősen PLEASE" teljes névvel, pontos címmel, telefonszámmal.**

 23 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

  1 

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3475228>

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](#).

[Attila64](#) • www.sagaontour.ca 2011.12.21. 12:37:34

Oké!

Bárlista helyett Facebook credit score

2011.12.21. 19:10 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [facebook hitel kölcsön minősítés score lendo](#)

Hogy miért nem mindegy, mit lehet rólunk találni a neten, azt már jószerével kitárgyaltuk az [Amit tudni akartál a Privacyról, de sosem merted megkérdezni](#) című színes, szélesvásznú sorozatunkban. Ám a valóság most már ezen is túllépett, és ahogy ez Hihetetlen történetek rovatunk mai adásából kiderül, **hamarosan akár új szempontokon is múlhat majd, ki kaphat hitelt és ki nem.**



Pici idő még, és [a Menekülő ember című film elevenedhet majd meg](#) a Való Világ, és egyéb mélyen intellektuális valóság show-k műsorán. Ám **a pénzügyi válság, és az ehhez kapcsolódó új szempontrendszer miatt van, aki a fejlődésben már ennél is előrébb tart**, az orrunk előtt integet, ám mi már nem biztos, hogy őszinte mosollyal orcánkon integetünk majd vissza neki.



Ahogy a leadben jelzett [kompromittáló szennyest üzemszerűen kereső](#) leendő munkaadók, kormányzatok, politikai ellenfelek, vállalkozási területen szereplő konkurens versenytársak, válóperes ügyvédek [60-90%-ban támaszkodnak a Facebookon fellelhető adatokra](#), egy új szereplő is becsatlakozhat ezen adatbányászokhoz: ez pedig nem más, mint a pénzügyi szektor.



Ahogy azt egy korábbi nemes veretű posztunkban már írtuk, vannak riasztóan érdekes dolgok Földön s égen, például **egyes helyeken az a szokás dívik, hogy [ha állásügyben jövünk, akkor az interjún elkérik a közösségi oldalakon használt jelszavainkat.](#)**



A hongkongi illetőségű Lendo cég ezúttal azzal az ötlettel állt elő, hogy a kölcsönért folyamodó delikvenstől bekérjük a Facebook, Twitter, Gmail, Yahoo és Windows Live belépési kódjait, de ezek közül minimum hármat kötelezően. **Az ott begyűjtött információk alapján aztán legenerálnak egy ránk jellemző mutatószámot, amely eldönti, megkaphatjuk-e az áhított kölcsönt vagy sem.** A végeredmény [titkos kalkulációs összetevők és szempontok mellett annak a kiértékelésén is múlik, milyen jellegű információkat osztottunk meg és kikkel](#), felvázolva rólunk egy szociális gráfnak nevezett közösségi médiából kinyerhető jellemzőt.



Ennek fényében elmondható, **egyre nagyobb súlyt kap és kaphat a közösségi média**, ha egy vállalkozás vagy cég nincs a Facebookon, már egyenesen hendikeppel indul. Ám a közösségi lenyomat a magánszemélyek szempontjából is egyre nagyobb jelentőséget kap, [nyakunkon a Timeline](#), és bár a fenti kölcsönkérvénnyel kapcsolatos vizsgálati módszer egyelőre csak a Fülöp-szigeteken fungál, **könnyen az új idők előfutára lehet, amire aztán hamarosan majd a teljes banki szféra is rákaphat. A jövő elkezdődött.**

Tetszik 117 személy kedveli ezt [Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.](#)

Megosztás +1 0

Ajánlott bejegyzések:



- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/3481456>

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.

Kellemes Karácsonyi Ünnepeket

2011.12.24. 17:06 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [karácsony](#) [xmas](#) [hellókarácsony](#)

Boldog Karácsonyt és sikerekben gazdag Új Évet kívánunk az oldal minden látogatójának!



[Az alábbi videóval](#) találtuk magunkat szembe, és kellően érdekesnek találtuk ahhoz, hogy a mai jókívánságokhoz csatolva mellékeljük.



*"The Christmas is coming, the geese are getting fat
Please put a penny in the old man's hat
If you haven't got a penny, a ha'penny will do
If you haven't got a ha'penny, then God bless you!"*

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3493661>

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.

Zöld erdőben jártam, üveggömböt láttam

2011.12.28. 13:00 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [it biztonság](#) [jóslat 2012](#)

Ősi dakota szokás, hogy az IT biztonsággal foglalkozó cégek áttekintsék a kártevők várható fejlődési irányzatait, és belenézve az üveggömbbe, felvázolják a következő, 2012-es esztendő lehetséges támadási vektorait.



David Harley (ESET) szerint az idei évben a PDF és SWF sebezhetőségeit sokszor és sokat támadták, ám **jövőre ugyanez a sors várhat a Java-ra is**. Ezt az irányt megerősíti a Microsoft Security riportja is, amely arról tanúskodik, hogy **már 2011 első félévében is erőteljesen célkeresztben állt az Oracle (korábban Sun Microsystems) Java Runtime Environment (JRE), Java Virtual Machine (JVM), és a Java SE Java Development Kit (JDK) környezet**.



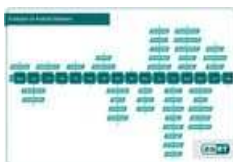
Harley szerint [a Javás sebezhetőségek ráadásul könnyebben kihasználhatóak a PDF és SWF exploitokhoz képest, valamint a támadáshoz való kártékony kódok is rövidebbek](#), kisebb méretűek, továbbá az is bonyolítja a helyzetet, hogy a Java környezetek naprakészen tartása, patch menedzsmentje sem egy kiforrott terület még.



Aryeh Goretsky (ESET) véleménye szerint további [fokozott támadások várhatóak a 64 bites rendszerek, a digitális tanúsítványok területén, valamint a Blackhat SEO és a social engineering sem fog veszíteni jelenlegi népszerűségéből](#). A szakember szerint **a BIOS elleni támadások nem lesznek tömegmértékűek**, bár az ilyen kártevők fejlesztése folyamatosan napirenden van, és várhatóan a Windows7 és Windows8 elleni támadásokról, kihasználható jelentős kritikus hibákról is fogunk majd hallani 2012-ben.



Damballák is kinyilatkoztattak a tárgykörben, ebben elsősorban a botnetek előretörése olvasható ki. Sajnos a botnetek leállítása nem hozta meg a várt eredményt, mert [a bűnözők is folyamatosan okosítják a C&C irányítás és parancsvezérlési módszereiket proxykkal, többretegű megvalósításokkal, így egy-egy vezérlő szerver leállítása szinte hatástalan](#). Ugyancsak megemlítik **az okostelefonos mobilmalak számának emelkedését**, és az e platformok elleni egyre szervezettebb támadási módokat.



Ezzel egybeesik [Sebastian Bortnik \(ESET\) véleménye is, aki az Androidos kártevőkben látja az új vadnyugatot](#). A világszerte üzemelő mintegy ☐milliárd mobilkészlet már eljutott arra a szintre, hogy megérje támadni, az App Store ellenőrzött és kontroll alatt tartott szisztémájával szemben itt bárkiből lehet ☐ndroid ☐pp fejlesztő, valamint itt is rendszeresen vannak olyan **támadható sebezhetőségek, amelyek kihasználhatóak**. Az Android a maga 43%-os részesedésével piacvezető, így a kártevők szempontjából ő lehet az új Windows.





Emellett a folyamatos ☐ ról ☐ indo ☐ s ☐ re való átállás hatásosan letörheti az olyan korábbi kártevők elterjedtségét, mint amilyen a 200-es Conficker féreg is volt. A közösségi oldalakkal kapcsolatos visszaélések mellett az egyéb internetes lokalizált támadások is várhatóan egyre gyakoribbak lesznek, de itt jobbra elsősorban inkább a spanyol nyelvterületen is bevezethető, orosz bűnözői körök által fejlesztett, és bárki által megvásárolható vagy bérelhető trójai eszközkészletekről beszélhetünk.



[A Symantec szerint a virtualizációs megoldások népszerűségével ez is egy olyan kiemelt terület, melynek biztonsági kérdéseivel folyamatosan foglalkozni kell.](#) A 2011-ben bekövetkezett egyre növekvő számú természeti katasztrófa is olyan tényező, melyet mindenkinek be kell kalkulálni. Reálisan nézve pedig 2012-ben is legalább ennyire vagy még ennél is többre kell felkészülni, itt a folyamatos rendelkezésre állás, a mentések fontossága, és még számtalan tényező játszik szerepet a vállalatok infrastruktúrájában.



Van aztán [Stephen Cobbtól \(ESET\) is egy színes szélesvásznú jövővdölés, ebben a fenti jóslatok kerülnek mintegy összefoglalásra.](#) Találkozunk akkor 2012. év végén, és akkor áttekintjük majd, ki milyen Nostradamusnak bizonyult az IT fenyegetettségek frontján.

 Tetszik  3 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

☐ ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

☐ bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/3501678>

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](#).

[bohocmasni 2011.12.28. 1:12](#)



ez a java kép :D

2011. legjelentősebb IT eseményei

2011.12.29. 13:40 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [apple](#) [facebook](#) [anonymus](#) [2011](#) [jobs](#) [tablet](#) [spotify](#) [google](#)

Lassan elfogy a 2011-es esztendő, és visszatekintve a gyorsan elrepült évre elmondhatjuk, bővelkedett eseményekben. Összességében talán a legjelentősebb hír az volt, hogy elvesztettük az Apple alapító guruját, Steve Jobsot. Megtapasztalhattuk politikai forrongások, események kapcsán, hogy a közösségi média mind jobban a tiltakozások jelentős eszközévé nőtte ki magát, valamint különféle hackercsoportok is komoly akcióikkal hallattak magukról az idén. Visszatekintő, összefoglaló következik.



Steve Jobs vezetői szerepe, látnoki és cégvezetői képességei megkérdőjelezhetetlen eredményeket produkáltak az évek során, melynek olyan ötletekkel és eszközökkel gyarapította a technológia fejlődést, amikkel aztán irányt mutatott, de a versenytársaknak is alaposan feladta leckét. Kütyüit világszerte sokan vásárolták, [vagy lettek a karácsonyi ajándékozás hön áhított tárgyai](#), mint például az iMac, az iPod, az iPhone vagy éppen az iPad. [Hogy mi lesz aztán Apple további sorsa, és Jobs nélkül is meg tudja-e őrizni az újítási képességét, sikerességét, majd elválik.](#)



Felértékelődött ugyanakkor a [közösségi kapcsolattartás, amelyre már a 2010 év végén induló Arab Tavasz, vagy az egyiptomi események](#) is ráirányították a figyelmet. A Facebook, Twitter és YouTube sikeresen adtak naprakész és hiteles képet távoli országok veszélyes eseményeiről. Ugyanakkor az is kiderült, bűnözői körök is hatékonyan felhasználhatják ezt a lehetőséget, hiszen emlékeztet, hogy [a londoni zavargások során BlackBerry telefonokon futó Messenger segítségével zajlottak a résztvevők közti egyeztetések](#), kapcsolattartás.



Aki eddig nem ismerte volna, 2011-ben biztosan megismerkedett [Guy Fawkes maszkjával, amit a V mint vérbosszú](#) című kult filmből ismerhetünk. [Az Anonymus és a Lulzsec hackercsoportok minden korábbi évre rácáfolva rengeteg betörést, és ezzel párhuzamosan rengeteg bizalmas adat publikussá tételét hajtotta végre, benne olyanokkal, mint kormányzati anyagok vagy éppen rendőrségi információk, személyes anyagok, levelezések.](#) Ugyancsak bebizonyosodott, hogy a hackertámadások hatalmas károkat, presztízavesztéseket, és ezáltal [óriási anyagi veszteségeket képesek okozni, ez lehet a Sony elleni támadássorozat](#) egyik nagy tanulsága.



Ami [más piaci szereplőknek nem sikerült](#), azt az Apple diadalra vitte. A tabletgépek minden korábbi várakozást felülmúlva [tarolnak a piacon](#), és lassan már a hagyományos asztali, illetve noteszgépek piacán is felülemelkednek. Bár a szereplők állandó piaci és szabadalmi csatározásban is vannak egymással, amely harc továbbra is nyitott, [egy szereplő mégis tudott ebben a helyzetben robbantani, ez pedig nem volt más, mint az Amazon Kindle Fire dömping áras gépe.](#)



A Facebook elképesztő és folyamatos fejlődése továbbra is a leglátogatottabb közösségi oldalként jelenik meg, és bár a közben megjelent Google+ is egyre gyorsabb ütemben gyarapszik, [a magánemberek között, illetve a vállalati eszköztárban egyelőre elkerülhetetlen piacvezető szerepe van a Facebooknak.](#) Adatvédelmi gyakorlatuk folyamatos kritika tárgyát képezte már régóta, ami miatt aztán [az FTC, azaz a U.S. Federal Trade Commission idei döntése alapján mostantól változtatásokra](#), illetve egyúttal minden második évben való rendszeres adatvédelmi felülvizsgálatra is kötelezték.



A már korábban is emlegetett szabadalmi csatározás minden eddigi mértéket meghaladóan a reneszánszát éli, **szinte nincs is olyan érdemi piaci szereplő, aki ne próbált volna beperelni mindenki mást.** Például az Apple, a Google, a HTC, a Microsoft, a RIM és a Samsung is részese ennek a harcnak, [amely miatt egyes országokban még be is tiltottak gyártmányokat](#), például a Samsung Galaxy Tabot. Sokaknak lehet érdekes az is, hogy [a Microsoft már olyan sok szabadalom, patent birtokosa, hogy tulajdonképpen a forgalomba hozott Androidos készülégyártók mintegy fele félelemből inkább fizet nekik jogdíjat](#), mintsem bizonytalan szabadalmi vitákba keveredjen.



A Google+ idei megjelenése **idővel esetleg átszabhatja valamennyire** a közösségi oldalak területét, de ehhez a versenyben maradva alaposan fel kell kötnie a felkötendőt. Emlékeztet, hogy folyamatos fejlesztések híján végül [a MySpace is elvázott ezen a fronton](#), igaz a jelenlegi jóslatok alapján talán éppen a Google lehet majd a Facebook valódi érdemi versenytársa. Mint ismeretes, [a Bloomberg szerint jövő év végére elérhetik a nem csekély 400 milliós felhasználói tábor](#)t.



Már érintettük részben **Jobs halála kapcsán, hogy minden várakozást meghaladóan sikeres volt az Apple**, és ez [az eredmény pénzben is egyértelműen kifejezhető volt, hiszen a világ legértékesebb vállalata lett](#). Hogy aztán Jobs nélkül is sikerül-e töretlenül megőrizni ezt a pozíciót, azt majd a jövő és a részvénytőke döntik el.



Ugyancsak idei hír volt, hogy **az IBM Watson nevű számítógépe februárban sikerrel vette az akadályokat a Jeopardy nevű televíziós műveltségi vetélkedőn**, ami az Egyesült Államok egyik legnépszerűbb műsora. Amint azt az IBM weboldalán is olvashatjuk, [az IBM gépe képes egy kérdés kapcsán mérhetetlen adatmennyiséget átvizsgálni, majd precíz megoldási javaslatot tenni](#) – a lehetséges válaszokat megbízhatóságuk szerint is rangsorolva, ami mindenképpen fontos mérföldkő a mesterséges intelligencia területén.



Végül, de nem utolsósorban [a Facebook és a Spotify bejelentett együttműködése szintén egy jelentős epizód](#) a közösségi zenehallgatásban, melynek **segítségével a Facebook profil birtokában például on demand jelleggel használható a streaming zeneszolgáltatás.** Amennyiben ez az izgalmas integrációs modell sikeres lesz, **jelentős mértékben előretörhet a birtoklás helyetti online hozzáférést biztosító módszer**, amely egyúttal állítólag a kalózkodás mértékét is képes csökkenteni. Mindenesetre az, hogy **egy ilyen rendszer megmutatja, mit hallgatnak éppen a barátok, ismerősök, széles körben képes megismertetni különféle zenei anyagokat, bevált modellé válhat.**



13 személy kedveli ezt [Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.](#)



Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés `trackback` címe:

`http://antivirus.blog.hu/api/trackback/id/3503983`

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.

Beváltak-e az idei jóslatok?

2011.12.30. 15:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [jóslat új boldog 2011 kártevő évet beválás](#)

Csak itt, csak most, csak Önöknek megmutatjuk, vajon mennyire volt találó a 2011-es év kezdetén megfogalmazott jóslat, [vajon tényleg azokat a kártevőket kaptuk-e a nyakunkba, amiket nekünk megígérték](#). Ne menjenek sehova!



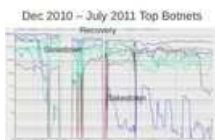
"Mobil vírusok: Az okostelefonok növekvő népszerűségének köszönhetően a mobil készülékeket érő támadások 2011-ben várhatóan többszöröződnek. A bűnözők számára az egyre növekvő piac jó terepet kínál, mivel a mobil biztonsági szoftverek használata még nem tartozik a felhasználói kultúra alapelemei közé."



Mondhatjuk, hogy ez így is történt, egy-egy, vagy időnként csoportos applikáció visszavonás történt a kártékony alkalmazások leleplezése után. Abban [sincs okunk kételkedni, hogy ez a terület nem fog további "fejlődést" felmutatni 2012-ben](#), így **valamilyen biztonsági program használata mellett az óvatos telepítésekkel tudjuk magunkat megóvni ettől a veszélyforrástól.**



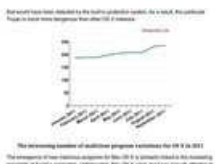
"Zombik támadása: Az ESET adatai szerint a botnetek mérete a számítógépeket zombivá tevő fertőzések számával együtt folyamatosan növekszik. A bűnözők a hálózatok irányítására a legkülönbözőbb csatornákat - például a Twittert - használják. Jó hír, hogy a biztonsági vállalatok egyre nagyobb sikereket érnek el a nagyobb botnetek lekapcsolásában, de ennek ellenére számolni kell a hálózatok számának növekedésével."



[Nem tűntek el a botnetek](#) se varázsütésre, se sehogyan a 2011-es évben. [Sok erőfeszítés történt a felszámolásukra](#), de mivel a bűnözők is folyamatosan okosítják a C&C irányítás és parancsvezérlési módszereiket proxykkal, többretegű megvalósításokkal, így egy-egy vezérlő szerver leállítása [ebben a harcban gyakorlatilag szinte hatástalan](#). **Felhasználói részről a naprakész vírusvédelem, a Windows rendszeres biztonsági frissítése lehet segítségünkre.**



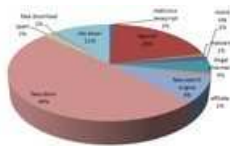
"Vírusok Mac-en: A Java/Boonana.A tavaly novemberi megjelenésével egyértelművé vált, hogy az OS/X rendszerek elterjedésének köszönhetően a Macintosh számítógépek felhasználói már vonzó célpontot jelentenek a bűnözők számára. Annak ellenére, hogy az Apple operációs rendszere szigorú biztonsági beállításokat tartalmaz, a kevésbé hozzáértő felhasználók bedőlnek a megtévesztő kártevőknek, és maguk kapcsolják ki azokat a korlátozásokat, amik megakadályoznák azok terjedését."



[Az emelkedés részben valóban megtörtént, igaz ez minimális mértékű](#), azaz egyelőre nem következett be itt komolyabb áttörés. Vonzó a Mac jüzerek pénze is, de nyilvánvalóan olcsóbb és kifizetődőbb volt 2011-ben is egyelőre inkább Windowsos kártevőket terjeszteni. A veszélyre való figyelmeztetés mindazonáltal ráirányította a figyelmet erre a területre is, ahol főként a trójai és klasszikus social engineering technikával lehet a gyanútlan Mac felhasználók gépére kártevőt juttatni. Szívesen látnánk egyszer arra is valamilyen statisztikát, hogy mindezek ellenére a felhasználók hány százaléka használ mégis valamilyen vírusvédelmi szoftvert. **A vírusvédelmi programok használata mellett a biztonság tudatos hozzáállás, és a megbízható forrásból származó telepítendő alkalmazások használata segíthet.**



"Mérgezett keresők: A legnagyobb keresők találati listájának eltérítése vagy mérgezése már 2010-ben is elterjedt volt. A technika lényege, hogy a bűnözők különböző keresőkefejezésekre optimalizálnak weboldalakat, majd megvárják, hogy ezek felkerüljenek a keresők találati listájának elejére. Miután ez megtörtént, megfertőzik őket, és rajtuk keresztül a felhasználók számítógépeit. Ugyan a keresők folyamatosan próbálják kiszűrni a mérgezett oldalakat a találati listájukból, a nagyobb volumenű támadásokkal szemben sokszor tehetetlennek bizonyulnak."



Ez a terület is olyan, ahol nem csak [bekövetkezett a folyamatos növekedés, hanem sajnos a jövő évben is szintén további emelkedésre számíthatunk](#). Bár a jelenség folyamatos tetten érhető, királyi esküvők, természeti katasztrófák, hírességek vélt vagy valódi halálhíre kapcsán kiterjedt kampányok erősítik fel az amúgy is magas fertőzött találati arányokat. **A kérértlen üzenetek, mellékletek mellőzése valamint a keresési találatok kellő gyanakvással való kezelése az, ami segíthet elkerülni ezeket a csapdákat.**



"Fertőző közösségi oldalak: A közösségi oldalakon az adathalászkok rendszerint valamilyen vicces, érdekes üzenettel és képpel vagy videóval keltik fel a felhasználók érdeklődését, majd egy alkalmazás segítségével megpróbálják megszerezni személyes adataikat. A problémát az jelenti, hogy lehetetlen megkülönböztetni, hogy egy adott bejegyzést valóban az ismerősünk írta ki saját üzenőfalára, vagy az egy kártevő működésének köszönhetően került oda."



A "ha melléütök is meghalsz" jegyében [egy Facebook a maga 800 millió tagjával jó terep](#) a különféle [hoaxok, adathalász, és egyéb kártékony linkek, tartalmak terjesztésére](#), hiszen ha csak 5% belesétál, az is 40 millió. Megszűnni ez sem fog várhatóan a következő évben, sokkal inkább további növekedés prognosztizálható. **Ha valamilyen üzenet nem tartalmaz kísérőszöveget, csak egy linket, vagy ha valamilyen ismeretlen vagy gyanús tartalom megismerése előtt lájkolni kell azt, inkább ne kattintsunk.**



És ha már jövőről van szó, [itt található a következő évre szóló jóslatsomag](#), ennek értékelését is elvégezzük majd egy 365 nap múlva. Egy [a 2011. legjelentősebb IT eseményeit összefoglaló](#) posztunk is megjelent, ha valakit érdekel, olvassa bátran. Várhatóan hamarosan megmutatjuk majd 2011. legolvasottabb antivirus.blog posztjait is, ám most zárásképpen **megköszönjük az egész éves figyelmet, és pezsgőkkel gazdagon ékesített Boldog Új Kívánunk mindenkinek!**



5 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/3506553

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.