

A Raural furmány

2010.01.04. 14:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [latin paypal betu](#) [adathalászat](#) [icann](#) [raural](#)

Egy egyszerű, rövidke példán igen szemléletesen lehet demonstrálni, milyen **extra veszélyforrások is** lapulnak az ázsiai arab és más, **nem latin írásjelekkel írt doménnevek** engedélyezésében.



[Érdekes helyzetet](#) teremthet a dolog olyan esetekben, amikor például a cirill betűs "raural" latinbetűs megfelelőjét kinézetre megvizsgáljuk:



Szakemberek **már korábban is igyekeztek felhívni a figyelmet** a tavaly évvégén [elfogadott szabállyal kapcsolatosan](#), de ez [a mostani írás talán minden eddiginél szemléletesebben teszi ezt](#), és pszichológiai nyelven remélhetőleg számos "Aha" élménynek nevezett hatást lesz képes okozni a fejekben.



Annai biztos, hogy a módszer **egy plusz lehetőséget adhat** [a már eddig sem kevés adathalász próbálkozásokhoz](#) is.

Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1644502>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010-es bug befigyel

2010.01.06. 11:50 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [windows](#) [német](#) [mobile](#) [2010](#) [symantec](#) [dátumhiba](#) [spamassasin](#) [bankkártya](#)

Mennyi? 2010. Mi 2010? Miért, mi mennyi? Bár világvége nem volt, átdolgozni való programsorok azért bőven akadtak az akkori 1999-2000 évváltás alkalmából. Akik [még emlékeznek az Y2K eseményre](#), netán még az [ominózus tévé adásokat is élvezhették](#) róla ;-), most lehet egy kis Deja Vue érzésük.



Most, hogy újabb érdekes évváltás jött el 2009. december 31 után, és világvége szintén elmaradt, de a Symantec és SpamAssasin felhasználók, valamint a német bankkártya tulajdonosok azért bosszankodhattak egy kicsit a szilveszteri kijózanodás közben.



[30 millió német bankkártya vált használhatatlanná](#), azaz a tulajdonosok nem tudtak vele fizetni boltokban, elfogadó helyeken. A gond a 2010-es év szám nem megfelelő kezelése miatt történt. Nem indul jobban az új esztendő a [Spam Assassin számára sem](#), ott a FH_DATE_PAST_20XX tett be a hibamentes működésnek.



A Symantec Endpoint Protection felhasználók esetében pedig [a 2010-es vírusismereti adatbázis szignatúra fájlok bizonyultak érvénytelennek, lejártak](#). Hogy a vírusvédelem megmaradjon, gyorssegélyként újra kiadták a vírusadatbázist, de ezúttal visszadátumozták azokat 2009-esre.



Viccesen néznek ki azok az SMS üzenetek is, amelyeket a Microsoft Windows Mobile Edition rendszert futtató telefonokon lehet látni, és az új évben érkeztek. Itt [a kijelzőn szintén egy dátumkezeléssel összefüggő hiba miatt a 2016-os év látszik](#) az üzenet dátumaként.



A fejlesztők már minden cégnél gőzerővel dolgoznak a végleges javításokon, és remélhetőleg hamarosan (2009 vagy 2016? ;-)) mindenhol helyre áll majd a normál működés.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Informatikai biztonság az egészségügyben](#)
- [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/1651022>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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>
[2010.01.06. 12:02:41](#)

Az SAP is ott focizik a csapatban:

www.basissap.com/2010/01/sap-spool-issue-affects-all-releases/



[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
[2010.01.06. 13:54:21](#)

Egy másik összefoglaló a tárgykörben:

www.eset.com/threat-center/blog/2010/01/06/millennium-falcon-crash-burn-revisited



[atko](#) **[2010.01.06. 14:12:36](#)**

Basszus a számokkal van a gond.

Szerintem a Bud Spencer és Terence Hill helyett a görög világuralomra törőnek kellett volna szurkolnunk, amikor el akarta törölni a számokat. Talán a Nyomás utána volt a film.

Na majd az újraforgatott digitális verzióban...

Víruselemző kurzus az egyetemen

2010.01.08. 16:58 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

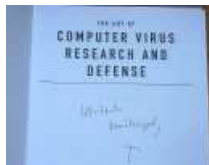
Címkék: [egyetem](#) [attila](#) [péter](#) [helsinki](#) [szőr](#) [kurzus](#) [suszter](#) [f](#) [secure](#) [víruselemzés](#)

Már két éve zajlik az olajozott együttműködés az F-Secure víruslaboratórium és a Helsinki Műszaki Egyetem között.



Érdekes kihívás előtt állnak azok a finn egyetemisták, akik szeretnének mélyebb ismereteket szerezni a vírusok elemzésében, azok visszafejtésében. 2010 tavaszán is lehetőségük van "[Malware Analysis and Antivirus Technologies](#)" szakra jelentkezniük. Bár éles vírushatásokat ilyenkor sem osztogatnak a hallgatók között, ennek ellenére valós kártevő esetekkel, tanulságos kódrészletekkel történik majd tanulás. Az 1986-os pakisztáni Brain vírustól kezdve napjaink rootkit eszközmeghajtó kódjainak elemzése is a terítéken lesz.

Az F-Secure kód visszafejtő versenyén egyébként már diadalmaskodott hazánkfia, egy 2007-es megmérettetésen az igen [előkelő második helyet érte el Suszter Attila](#).



Azt is jó látni, hogy a kurzushoz [ajánlott szakirodalom](#) között szerepel a szintén magyar Szőr Péter: [The Art of Computer Virus Research and Defense](#) című örökbecsű munkája.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [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/1656679>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Kártékony Android alkalmazást találtak

2010.01.11. 12:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [market trójai android](#) [kártékony adathalász droid09](#)

A trójai programok komoly kockázatot jelentenek minden platformon. A letöltő, a felhasználó hasznos alkalmazásnak hiszi azt, a program viszont vagy eleve nem az aminek látszik, vagy később valami mást is művel még titokban.



Nem régen [adtunk hírt olyan iPhone játékokról, amelyet az iTunes App Store-ból lehetett letölteni](#), míg aztán fel nem figyeltek kártékony viselkedésükre. Az ingyenes játékok - mint például a iMobsters vagy a Vampires Live - **egy beépített hátsóajtón titokban továbbították a fejlesztőknek a felhasználó telefonszámát**, illetve telefonkönyvében szereplő számokat, hogy ösztönözhesék őket a teljes változat megvásárlására. A programokat ekkor törölték a kínálatból.



Most érdemben hasonló helyzet adódott az Androidos telefontulajdonosok számára azzal, hogy [a Droid09 nevű alkalmazás lepleződött le](#). A program a felhasználók banki adatait próbálta megszerezni. Az [Android Marketplace ellen indított adathalász támadást](#) még decemberben, azóta viszont szintén eltávolították a kínálatból az inkriminált szoftvert. De a történet jó példa arra, nagyon inycenek, tájékozottnak és válogatosnak (szerencsésnek?) kell/érdemes lenni, amikor **alkalmazások telepítéséről van szó**. Szinte kivédhetetlen az az eset, hogy mikor az alkalmazás levizsgázik és bekerül a kínálatba, még korrekt, de aztán **egy váratlan frissítéssel már bele lehet helyezni a trójai funkcionalitást - amíg észre nem vesszük**, és le nem leplezik.



És még egy apró adalék az oda nem figyelésre: [Mac alatt létezik egy "játék", amelynek a licence jelzi, hogy véletlenszerűen törölget majd a számítógépen az állományok közül](#). Azon túlmenően, hogy azt gondoljuk, **játszon vele az, akinek shanghai táncosnő az öreganyja és baltával pucolja az ablakot**, sokan töltik le mégis úgy ezt az alkalmazást, hogy next-next-finish, aztán pedig ártatlan arccal csodálkoznak, hogy nincs szerencséjük. Pedig ott formailag még be sem csapnak minket, szemben az előző két esettel.



A Droid09 letöltőknek a szakemberek minden esetre azt tanácsolják, **távolítsák el az alkalmazást a telefonjukról**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Tizből öt kártevő hátsóajtót nyit](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/1663196

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Conficker uralom

2010.01.12. 12:40 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

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

Hat trójai is szerepel az ESET tízes kártevő toplistáján. Ez arról árulkodik, hogy gyakran hiányzik a kellő gyanakvás az új programok, alkalmazások telepítésénél.



Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melynek elemzése mindig tanulsággal szolgálhat a felhasználók számára.

A toplistán csak minimális változások történtek az élmezőnyben az előző hónaphoz képest. **Masszívan tartja az első helyet a Conficker**, amelyet előzőleg is többször birtokolt már. A Conficker egy olyan hálózati féreg, amely a Microsoft Windows egyik biztonsági hibáját kihasználó exploit kóddal terjed, gyenge admin jelszavak elleni támadással, valamint az automatikus futtatási lehetőségén keresztül is terjed a fertőzés.



Egy másik régi szereplő, a Virtumonde viszont lekerült a tablóról, helyét egy újonc trójai vette át. **A Win32/Injector a megtámadott gépen hátsó ajtót nyit, és a newvalarsrent.ru weboldalhoz csatlakozik**, ahonnan további fájlokat próbál meg letölteni. **Rootkit komponenssel is rendelkezik, működése során fájlokat rejt el** a fájlkezelő alkalmazások elől (pl. EXPLORER, FAR MANAGER) még akkor is, ha ezek nem rejtett attribútummal rendelkeznek.



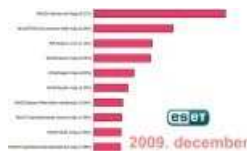
Összességében ami hónapok óta jellemző a toplistára, az hogy **a trójai programok aránya rendre igen jelentős az élmezőnyben**. A kétes alkalmazásokat a felhasználók maguk töltik le, indítják el, illetve telepítik fel, ez ellen pedig két dolgot lehet tenni. Egyrészt óvatosabban, megfontoltabban kellene átgondolni és kiválasztani, mit is akarunk feltelepíteni a számítógépünkre.

Érdekes a kínálózó, érdekes új programoknak először alaposan utána nézni, és csak ha biztató referenciákat találunk róla, akkor futtassuk. Másfelől a vírusvédelmi program beállításainál biztonságunk érdekében továbbra is érdemes a „Reklámprogramok, kémprogramok és biztonsági kockázatokat jelentő programok keresése”, a „Kéretlen alkalmazások keresése” valamint a „Veszélyes alkalmazások keresése” **opciókat megjelölni, kiválasztani**.



Az ESET víruslaboratóriumának szakértői szerint a hagyományos vírusfertőzések helyett **a jövőben egyébként is a felhasználók figyelmetlenségét vagy tudatlanságát kihasználó kártevők előretörése várható**. Előrejelzéseik szerint 2010-ben csökkenni fog az operációs rendszerek biztonsági réseit kihasználó károkozók száma, ugyanakkor a felkapott eseményekkel – például az idei labdarúgó-világbajnoksággal – kapcsolatos **fertőzött linkekre mutató e-mailek száma várhatóan növekszik** majd.

A közösségi oldalak felhasználóinak sem árt óvatosnak lenni, hiszen a személyes adatokra utazó **social engineering támadások előreláthatóan erősödni fognak**, míg az online játékosok belépési adatainak megszerzésére irányuló támadások az eddigieknél valószínűleg jóval intenzívebbek lesznek. 2010-ben **áttörés várható a mobil eszközök területén is**, ugyanis – az operációs rendszerekkel ellentétben – az egyre elterjedtebb okostelefonok **számos eddig fel nem fedezett biztonsági rést tartalmaznak**.



Végezetül következzen a magyarországi toplista. Az **ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2009 decemberében** az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. Ezek együttesen 36%-ot tudtak a teljes tortából kihasítani maguknak.



1. Win32/Conficker.AA férgek

Elterjedtsége a decemberi fertőzések között: 9.27%

Működés: A Win32/Conficker egy olyan hálózati férgek, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt biztonsági hibáját 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 férgek módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.

Bővebb információ: <http://www.eset.hu/virus/conficker-aa>



2. Win32/PSW.OnLineGames.NNU trójai

Elterjedtsége a decemberi fertőzések között: 5.58%

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekeznek állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók 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/virus/psw-onlinegames-nnu>



3. INF/Autorun vírus

Elterjedtsége a decemberi fertőzések között: 4.12%

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



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

Bővebb információ: <http://www.eset.hu/virus/autorun>



4. Win32/Injector trójai

Elterjedtsége a decemberi fertőzések között: 4.00%

Működés: A Win32/Injector trójai olyan Registry bejegyzéseket, illetve külön állományokat hoz létre a számítógép megfertőzésekor, amelyek egy esetleges újraindítást (boot-olást) követően aktivizálják a kártevő kódját, gondoskodnak annak automatikus lefuttatásáról. A Windows System32 mappájában (alapértelmezés szerint C:\ Windows\ System32) található wsnpoem, illetve ntos.exe lehet áruklódó jel. A megtámadott gépen hátsó ajtót nyit, és a newvalarsrent.ru weboldalhoz csatlakozik, ahonnan további fájlokat próbál meg letölteni. Rootkit komponenssel is rendelkezik, működése során fájlokat rejt el a fájlkezelő alkalmazások elől (pl. EXPLORER, FAR MANAGER) még akkor is, ha ezek nincsenek ellátva rejtett attribútummal.



A számítógépre kerülés módja: a felhasználó maga telepíti

Bővebb információ: <http://www.eset.hu/virus/injector-k>



5. Win32/Agent trójai

Elterjedtsége a decemberi fertőzések között: 2.83%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/agent>



6. Win32/Kryptik trójai

Elterjedtsége a decemberi fertőzések között: 2.40%

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm, illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani.

Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró-adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.



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

Bővebb információ: <http://www.eset.hu/virus/kryptik-gt>



7. Win32/Adware.WhenUSave alkalmazás

Elterjedtsége a decemberi fertőzések között: 2.04%

Működés: A Win32/Adware.WhenUSave működése során létrehozza a saveupdate.exe nevű állományt. Az ilyen nem kifejezett kártevő, hanem inkább a veszélyes vagy nem kívánt programok kategóriába tartozó kéretlen reklám programok sok esetben élnek olyan trükkökkel, hogy különféle további könyvtárakban is létrehoznak magukból másolatot. Ennek kettős célja van: egyrészt egy esetleges vírusirtást követően egy eldugott helyen megmaradhatnak a fertőzött állományok, másrészt helyi hálózatokban, megosztott könyvtárakban, peer-to-peer hálózatokban is képesek terjedni. Futása során megkísérel a web.whenu.com weboldalhoz kapcsolódni, ahonnan kéretlen reklámokat valamint saját program frissítésit tölti le. A fertőzött gépen aktív böngésző esetén linkeket, időjárás jelentést és más kéretlen reklámokat

jelenít meg.



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

Bővebb információ: <http://www.eset.hu/virus/adware-whenusave>



8. Win32/TrojanDownloader.Swizzor trójai

Elterjedtsége a decemberi fertőzések között: 1.96%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat tölt le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amelyek látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálják, valójában azonban maga a kártevő lapul a „csomagban”. Emellett hátsó ajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.



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

Bővebb információ: <http://www.eset.hu/virus/trojandownloader-swizzor-nbf>



9. Win32/VB.EL féreg

Elterjedtsége a decemberi fertőzések között: 1.92%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows 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 főkönyvtárban.



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

Bővebb információ: <http://www.eset.hu/virus/vb-el>



10. Win32/TrojanDownloader.Bredolab.AA trójai

Elterjedtsége a decemberi fertőzések között: 1.88%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, melynek segítségével a távoli oldalakról letöltődnek és végrehajtnak ezek a kódok. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is a bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságítámozgatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célsziszolgálóra.



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

Bővebb információ: <http://www.eset.hu/virus/trojandownloader-bredolab-aa>

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [Android kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1665844>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Doktor Adat és az ő jó édes anyukája

2010.01.13. 12:40 | [Csizmazia István \[Rambol\]](#) | [6 komment](#)

Címkék: [2010 kártevő data doctor zsaroló ransomware](#)

Többször is értekeztünk már a hamis antivírusok nyomán, amely [a tapasztalatlan felhasználóknak szerezhet néhány kellemetlen percet](#). Ha korábban egyáltalán nem volt valódi vírusirtója a gépen, igen nehéz az új szerzeménytől megszabadulni. [Esetleg ha nagy naívan még meg is vásárolja az "irtani is képes" fizetős változatot](#): kidobott pénz az ablakon. Most azonban úgy tűnik, a kártevő szerzők az évvégével még ennél is magasabb fokozatba kapcsolnak.



Mostani programunk a [Data Doctor 2010 már mutatja](#) azokat a tüneteket, amikre azt mondhatjuk: **látszik és beérett a napi nyolc órás állandó fejlesztési munka**. A weboldáról bekapott fertőzés első jeleként az olyannyira utált Blaster juthat az eszünkbe: **a visszaszámlálás elkezdődik**, és a gép leáll.



A restart után sem érezhetjük magunkat azonban a szerencse fiának, mert **egyes dokumentumaink elérhetetlenné, kódoltakká váltak**. Egy, azaz 1 (ágyin, one, een, ein, uno, jeden, une) állományt enged a program mindösszesen helyreállítani, továbbiakat nem.



És igen-igen, jól mondja, aki zsetonjait a pénzért mindent kockára helyezte, van megoldás, csak [meg kell vásárolni a Data Doctor 2010 fizetős, regisztrált változatát](#). Komolyabb az ijesztés, [rámenősebb a pénz kiszarolása](#), és aligha tévedünk, ha azt jósoljuk, ebbe az irányba több hasonló kísérletet látunk még a jövőben. Felnőttünk már, az évek múltával szaporodik fogunkban az idegen anyag, ezenközben a Google találatok között pedig a [How to Remove kezdetű bejegyzések](#).



Mivel azt nem igazán tudjuk elérni, hogy hosszú távon Doktor Adat eszentül csak és kizárólag azzal játsszon, ami egyidős vele, ezért **a másik fronton van esélyünk a hatékony védekezésre: használjunk megbízható naprakész vírus és kémprogram védelmet, hogy elejét vehessük az ilyen incidenseknek**. És emellett persze rendszeresen: **menteni, menteni, menteni...**

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1668699>

Kommentek:

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



buherator • <http://buhera.blog.hu> 2010.01.13. 13:21:40

Helyreállító eszköz a titkosított fájlokhoz:

community.ca.com/blogs/securityadvisor/archive/2010/01/09/another-recycled-ransomware-datadoctor2010.aspx



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.01.13. 13:36:12

Köszike, lehet, hogy jól jön majd valakinek :-)

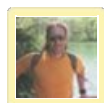
RoFä 2010.01.29. 05:56:38

Ez a jó édes anyukája egy nagyon finom, hovatovább eufemisztikus megfogalmazás.



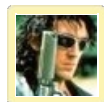
Yann Le Pentrec • <http://lnk.bz/t7c> 2010.03.04. 09:01:43

A legnagyobb okosság ebben (legalábbis a ransomware írói részéről), hogy nagy a merítés. Azaz rengeteg a tudatlan, számítástechnikailag rosszul informált user, és ezektől lehet kicsalni a zsíros bankókat, főleg a tengerentúlról.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.03.06. 13:31:41

Jött már olyan álláshirdetés spam, aminek a linkje aztán orosz társ keresőnek álcázott szexoldalra mutatott, ahol egy Windows Live Messenger szerű ablaknak látszó tárgyban volt egy üzenet, hogy Marija, Lena, és társaik már várnak. Gondolom, az ilyenre is kattint majd a 10 százalék, meg itt van most az XP help F1-je, tuti hogy behamisítják majd a kártevő írók azt is.



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.03.09. 14:52:52

Én meg mostanában a "Blizzard"-tól kapok World of Warcraft-témájú emaileket, miszerint adjam meg a logint/pass-t egy bejelentkező oldalon. Hogy hogy nem, a link egy totál más oldalra irányítana, a mail source-ba belenézve pedig világossá vált, hogy a Blizzard nem nagyon szokott hotmail-es emailről üzenetet küldözgetni... :)

Alapértelmezett lett a HTTPS

2010.01.14. 15:15 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [google](#) [gmail](#) [ssl](#) [https](#) [default](#)

Aki akarta, már 2008 óta használhatta a HTTPS beállításokat. Mostantól viszont [ez lett az alapértelmezett a Gmail-nél](#).



A Google közleménye szerint : "A HTTPS-alapú titkosítás **biztonságossá teszi az üzeneteket**, miközben azokat a rendszer a böngészőtől a Gmail szervereiig továbbítja, így mások, akik esetleg kedvenc kávézójának nyilvános Wi-Fi kapcsolatán osztoznak Önnel, nem tudják őket illetéktelenül elolvasni. A **bankok és a hitelkártyacégek ugyanezzel a protokollal teszik biztonságossá** az online számlákat. A **Gmail-fiók védelme érdekében mindenki számára bekapcsoltuk a 'Kötelező a https használata' opciót**. Ez az újabb biztonsági réteg lelassíthatja egy kicsit a Gmail működését, ezért ha nem használ titkosítatlan vezeték nélküli kapcsolatokat, kikapcsolhatja ezt a beállítást".



Érdemes mindig ezt használni, ha valaki eddig esetleg nem így tette volna. A név-jelszó adat a [HTTPS esetén így nem kifürkészhető clear text alakban utazik például a neten](#). Szóval örülünk, de szerintünk **már régóta így kellett volna lennie**. Közben pedig türelmetlenül várjuk már az alapértelmezett, vagy egyáltalán választható HTTPS blog.hu belépést is ;-)



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [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](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1671912>

Kommentek:

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

Nincsenek hozzászólások.

Nem kapsz pofont a kocsmában, ha be se mész

2010.01.18. 15:10 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [privacy facebook képek feltöltése settings](#)

Látja? Nem látja? Na látja! Röviden így foglalható össze a Facebook privacy settings nem létező lényege, ha az oda feltöltött képeinkről van szó.



Az F-Secure blogjában láthatunk egy kis bemutatót, mennyit ér az "only me" opció a kép feltöltésekor. Ugyanakkor az is látható, hogy extrovertált világunkban mennyire a kitérő a nagy divat, hiszen [a share, a másokkal való megosztás az alapértelmezés](#).



A megosztás a bizalmas baráttal pedig abban áll, ha a kép egyébként publikus linkjét elküldjük neki. Bár tulajdonképpen nem butaság, hogy az itteni rendszer ennyire szépen segít a szétkürtölésben, képek feltöltésében, mert a [töröljük a netről projekt-szerű fizetős renomé javító vállalkozások](#) meg később hálásak ezért, és jól beszedik a pénzt ugyanennek a műveletnek a fordítottjért.



A blogíró emellett még kitér arra is, hogy csoda, hogy a Koobface kártevő egyik új variánsa sem mozdult még rá eddig a fertőzött accountokban ezek gyűjtögetésére.



Hogy a kísérletező kedvű nagy honi elődökről is ejtsünk szót, Hancu mester már több körben is próbára tette a Mátrixot, és mind [a feltöltött, majd letörölt képek](#) esetén, minden pedig a [levelező rendszerek háza táján talált ugyanilyen](#) fehér foltokat a rejtek vagy nem rejtegető problémákban. (A címkép egyébként a klasszikus The Hunted, 2003. című filmből való, rajta a terepszínű ruhás vadászok ríktó narancssárga mellényben.)



És hogy a poszt cím igazságára visszautaljunk, az F-Secure blog is nagyjából így lövi be a bombabiztos tanácsát: "If you absolutely don't want to share it, [then don't upload it to a SOCIAL networking site.](#)" Maximálisan egyetértünk :-)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony vírusok - villám őrjárat 8.](#)



- [Akiknek a Captcha kinszenvedés](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1681451>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Mivel nyissunk meg PDF-et?

2010.01.19. 17:30 | [Csizmazia István \[Rambol\]](#) | [71 komment](#)

Címkék: [javascript pdf támadás exploit](#)

Az is egy helyes válasz lehet, hogy semmivel ;-). Meg lehet közelíteni a másik oldalról, hogy [inkább mivel ne: Adobe Readerrel](#). Lehet másik kisebb, gyorsabb program, jöhet a Foxit, a Sumatra és barátai. Akárhogy is, a JavaScript futtatást viszont mindegyikben legjobb élből letiltani. Végül a Linux alól sem egy rossz alternatíva. **De lássuk csak, miért is e nagy szkepticizmus?**



Réges-régen (mikor a hülyét még pontos jé-vel írták :-), [a PDF állományok még biztonságosnak tűntek](#), bátrabban nyitogathattuk a Portable Document Format állományokat. (Több PDF-et nyitottunk, mint kilincset ;-). Manapság azonban még abban sem lehetünk biztosak, hogy szabályos, használható dokumentumot vagy csak azt kapunk. Sőt, **ha kéréstlen levélben, vagy linken küldik ezeket, akkor szinte mérget vehetünk rá**, hogy valamilyen szándékosan félreformázott, sebezhetőséget kihasználó dokumentum vicceskedik nálunk.



Érdekes [célzott módszerrel próbálkoztak támadók az USA Védelmi Minisztériumának üzleti partnerei, beszállítói ellen](#). Egy valós, létező konferenciára invitáló PDF állományt tartalmazott a kiküldött levél, azonban [egy Adobe Reader sebezhetőséget kihasználó kód is](#) szerepelt benne. Az F-Secure azt is visszanyomozta, hogy **a letöltött backdoor egy tajvani IP címre kísérelt meg csatlakozni**.



Ha mégis meg kell nyitnunk ilyen, érdemes a PDF ID programmal, vagy a VirusTotalon megvizsgálni, persze szigorúan előtte.



És még egy érdekesség, sokszor van olyan, **amikor a látszatra még minimálisan sem ügyelnek** - egy igazi James Bond soha nem tenné ilyen. Nézzük: a **beérkező kártékony PDF állomány teljes mérete 3 KB**: phhh. Ebben aztán tényleg csak a Metasploit javascript shellcode fér bele cipőkanállal, **más hasznosnak vagy érdekesnek hazudott tartalom már nem igen**. Amíg nem jönnek az újabb, már elegendő számú nullával felhízlalt hihető méretű dokumentumok ;-), addig ezt is [lehet persze nézegetni mondjuk egy \(hexa\)editorral, de kizárólag annak, aki tudja is, mit csinál](#).



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



Ajánlott bejegyzések:

- [Az XP él, az XP él, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1684654>

Kommentek:

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



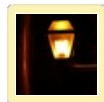
[atko 2010.01.19. 21:31:35](#)

A Linux valóban jó alternatíva :-).

[Átvitel honvéd 2010.01.19. 22:24:40](#)

Mióta a gyári Adobe Reader ilyen ocsmány, felhízalt bloatware lett, Linux alatt sem használom. ...Valahol 2008 táján telt be a pohár. Azóta csak kpdf, ill. pár hónapja "okular" (ami a KDE4-gyel együtt nem nagyon nőtt a szívemhez, de az AR-nél még mindig jobb kompromisszum).

...Hihetetlen látni, hogy ehhez az egyébként nagyon jó alapkoncepciójú dokumentumformátumhoz (...ps-ből mint kiindulópontból mondjuk nem volt nehéz) idővel milyen gázos gyári szoftverek jöttek ki. Gyakorlatilag a nagy semmiért, iszonyú nagy és persze erőforrásigényes, de legalább a korábbiaknál sebezhetőbb programok. Mindez (talán?) azért, mert az Adobe nyakkendősei úgy gondolták, hogy egy dokumentumnézőbe még ez is, meg még ez is, meg még ez is "kell", no nem, mintha a felhasználóknak fontos volna, hanem mert mi lesz az Adobe-val (konkrétan: a saját, potenciálisan lábbal illetett seggükkel), ha "nem fejlődik" a "termék"... nevetséges. Sic transit...



[ladislaus 2010.01.19. 22:24:51](#)

Preview -al, OSX-en.
szép estét mindenkinek!

[MCsaba • http://alegy.blog.hu/ 2010.01.19. 22:25:40](#)

Ma már miben nincs (vagy nem lehet) vírus... bár nem ismerem nagyon a Linuxot, de arra is írnának egy rakat vírust naponta, ha olyan elterjedt lenne mint a Windows!! És ez az összes egyéb népszerű progira is igaz (pl, Adobe)

[Átvitel honvéd 2010.01.19. 22:29:30](#)

[@MCsaba](#): Nem teljesen igaz; valószínűleg több próbálkozás volna, és volna néhány siker is, de mivel OS-szinten jobb, feszebb az alapkoncepció, nehezebb volna rá hatékony vírust írni. A feltételes mód azért, mert mióta linuxozok (nyolc éve?...), még egyet sem láttam.



[Iustizmord 2010.01.19. 22:29:34](#)

ludditák, rohamra !

[Sonka Nery 2010.01.19. 22:47:12](#)

kpdf-fel nyomom, no vérus :)

[Sonka Nery 2010.01.19. 22:48:03](#)

[@MCsaba](#): látszik hogy nem ismered nagyon a linuxot, azért írsz ilyeneket :)

[lessknownJFK 2010.01.19. 22:50:18](#)

[@Iustizmord](#): ludditák, esetleg.

[Robi, a hód 2010.01.19. 22:52:19](#)

[@MCsaba](#): Persze, egy igazi krekker már csak hecből is írna egyet, ha tudna Linuxra. A gond az, hogy a Linux rendszere úgy lett megírva (mint más Unix-szerű rendszer), hogy a fájlokat nem lehet csak úgy módosítani, ha a rendszergazda nem akarja.

Ilyet, hogy letöltött egy exe fájlt a netről és elindítja... Nevetséges.
Na ilyen a Linuxon nincs.

Átvitel honvéd 2010.01.19. 23:07:03

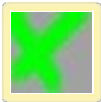
@lxrose: azé' a másik felét is nézzük meg...

Bloat cuccokat már "mi" is futtatunk, amelyek mindenféle huncutságra képesek; Firefox, Opera, Thunderbird, Kopete, aztán az ooffice, a Skype... vagy, hogy ne menjek messze, a Shockwave Flash plugin, ami ráadásul minden tisztességes laphoz "kell", és a gyári plugin closed source / binary only, valamint a gyártó tudomása szerint is full of bugs. Azt elérni, hogy root lehess (magát az OS-t feltörni), valszeg nehéz volna velük (pláne ugyanazzal a kóddal több dist több verzióján), de hogy userként, script-alapon, valaki valami huncutságot csináljon (mondjuk spamtek terjesztéséhez bot legyen, vagy ilyenek), az esetleg sanszos. Még itt is. ...Bár ez nem Linux-specifikus, ez bloatware-specifikus dolog.

MCsaba • <http://alegy.blog.hu/> 2010.01.19. 23:09:48

Mondtam, hogy nem ismerem annyira a linuxot! :)

Én egy Firefox-féle effektusra gondoltam (persze lehet hogy itt is a Win féle metódus a hibás): megjelent, lassan terjedt, kiderült hogy biztonságosabb mint az IE, elterjedt, jöttek kiegészítők, kiderültek sebezhetőségek, + kisebb-nagyobb foltok a pajzson, gyorsabb javítások (és így tovább) Most meg a Chrome lett az alternatíva... persze lehet hogy tévedek, de nekem ez valahogy így jön le!! :)



twollah / bRoKEn hOPe, sUppLeX •

<http://freewaresoftwarenews.blogspot.com/> 2010.01.19. 23:17:00

En Foxit Reader-rel szoktam megnyitni azokat.



pingwin • <http://pingwin.blog.hu> 2010.01.19. 23:36:54

@lxrose: de hujje user root joggal igen.

bellini • <http://doily.hu> 2010.01.19. 23:46:25

Vagy betöltheted Google Docs-ban.

Slowly 2010.01.19. 23:52:50

G reader pontosan... onnan html nézeben még a copyzás tiltással ellátott doksiból is lehet másolni...



Dervenkál Egon • dervenkai.blog.hu 2010.01.20. 00:06:35

Bizony preview.

TroppauerHümér 2010.01.20. 00:16:28

A pdf readereknek van egy közös hibája: ha a lemezen megváltozik a file (tipikusan, mert editálsz és fordítod pdf-re), akkor megvész. Pl. az acroread is. Az xpdf nem ilyen volt, azzal lehetett beamerben dolgozni.

A másik tipp az evince, nem beamer esetén azt használom.

pudliho 2010.01.20. 00:24:34

notepad - fejben visszafejtem aztán az eredményt leírom / lerajzolom egy lapra amit beszkennelek :-)

G. docs nekem is bevált



Dervenkál Egon • dervenkal.blog.hu 2010.01.20. 00:25:00

Na és mivel nyitunk meg chm-et? Emlékszik még valaki az MS féle pdf kísérletre. Sajnos a net tele van vele.....

emzperx 2010.01.20. 00:31:29

PDF-et élből konvertálok DJVU formátumba és azt használom.

Utólag OCR-ezem, hogy legyen benne text layer ami azután HASZNÁLHATÓ. A WinDjvuview megjegyez minden beállítást, hogy hol tartottál az olvasásban szövegrész vagy téglalap oldalrészletet BMP-ben tudsz vágólapozni, a lap bármely részére jegyzetelhetsz, könyvjelzőket vehetsz fel, fél mega a program, telepítés nélkül fut. Sok képpel megpakolt doku hatszor-nyolcszor kisebb mint az eredeti PDF és ugyanennyiszer gyorsabb is, oldalszámba ugrás Ctrl-G és nem öttezes shortcut! Keresőfunkció úgy működik mint mindenhol máshol, vagyis ÉSSZERŰEN, nincsenek felesleges de annál zavaróbb extra baromságok. Nyílt formátum. Sorolhatnám reggelig.

TroppauerHümér 2010.01.20. 00:34:07

@Dervenkál Egon: chmsee

nevermind 2010.01.20. 01:08:25

Jó hír. Több mint egy hete javították a hibát.

searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1238576,00.html

A nick már létezik 2010.01.20. 04:47:18

Hogy lehet kilincset nyitni?

Mert felénk kilincsel szoktak ajtót.



J. McClane 2010.01.20. 05:17:45

Hogy meghallgatásék a másik fél is:

Cégnél Acrobat Reader a nyerő. A Foxit ugyan freeware, de sajnos a bizodalmam benne kb ugyanekkora. Ráadásul 1 év után sírt, hogy vegyük meg. Csak belegondolni is rossz mennyi kiskapu, vagy sebezhetőség van benne. Persze ez nem derül ki a nagy portálokon, mert a kutya nem foglalkozik vele, hogy foxit sérülékenységeket vizsgáljon.

Tehát mi Acrobat Reader nyomjuk, igaz állandóan a legmagasabb patch szinten vannak a kliensek.

Nick Leeson 2010.01.20. 07:19:10

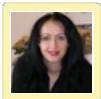
Szerintem az Acrobat Reader agyon lett bővíve. Szar az egész.

Másrészről nem értem ezt a hatalmas vírus parázást.

A vírusmentességnek 3 alapfeltétele van:

1. rendszeresen frissített vírusirtó, lehetőleg nem a legvacakabb
2. nem kell megnyitni olyan levelet ami szemmel láthatóan is gyanús
3. kalóz szoftvert csak óvatosan használunk

Az utóbbi 10 évben kb. 150 gépet felügyelem a munkám során. Szinte mind Win-es volt. Ez idő alatt max. 2-3 komoly vírus fertőzésre emlékszem, mind a kettő fent említett hibáknak volt köszönhető... A felismerés után, jóformán adatvesztés nélkül orvosolható volt a probléma.



Vidi Rita • <http://www.hosnok.hu> 2010.01.20. 07:22:19

Rambo, te vagy számomra az új kor Rejtő Jenője :)

Valaki segítene? Google Docs-ban PDF-et hogyan nyit sz meg? Mármint ami a neten van fenn, olyan PDF-et. Letöltés mindent,

aztán feltöltöd a docs-ba? Ezt most nem értem...

Hmm, már én is tartozom az olvasóimnak egy ilyen: ne használj adobe-t - írással, és egy foxit segédlettel, de az utóbbi időben rámborult a még mindig IE6-ot használók problémája...



[feketebarany666 2010.01.20. 07:51:18](#)

Hihi nekem elég ha megnyomom a space-t! :)

[eszkep 2010.01.20. 08:00:12](#)

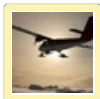
Foxit Rearer-rel.

Eleve a telepített mérete kb. 1/10-e az Acrobat Readerhez képest, ez a sebességen is meglátszik.



[Herlock Sholmes 2010.01.20. 08:37:55](#)

Tracker Software
PDF-XChange Viewer



[Bukowszky • http://bukowszky.blog.hu 2010.01.20. 08:42:29](#)

én is undorodom az adobe reader lassúságától és folyamatos zaklatásától



[Morci úr • http://suttyok-ket-kereken.blog.hu 2010.01.20. 08:45:58](#)

Még leszedni sem egyszerű.



[AiRLAC 2010.01.20. 09:06:43](#)

Preview, OSX :)

[Sörjárőr 2010.01.20. 09:17:37](#)

Én Sorax Reader-t használok (soraxsoft.com), kicsi, gyors.

[Birkesz 2010.01.20. 09:19:06](#)

[@pingwin](#): "de hujje user root joggal igen. "

Így van. Hiába überszuper "törhetetlen" a Linux, ha a doksit megnyitva az pl. feldob egy figyelmeztetést, hogy neki kell a root jelszó. A user megadja és voálá...

Egyébként meg éppen ezért nem fog elterjedni a Linux: macerás, hogy mindig minden le van korlátozva, szokatlan működési mód, meg egyébként is, ismeretlen. Hozzászoktak/tunk a jóhoz és egyszerűhöz Windows alatt, hiába sebezhető.

[tom sailor 2010.01.20. 09:39:37](#)

A .pdf teljesen biztonságos és bármivel megnyitható.

Ha:

1. Ismerem a feladót.
2. Van ilyen témájú közös projectünk
3. Netán még rá is kérdezek, hogy tényleg ő küldte...

Aki megnyitja a John Bigcock által küldött freepussy.pdf állományt az magára vessen.

Átvitel honvéd 2010.01.20. 09:40:42

@Birkesz: user error ellen nem tudsz mit tenni (vagy de: mondjuk, nem adsz neki root-jelszót, vagy sudo-jogot :-D).

A többi érv szerintem semmis. Amire célzol, az az, hogy Unixban élesen elkülönül a user ügyes-bajos dolga és a rendszeradmin-funkció (azaz nincs olyan laza szambázgatás rendszer- és userszintű feladatok között, mint egy trén (=kényelmes alapértelmezés) beállított windowsban). A helyzet azonban az, hogy a kérdésre a választ már megadták azok, akik OS-X-et használnak. Ebből a szempontból az sem különbözik. OS-X-ben egy BSD Unixon dolgozol, userként, és ha valami rendszerszintű műveletet akar csinálni, akkor megadod a jelszavadat (nem a root-jelszót, hanem a sajátodat), már feltéve, ha van sudo-jogod (mert pl. telepítéskor adtál magadnak). (Félreértés ne essék: attól, hogy a saját jelszavadat írod be, nem a root-jelszót, egy esetleges vírus még nincs jobb helyzetben... "ő" ugyanis egyiket sem tudja, azaz nélküled nem tud sudo-zni). ...Azt gondolom, elég sokan döntöttek eddig már az OS-X "kényelmetlensége" mellett. Ami Linuxon ehhez képest plusz kényelmetlenség, az az OS ill. a grafikus felület gyorsabb változása, relatíve kevésbé felhasználóbarátsága (de azért próbálj ki egy Ubuntut, ha arra jársz).

Megjegyzem, egy Linuxban v. OS-X-ben az rendszer- és userfeladatok szétválasztása miatti "kényelmetlenség" nem igazán zavaró, mivel a Unix mindig is ilyen volt, és idővel megpróbálták az ebből eredő kényelmetlenséget könnyíteni (lásd sudo). Ezzel ellentétben a "jól" beállított Windows-ban, ahol eredetileg ezt mindenki nyugnek tekintette (mindenki god mode-ban dolgozott/ik, "persze tudjuk, hogy így nem jó, de kit érdekel"-alapon), ez a dolog láthatóan jól utólag került be a képbe, és a megvalósítás olyan ("kényelmes") is.

arconfosom 2010.01.20. 09:45:37

A Linuxhoz picit értők (értsd: sikeresen telepítettek már) mindig azzal jönnek elő, amihez nem értenek... :)
Még hogy webről exét letölteni és elindítani nem lehet csak Winfoson... Meg hogy nincs vírus linuxra muhahaha
Életükben nem láttak még win7est
Na mindegy

Van egy freeware pdf nézegető, ami ráadásul a képeket, szöveget is kimentí fájlba, ha kell
De nem jut eszembe hirtelen a neve, és csak otthon használom

Ha valakit érdekel - kicsi, gyors és ingyenes, annak megnézem

Vidi Rita nagyon tetszik! :)
Nem jársz te is HDMFC-be?

aqswdefr 2010.01.20. 09:54:36

Az Adobe Acrobat tényleg tartalmaz csomó bővítményt, ettől nagy, de ezeket ki lehet kapcsolni, és akkor ugyanolyan gyors lesz, mint a foxit.

Átvitel honvéd 2010.01.20. 09:58:52

@arconfosom:

1.) tölts le egy fájlt Linuxon (ahogy Windows-on tennéd exe-vel és társaival), mentsd el, és indítsd el (hülyeuser-módra, nem biztos Unix-tudással!), ha tudod.

2.) (Linux vírus): várjuk a felsorolást...

Robi, a hód 2010.01.20. 10:07:49

@Birkesz: Nyilván a hülyeség ellen nem véd semmi. Aki nem ért kicsit jobban a Linuxhoz, az ne legyen benne a sudoers fájlban, vagy ne ismerje a root jelszót!. A számítógéphasználathoz ész kell, hiába.

arconfosom 2010.01.20. 10:11:37

@pozitív szemidefinit mátrix:

Hát, tudod, már ott bukott a dolog, mi szerint el akarod indítani a pdf-et :D

De se baj, valamiben egészen biztosan fejlődőképes vagy ;)

arconfosom 2010.01.20. 10:24:53

2.

Biztos csak pénzkidobás a vírusvédelem linuxra, mert linuxra nem is létezik vírus :D

2002, Slapper ? Hm?

És az ELF fájlok sem sebezhetők, meg a forrásba sem tudja magát belefordítani

www.pandasoftware.com/download/linux/linux.asp

www.f-prot.com/products/home_use/linux/

www.kaspersky.com/anti-virus_linux_workstation

www.mwti.net/linux/linux_products.asp

Írd már be a keresőbe, hogy known viruses on linux :)

ÉS egy tökéletes magyarázat, hogy miért VAN kevesebb vírus linuxra

So why hasn't there been more malicious code for Linux? The dominance of Windows, particularly as a desktop operating system, is the key reason. Malware authors want the biggest possible bang for their buck so they target the operating system that is most widely used. Linux simply isn't widespread enough to be a serious target - at the moment.



Kontárblog • http://kontar.blog.hu/ 2010.01.20. 10:27:20

nekem az a fő bajom, hogy win7-em van, és se az adobe, se a foxit nem hajlandó a böngészőben megnyitni pdf-et mindent le kell töltenem, semmilyen online pdf-et nem tudok megnyitni. Nem találok a bugját, csak nekem produkálja ezt...



Hurrá Torpedó • http://www.youtube.com/watch?v=br-D7UneS0E 2010.01.20. 10:29:13

Win-en sem lehet csak úgy exéket futtatgatni a vakvilágba, csak rendszergazdaként. Az most más kérdés, hogy az install után a linuxon létrehozott user fiók az tényleg user szintű jogokkal rendelkezik, mígy win-en rendszergazda jogokkal.

na ez a szomorú, hogy minden balfék ember rendszergazdaként netezik, emailezik, pdf-fel. naná hogy terjednek a vírusok.

a win rendszergazda fiók az otthoni win-es gépek 99%-án sosem volt használva, mert mindenkinek admin a saját usere. innen látszik hogy az emberek nem értenek az informatikához. a microsoft meg baszik tenni bármit is a biztonságért, mert alapesetben a telepítéskor létrehozott usernek csak user jogot kéne adnia. (aztán ha utána az ember adminra állítja az már az ember baja)

joszip 2010.01.20. 10:30:31

"3KB...Ebben aztán tényleg csak a Metasploit javascript shellcode fér bele "

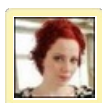
Hát nyilván. Nagymamám hívta fel rá a figyelmemet nekem is.

Judy Epokit 2010.01.20. 10:41:30

@pozitív szemidefinit mátrix:

en.wikipedia.org/wiki/Linux_malware#Viruses_and_trojan_horses

kicsit görgess lefelé. Ennyit a vírusmentes OS-ről. A DE kezdetű fanboykodást meg tartsd meg magadnak, mondom ezt úgy, hogy én nem állítom, hogy ismerem a linuxot csak használom 10+ éve.



In Motion 2010.01.20. 10:49:50

Preview, mert az jó. :)

Átvitel honvéd 2010.01.20. 10:50:45

@arconfosom: webről letöltött exe el nem indíthatóságáról te beszéltél, b+.

Romkocsmák homályában merengő főállású troll

2010.01.20. 10:53:15

[@Hurra Torpedó](#): Lehet hogy balfék vagyok, de én rendszergazdaként netezek, UAC is ki van löve a Win7-ben. A gép legyen alám rendelve, ne fordítva :)



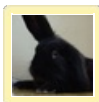
röntgenszeműlány 2010.01.20. 10:55:24

Acrobatban is ki lehet kapcsolni a javascriptet. Akkor most miért is ne?



röntgenszeműlány 2010.01.20. 10:56:26

[@Sün! balázs](#): Hát nem tudod, hogy attól leszel power user ha percenként tizenhatszor be kell írnod a passwordödet?



GZoli 2010.01.20. 10:57:52

[@Kontárblog](#): A foxit pl. azonnal beépül firefox-ba és simán megnyit mindent, lehet a többi is, de én ezt használom.

Átvitel honvéd 2010.01.20. 10:58:30

[@Judy Epokit](#): Hány év alatt? Mennyi is?
Hány valós (terjedni nem csak elvi síkon képes) threat?
Hány, root-jogot elérni, komplett rendszert felnyomni képes kód?

...Nulla?

Csorfab 2010.01.20. 11:12:49

[@ladislaus](#): +1

Romkocsmák homályában merengő főállású troll

2010.01.20. 11:13:23

[@röntgenszeműlány](#): Ja, jut eszembe, jelszót sem kér a gép indításkor, rühellném :)

Átvitel honvéd 2010.01.20. 11:16:37

[@arconfosom](#):

Linuxban ott bukik a dolog, hogy tool-okat nem mindenféle helyről, hanem leginkább a disztribúcióból telepítesz, és a csomagoknak minimum független ellenőrzőösszege van (arra az esetre, ha tf. a tükröt, ahonnan a csomagot leszeded, fe is ltörték). Tetszőlegesen akárhonnán letöltött elf kódot nemigen futtatsz a Linuxodon, már csak azért sem, mert 1.) nincs rá szükséged (lásd dist), 2.) erősen kétesélyes, hogy elindul (architektúra és libek esetleges különbözősége), azaz nem szeretjük (a készítő sem, mert külön macera mindenféle disthez bináris csomagot gyártani, még ha sokan meg is teszik), 3.) ha mégis valami olyan dologra van szükséged, ami nincs benne a kiadásban, akkor leginkább forrásban szeded le, és te magad fordítod le, telepíted fel... ami azt jelenti, hogy már nem vagy egységsugarú user, aki csak klikkelget, hogy persze, hogyne, mindjárt adom a jelszavam is... magyarul, vélhetően tudod, hogy mit csinálsz. (Arról nem beszélve, hogy egy nyílt forrású cuccnál mekkora botrány követi, ha adott site-on letölthető forráscsomagba valami ajándékot csomagolt a site gazdája). Azaz hiába módosítható az elf, hiába "lehet" "fertőzni" a forráscsomagot, a veszély sokkal kisebb, mint a mindenféle helyről cuccot üzemszerűen letöltőgető/elindítógető/feltelepítőgető (mert nincsenek repository-k) Windows-os fanoknak.

Az általad megjelölt víruskeresők Linuxon futnak, de nem azért, mintha Linuxon ennyi vírus volna, hanem mert vállalati környezetben gyakran használnak fájl- és levszervereknek Linuxot. A linuxos víruskergető az ezeken a szervereken levő fájlokat masszírozza... váratlan módon, windows-os vírusokat keresve.

Ha elolvastad azt a cikket, akkor azt is olvashattad, hogy ezzel ellentétben a világon üzemeltetett webserverek döntő többsége linuxos... ehhez képest a valós, Apache-exploitok kihasználására épülő valós threat-ek kihasználása minimális. Hogy lehet ez?

arconfosom 2010.01.20. 11:16:46

[@pozitív szemidefinit mátrix](#): Te B+

lxrose írta:

"Ilyet, hogy letölt egy exe fájlt a netről és elindítja... Nevetséges."

Én erre reagáltam :

"webről exét letölteni és elindítani nem lehet csak Winfoson..."

Míg te ezt:

"tölts le egy fájlt Linuxon (ahogy Windows-on tennéd exe-vel és társaival), mentsd el, és indítsd el"

Ezek után nem tudom mit akarsz bizonygatni, én csak idéztem, illetve utaltam egy másik hsz-re

De beszéljünk a linux vírusok nem létezéséről! :DD

arconfosom 2010.01.20. 11:22:35

[@pozitív szemidefinit mátrix](#):

Szerintem hagyjuk

Olyannal nincs értelme beszélgetést folytatni, aki elvből tagad valamit

Ha ismernéd a linuxos (unix) alatt terjedő vírusok működési mechanizmusát, nem is írtál volna feleslegesen ilyen disszertációt a disztribúciós csomagok fordításáról, mert közben rájöhettél volna, hogy felesleges.

Ez itt már erősen átment linux kortes hadjáratba!

Én nem foglaltam állást egyik OS mellett sem, mindegyiknek van gyenge pontja, badarság bármelyiket tökéletesnek kikiáltani

De ez a komment lehetőség itt az elterjedt Adobe megalomániás olvasó kiváltásának lehetőségeinek kiaknázására való, nem egymás győzködésére

A Foxit reader jó alternatíva, de fizetős.

Punktum



Hurrá Torpedó • <http://www.youtube.com/watch?v=br-D7UneS0E> 2010.01.20. 11:34:41

[@Sün! balázs](#): aki tudja hogy mit csinál, és úgy használja adminként a windowst az nem balfék. viszont te nem fogsz gondolom összevissza exéket elindítani, istentudja milyen progikat installálni. (ha igen, na akkor tényleg balfék vagy)

otthon én is admin vagyok, de megfelelő védelemmel rendelkezem, és ésszel gépezek (ha meg mégis balfék voltam 5 perc alatt visszatolom a backupot).

viszont a cégnél kizárt dolog hogy bárki admin legyen. itt én is sima user vagyok, és ha kell csak akkor admin. sőt itt bizonyos munkagépeknél még a net is tiltva van, ha nem kell a munkakörhöz.

Átvitel honvéd 2010.01.20. 11:35:48

[@arconfosom](#): Az eredetileg úgy szólt (mellesleg lxrose-ra reakció nélkül) hogy

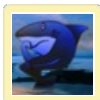
"Még hogy webről exét letölteni és elindítani nem lehet csak Winfoson... Még hogy nincs vírus linuxra muhahaha"

Én erre közöltem (arra utalva, hogy ezek szerint Te azt mondod, hogy ilyet -- "exét letölteni" és "elindítani" -- szerinted Linuxon is (implicit: könnyen) lehet) -- hogy O.K., ha így van, próbáld meg, mennyire könnyű. De ne mély Unix-tudással, hanem ahogy a mezei user tenné. (Magamban még azt is hozzátettem, hogy választhatsz -- elf-et töltesz le és próbálsz futtatni az executable flag megelőlegezése nélkül, vagy windows exe-t, úgy, hogy valamilyen dist-ben implicit elindul rá a wine -- amit szerintem nem tesz).

Erre te azt mondod, hogy mekkora barom vagyok, mert a pdf-et el akarom "indítani". Meg, hogy másban egészen biztosan fejlődőképes vagyok. Hát gondolkodj egy kicsit legalább azon, hogy te magad mit írtál le.

Átvitel honvéd 2010.01.20. 11:51:22

@arconfosom: Ez így elég "fluffy". De, ahogy gondolod.



Daily Shark • <http://dailyshark.blog.hu/> 2010.01.20. 11:56:24

Mi a helyzet az Acrobat Professionallal? Nalunk az nyitja meg a PDF-et...

Judy Epokit 2010.01.20. 12:01:10

@pozitív szemidefinit mátrix: Fanboi lolbammeg

"2.) (Linux vírus): várjuk a felsorolást..."

Átvitel honvéd 2010.01.20. 12:05:41

@Judy Epokit: az alapkérdésre nem válaszoltál...



gothmog 2010.01.21. 08:22:27

@Judy Epokit: Így-így! Nagyon helyesen látod. A valaha volt összes linuxos kártevőt fel lehet sorolni ~1 képernyőoldalon. Nnna. :) Most próbáld meg ugyanezt a windowssal.

Van itt kettő komment, ami felszínesen az egyszerű felhasználó számára elmeséli a "miért biztonságosabb a linux" kérdéskört: ubuntu.hu/node/10913#comment-121498
ubuntu.hu/node/10913#comment-121561

(persze bazmegolhatunk is, annak is megvan a szépsége)



atko 2010.01.21. 15:10:04

Huh végigolvastam a fentieket és egy jó nagyot szenvedtem. Szerintem ez majdnem csúcs a blog életében (hsz szám) pedig csak a pdf sebezhetőségről írt Rambo.

Az eredeti témához hozzászólva: Én amikor Linux alternatívát helyeztem természetesen nem a linuxos acrobat-ra gondoltam. Jómagam megelégedéssel használom az Okulárt a kde4-el egyetemben és egy nap kétszer írok be jelszót: bejelentkezéskor és a Digitális notesz elindításakor. Vírusom nincs, fent van a gépen a Végre Linux alatt is használható Nod32 de semmit nem talált.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.01.21. 15:48:31

Hello Atko, Rita, Többiek!

Hú, egész komment hegy érkezett :-O Köszönöm :-D

A Google Docs-nál én is a saját gépről feltöltött PDF-et ismerem, URL-ről nekem sem importál közvetlenül.

A kisebb PDF olvasó cuccok jobbák szerintem, de persze ez korántsem jelenti azt, hogy azokban aztán ne lenne exploit lehetőség. Itt hergeltünk Foxitot:

antivirus.blog.hu/2007/10/31/minden_es_mindenki_tamadhato

A Linux dologhoz hozzászólva engem a hideg kiráz, mikor valaki ezt használja, és közben meg Windowsos programok telepítését erőlteti: fizetős Nerot (K3B, GnomeBaker, stb. helyett) vesz rá, a Total Commandert akarja Wine alatt használni (Krusader, Gnome Commander, Tux Commander, Mucommander, Midnight Commander helyett) vagy éppen Adobe Readert (Evince, Kpdf, stb. helyett). Nekem az eszem megáll ettől, hiszen azért vált az ember, hogy ingyenes legyen, azért vált, mert ott mindenre meg van a gyors és biztonságos natív alternatíva. Persze IMHO :-)

emzperx 2010.01.23. 19:39:38

Valaki magyarázza már meg miért kell egy kurva dokumentumformátumba futtatható kód lehetőségét tenni és az olvasóba azt futtató szolgáltatást? Mert ha már nagyon kell, lehet olyat is csinálni ahol a script hatásköre kizárólag az őt tartalmazó dokumentre korlátozódik, anno még a wordperfect idejében ezt meg tudták oldani.

Mondjon valaki nekem egy ilyen felhasználásra példát ahol minden más megoldás ésszerűtlenül bonyolultabb!

Ugyanez a meccs már lement anno a mikrofos ofisszal, aztán a hülye ótlúk levelezővel. Mindig az történik, hogy kódot lehet belerakni amit a barom readerük mindenféle jelzés nélkül lefuttat. Ezt a gyártókon, vírusírókon kívül más -főleg aki használja- nem tudja.

Tippelek hogy van egy stika megállapodás az ilyen bloatware gányoló multik és a vírusirtó cégek között.



Celtic 2010.02.20. 10:00:09

[@Csizmazia István \[Rambo\]](#): Azert a Total Commander eleg vilagvero. mc-elmaradott, de mar fejlesztik. Krsader-kde depend, Gnome Commander-Gnome depend, tobbit nem ismerem, de igazan orulnek egy TC-szintu filekezelonek Linuxon, aminek csak X kell.

K3B- KDE depend

GnomeBaker- Gnome depend

growisofs :) Behanyja egy konyvtarba az ember a kiirando cuccot, aztan:

mkisofs -J -r -o dvd.iso DVD/

growisofs -dvd-compatible -overburn -speed=4 -Z /dev/hdc=dvd.iso

Kesz is. Sajnos, az ellenorzes hianyzik belole :(

En mar csak amondo vagyok, hogy iszonyuan hianyzik a TC es az IrfanView Linux alol. gthumbs nem rossz, de azert az Irfan szamomra midnent ver.



Celtic 2010.02.20. 10:19:21

Jaigen, pdf-re meg ott az xpdf. Kicsi, (aranylag) gyors.

No School, No Job, No Problem

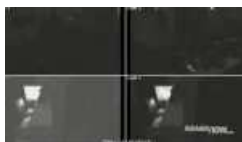
2010.01.21. 12:02 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [ausztrália](#) [kamera](#) [biztonsági kémprogram](#) [állásközvetítő](#)

Nagy a verseny az állás piacon, és mindenki a sikeres elhelyezkedés biztos receptjét kutatja. Nos, egy ausztrál "úriembernek" (rendőri szakzsargonban) ez sikerült, sőt még film is készült róla. Csillag született, bár ez utóbbinak valamilyen rejtélyes okból kifolyólag ő maga nem örült igazán.



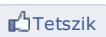
Bulvárosodik minden, manapság már nem hír, ha a postást megharapja a kutya, hanem éppen fordítva, ha a postás harapja meg a kutyát. Ugyanígy kevésbé érdekes, ha [a munkaadó kémprogramot telepít, és megfigyeli a dolgozóit](#) - napi rutin, így megy ez. Akkor ennek szellemében következzen most egy valóban ÉRDEKES hír. Egy dél-ausztráliai illető egy vadonatújnak nevezhető módszerrel próbálta beelőzni a mezőnyt. Mennyivel kényelmesebb lenne otthonról, a fotelból megtudni minden, hangsúlyozom minden adatot - morfondírozott. Az éjszaka leple alatt aztán visszatért a Dulwichben található munkaerő közvetítő cég irodájába, és távoli hozzáférést biztosító programot csempészett a számítógépre.



Pechjére azonban [a biztonsági kamerák felvették](#), amint a kémprogram feltöltéssel bíbelődött. Mivel a hivatkozott weboldalon igen hangya méretű ez az FLV mozi, ezért érdemes lehet inkább lementeni és valamilyen nagyítással megnézni.



Hiába, [a hazug embert könnyebb utólélni, ha sánta vagy ha áll :-\)](#) A cselekmény mindenesetre merőben újszerű, lehet hogy divatot teremt. Jó figyelmeztetés lehet minden, személyes adattal dolgozó hivatalnak, irodának, hogy védjék jobban az általuk kezelt bizalmas adatokat, és fizikailag is az ezeket tartalmazó irodai számítógépeket. Akkor [már csak távolról törhetik fel](#) az SQL adatállományokat ;-)

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1689635>

Kommentek:

petportal 2010.01.22. 09:58:14

Ugyanarra a felkérésre jelent meg az alábbi tanulmány is, ami miatt írtunk a témáról:
pet-portal.eu/?page=articles&func=view&id=19

Gábor

Johnny Depp, az élő halott

2010.01.25. 16:45 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [google csalás](#) [trójai](#) [johnny kártevő](#) [depp kryptik](#) [halálhír](#)

Folyamatosan komoly energiákat mozgatnak meg a keresőkben a kártevő terjesztők, hogy odatereljék a kellő számú balekot a letöltési oldalukhoz. Mindig minden ünnep, katasztrófa, földrengés, breaking news erről szól: hogyan tudják a Google találatokat megmérgezni. Mivel állítólag az, akinek a halálhírét keltik sokáig él, bátran készülhetünk hát A Karib tenger kalózái 86. epizódjára ;-)



Johnny Depp autóbalesetben elhunyt Franciaországban. Még a CNN is megaszondja. Vagy mégsem? [Jé, hiszen a link nem is a CNN-re mutat, azt a...](#) A rajongók azonban ilyenkor már tűzbejönnek, nem figyelnek fel ilyen apróságokra, kattintanak, mindent tudni akarnak, Izaurának pénzt gyűjtenek.



Vegyük észre, [az Angelfire hamis oldal éppen az első a Google találatai](#) között. Van egy Gauss görbéje az érdeklődésnek, amely időben ugyanúgy emelkedik felfelé, ha valóságos hírről van szó - gondoljunk például a [Sony rootkit](#) DRM leleplezésére - de a kitalált hírek is önálló életet élnek egy idő után a virtuális térben, itt is jön harang görbe.



Az igaz, hogy néha valóban vannak helyzetek, mikor egy tumblr, egy twitter frissebb, naprakészebb lehet: [éppen lövik a moszvai parlamentet](#), vagy Iránból kapunk híreket. Azonban sosem tudhatjuk, hiteles-e amit "elsőkézből" írnak, és még többször azt sem, pontosan ki is írja mindezt. A "Johnny Depp dead video" szavakra keresve még érdekesebb lesz, már videó beszámolókat is ígérnek.



Akit a Kínában hosztolt weboldal sem ejt különösebben zavarba, az még szembesülhet az alábbi figyelmeztetéssel: "WARNING! Possible, in you pc not installed needed version of Video ActiveX codec. Please install codec for watch this video. Install is easy and will not take more than a minute. (IE 5,6,7 MyIE, Google Chrome, Netscape, Safari, Opera, Mozilla Firefox compatible)."



Mindez magyarról magyarra fordítva: "[Hé te, rohadt kis klambó...](#) Éppen most akarunk átkampózni egy kodekletöltésre hivatkozva. Nem kapsz két óriási pofont, ha letöltöd gyorsan a kártevőnket, amely a világ összes böngészőjével kompatibilis, höhő." :-)



Érdekes tehát megfontoltabban hozzáállni a váratlan hírekhez: hihető-e, igaz-e, hamis-e, [más különálló autentikus forrás megerősíti-e](#), és még egy: ha a vadonatúj hírhez, [videóhoz csak egy EXE kiterjesztéső videokodek](#) árán juthatunk, [kattintás helyett](#) inkább együnk [egy kis csokoládét](#).

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1700567>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 Adsense, a kártevő

2010.01.26. 21:11 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [google](#) [frissítés](#) [adsense](#) [kaspersky](#) [hibás](#) [mindenkivel](#) [előfordulhat](#)

Mindig félelemmel vegyes figyelemmel kíséri a szakma, mikor egy konkurens AV cég adatbázisa [tévesen riaszt be tiszta Windows](#) rendszerfájlokra. [Ez szinte minden csapattal előfordult már](#). Most ehhez hasonló kellemetlen baleset történt, amikor egy nem megfelelő felismerés miatt [a Kaspersky tévesen kártékony szkriptnek azonosította a Google Adsense kódját](#).



Egyre gyakrabban fordul elő, hogy különféle nagylátogatottságú oldalakon kártékony kódok bukkannak fel, [gondoljunk csak a BKV weboldalára](#), vagy [a mai e107 malőrre](#). Nagy volt a riadalom hétfőn a felhasználók körében, volt aki gyanakodott már vakriadóra, [de biztosat eleinte még senki sem tudott](#). A fejlesztők aztán a sűrű bejelentések nyomán észlelték a problémát, és [kénytelenek voltak egy javított frissítést kiadni, amely mintegy 12 órát vett végül igénybe](#). Elnézést kértek a felhasználóktól az okozott kényelmetlenség miatt, és [igyekeztek tájékoztatni minden lehetséges fórumon, még Twitteren is](#).



Mégis miért ilyen kényes és nehéz feladat ez a frissítés? Mind a felismerést biztosító szignatúra állomány, mind pedig a heurisztikus keresést végző algoritmusnak tökéletesnek kell mutatkoznia a kiadás előtti teszteléskor, amelyet nem csak az ismert fertőzött állományok sokaságán kell ellenőrizni, hanem **ellenpróbaként mindezt el kell végezni a rendelkezésre álló nagy számú ismert tiszta állományok csoportján is**. Ez utóbbi művelet sok időt vesz igénybe, de végrehajtása arról hivatott gondoskodni, hogy **a vakriasztások száma lehetőleg minimális, vagy éppen nulla legyen**.



Mivel a kibocsátott rendszeres frissítések napi száma az utóbbi években egyre nőtt, ezzel egyúttal megnövekedett az ellenőrzési és tesztelési feladat is, ami - a kártevők számának exponenciális emelkedése mellett - **óriási terhet tesz a víruslaboratóriumok munkatársaira**.



Minden ilyen malőr esetén **az összes antivírus cég újból áttekinti a saját tesztelési, ellenőrzési módszerét**, és igyekszik a más kárán **tanulva még precízebb lenni**. Emellett a versenytárs nem ellenség, **nincs semmiféle etikátlan kárörvendés**, és **igyekeznek egymásnak minden technikai segítségét is megadni, ha ez szükséges és az adott partner kéri**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [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/1704725>

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>
[2010.01.29. 08:53:10](#)

Symantec slaps Trojan alert against Spotify:

www.theregister.co.uk/2010/01/28/symantec_spotify_false_alarm/

22 millió számítógép 48%-a fertőzött

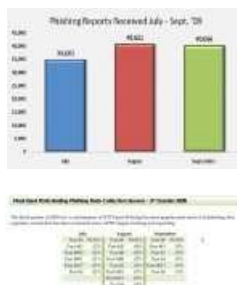
2010.01.28. 18:20 | [Csizmazia István \[Rambol\]](#) | 116 komment

Címkék: [linux statisztika](#) [live cd](#) [bankolás](#) [fertőzött számítógépek](#) [adathalászat](#) [apwg](#)

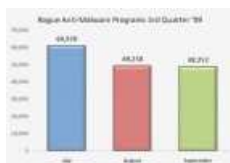
Habár ez most **nem** a Gyilkos számok című sorozat különkiadása, de abban talán Charlie Eppes is egyetértene, **nem kicsi ez az érték**.



Az **Anti-Phishing Working Group** most megjelent [2009 III. negyedéves jelentéséből](#) nemcsak ez derült ki, hanem bepillantást kaphatunk **az adathalászzal kapcsolatos trendekről, a regisztrált visszaélések számának alakulásáról**, az adathalász adatok összegyűjtésével foglalkozó szerverek portszám szerinti megoszlásáról: a 80-as portnak nem volt érdemi ellenfele. Szeptemberben láthatóan minden picit visszaesett, talán hogy újra nekigyürkőzve még magasabb szintre menjen majd októberre (vagy iskolakezdés volt ;-).



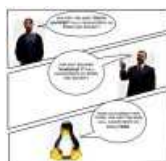
Kapunk ezenfelül **információkat az ál-vírusirtó programokról is**, ezek száma sajnos nem igazán csökkent a tavalyi harmadik negyedévben, és azóta sem. Sőt, inkább új utakra lépnet, nemrégiben adtunk mi is hírt **egy fejlettebb, már titkosítással is operáló zsaroló programról, a Data Doctor 2010-ről**.



A kártevőket terjesztők dobogós országai Kína, az Egyesült Államok és Oroszország lett. Az **nem derült ki, pontosan hogyan lehetséges ez a 48%**, mindenestre óriási számnak tűnik. Ha elkezdünk durva becslésekkel közelítgetni, hogy mennyien nem használnak antivírust, mennyien nem frissítik az operációs rendszerüket és alkalmazásaik biztonsági hibáit, elavult vagy nem megfelelő védelmi programot használnak, hozzáadjuk a dátumot is, stb. talán ki is jön.



A **Wired cikk vége felé aztán idéznek egy korábbi írást is**, amin lehet hogy érdemes lenne elgondolkodni: **"ideje leszokni a Windows alatti bankolásról"** lehetne érdemben a címe, és nagyjából arról szól, mennyire **hasznos lenne minden Windows tulajdonosnak, ha a bankolást, online vásárlást is egy külön erre a célra elkészített Linuxos Live CD-vel oldanák inkább meg** (esetleg virtuális géppel). Az ABA (American Bankers Association) korábban egy olyan **figyelmeztetést adott ki a kisvállalkozások részére**, amely egy dedikált, csak a bankolás céljára használt számítógép felállítását javasolja számukra a visszaélések, csalások elkerülésére.



Talán a fenti számok, és a fenti hideg-rideg statisztikai adatokhoz tartozó elcsalt pénzmennyiség is csökkenhetne ezekkel. Most viszont **egyelőre úgy tűnik a túlzott kényelem áll nyerésre**: odabankolunk, ahonnan böngészünk.



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

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1709031>

Kommentek:

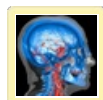
A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói tartalomnak minősülnek, értük a [szolgáltatás technikai](#) üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a [Felhasználási feltételekben](#).

[Szeretném látni az összes kommentet! \(116\)](#)

Az utolsó 100 komment:

Énszóltam 2010.01.29. 02:57:58

Látom felébredtek a Bill Gates Jugend tagok, és jönnek harcolni a führer védelmében az alacsonyabbrendű szolgálafaj linux ellen (amiről azt hiszik, hogy egy parancssor villogó kurzorral).



röntgenszeműlány 2010.01.29. 03:14:48

"(esetleg virtuális géppel)"

Tessék mondani, és az hogy véd meg a háttérben futó vírusoktól?

phare 2010.01.29. 03:28:28

Én egész egyszerűen nem érzem magam biztonságban windowssal a neten. Hiába van profi internet security és profi kémprogramirtóm, bankolni nem mernék róla. Most mit kezdjek biztonság szempontjából egy olyan operációs rendszerrel amire a sunbelt blog szerint csak naponta ötvenezer különféle kártevő jelenik meg? Nincs az a vírusirtó, ami bírja ezt az iramot. És a mai linuxok nagyon felhasználóbarátok, pl. az ubuntu negyed óra alatt felmászott a gépemre és egyből minden működött, nem kellett tökölni a különféle driverekkel (hangkártya, tv tuner, stb) még az ati drivert is leszedte és telepítette automatikusan. Én megmondom őszintén, akinek nem igénye az új játékok, az nem értem miért használ még mindig windowst. Az ubuntu a szoftvertelepítés csak annyi hogy megnyitom a szoftverközpontot és válogathatok a sok ezer alkalmazás közül, amit csak kijelölök és magától letölti és telepíti. Az ubuntu szoftvertelepítéseit látva, a windows csak megbújhat a sarokban és csendesen zokoghat. :))

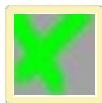
Én azt mondom egy ubuntut még egy hülye is tud használni, sokkal kevesebb számítástechnikai ismeret kell hozzá, mint a windowshoz.

Az én 68 éves édesanyám egy nap alatt belejött az ubuntu használatába, pedig eleinte nem tudta megkülönböztetni a bekapcsológombot az egértől.

phare 2010.01.29. 03:47:09

Az Ubuntu telepítése Wubi segítségével

sugo.ubuntu.hu/community-doc/intrepid/main/install/install-wubi.html



twollah / bRoKE n hOPe, sUppLeX •

<http://freewaresoftwarenews.blogspot.com/> 2010.01.29. 04:33:11

Linuxot kene hasznalni...

phare 2010.01.29. 04:51:22

[@twollah / bRoKE n hOPe, sUppLeX:](#)

És ez hogy jön ide?

Windowsra is vannak ingyenes szoftverek és linuxra is vannak fizetősek. Más kérdés, hogy ubuntu rendszerre vannak a szabad szoftverek a szoftverközpontban, csak rákeresel mi kell és magától letölti és telepíti.

Én például megvettem a Quake 4-et, a DOOM 3-at, az Enemy Territory Quake Warst csak azért mert ezeknek a játékoknak van natív linuxos portjuk. Persze az is igaz, hogy csak és kizárólag ezek a játékok azok a szoftverek azok amikért fizettem linuxos környezetben, az összes többit meg tudom oldani az ingyenes, szabad szoftverekkel.

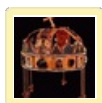
phare 2010.01.29. 05:12:58

[@twollah / bRoKE n hOPe, sUppLeX:](#)

Ja, most látom nem linkeltél, hanem a nickedben van benne a link. Bocs.

BKV reszelő • <http://praxisfree.blog.hu> 2010.01.29. 05:13:10

[@Énszólta](#)m: És hála istennek, igazuk van. Az X az nem linux. Én ezért szeretem, mert nem kell sikálni az egérrel az asztalt, várva, hogy megnyíljanak az ablakok, hanem parancs beír, lefut, munka kész.



kitvalasztanal.hu - Választási tippért notebook! •

<http://www.kitvalasztanal.hu> 2010.01.29. 07:11:51

[@hami](#): Én ismerem ubuntu-t, egyik gépen az fut itthon. Macera. Be sem kapcsoljuk...

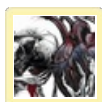
Amíg számítésh. szervizes azt mondja az ügyfélnek, hogy minek tűzfal és vírus irtó, addig persze, hogy lesznek fertőzött gépek. Mac ugyanez a filozófia..

És mivel már van multiplatform vírus kezdemény, kenheti mindenki a hajára a linuxot is.



kermi 2010.01.29. 07:35:54

[@kitvalasztanal.hu - Típelős választási oldal](#): Akkor minek van azon a gépen rajta? :)



Viktus 2010.01.29. 07:38:48

[@kermi](#):

Te utóljára melyik win-t használtad? :P nekem van olyan xp-s gépem amin négy éve fut gond nélkül a cucc ... igaz nem

telepítgetek mindenféle hülyeséget rá.



Viktus 2010.01.29. 07:41:58

@Androsz:

Én biztonságosan érzem magam, aki beakarna nyomulni betudna, akármilyen rendszer fut a bankolás gépemen, amely router-en keresztül csattan a netre, van vírusirtó, tűzfal na meg a bankom hardver kulcsot is adott :P , amíg az nincs bedugva nincsen bankolás.



Viktus 2010.01.29. 07:56:46

@Birkesz:

Már mondtam az oktatás, és a mindennapi jómunkás környezet a lényeg. Az iskolákba microsoft cuccok ketyegnek a legtöbb átlag melóhelyen is azzal fog találkozni az ifjú titán, akkor meg minek foglalkozna linux-al? ez ilyen egyszerű.

A Linuxnak éppen ez a legnagyobb baja nincsen marketingje, mert nem áll mögötte egy piaci szervező. A microsoft meg okosan korán elkezdte behálózni az embőrt.



Celtic 2010.01.29. 08:00:39

En viszont annak nem orolnek, ha mindenfele USB-s kutyut adna a bankom, ami _csak windows_ alatt lenne használható.



Viktus 2010.01.29. 08:09:34

@Celtic:

Különböző ízlések. Én szeretem van egy usb-s kártya olvasó külön egy kártya ami beizzítja meg még a kódot is meg kell adni ... akinek megérné pöcsölni a kis pénzemért az jobban jár, ha mindjárt a bankba tör be :P

Ske 2010.01.29. 08:14:28

Nem tudom, ki hogy van vele, én is windows alól bankolok, csak én használlok vírusirtót (még fizettem is érte, mert mint tudjuk, olyan nincs, hogy valami ingyen van), frissítem is a gépemet, és érdekes módon még sosem volt semmilyen gondom.



igazi hős 2010.01.29. 08:17:51

@röntgenszeműlány: A virtuális gépen van egy firefox és semmi más. Elindítod, 15 mp múlva belépsz a böngészőbe, bankolsz, majd kilépsz a Virtual PC-ből. Max fél perc a többlet, cserébe mindegy, hogy milyen honlapokat látogatt az unokaöcséd a valódi windowsodon levő IE-vel, abból semmi nem jut át. Mondjuk ezt én fizikai géppel oldom meg (van anyá notebookja, apa notebookja és egy asztali amin játszani lehet), de a VirtualPC olcsóbb, mivel ingyenes.



pingwin • <http://pingwin.blog.hu> 2010.01.29. 08:29:40

@Androsz: sot meg ennyit sem, hanem live cd-rol, mert az ugye csak read-only.

nem kell telepíteni, használni, csak bankolashoz.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.01.29. 08:31:53

Üdv mindenkinek!

Nem OS hitvitáról van itt szó, hanem ahogy Igazi hős (talán Európa Kiadó?) fogalmazott: biztonságos bankolásról. Egy ilyen szeparált környezetből a cookielopás esélye roppant csekély, szemben a minden másra használt böngészővel közösködve, bármi legyen is az. Az pedig már külön csapás, ha az éppen Internet Explorer.

[|Z| 2010.01.29. 08:32:33](#)

[@Viktus](#): és szerinted ez megvéd az olyan rosszindulatú kódtól, amelyik a böngésződben átírja a tranzakció adatokat????

Segítek, a helyes válasz a: nem, nem véd meg...

en.wikipedia.org/wiki/Transaction_verification

[Birkesz 2010.01.29. 08:40:02](#)

[@Viktus](#): Így van, jelentős részben az az oka annak, hogy nem ismerik és szeretik, hogy nem találkoznak vele.

Énszólтам: a kutya sem védte a Windowst. Csak felsoroltuk, miért nem terjedt el a Linux. Ami ugye alsóbbrendű szolgafaj, parancssorban villogó kurzorral ;)



[pingwin • http://pingwin.blog.hu 2010.01.29. 08:40:30](#)

[@kermi](#): sztem, ha rahuznank egy win skint az ubntura nem venneek észre, hogy nem win



[pingwin • http://pingwin.blog.hu 2010.01.29. 08:41:42](#)

[@Birkesz](#): matrix utanerzes



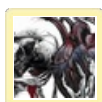
[igazi hős 2010.01.29. 08:43:50](#)

[@Csizmazia István \[Rambo\]](#): OFF Talált, de kis i-vel, egy egyszerű "első osztályú vidéki srác" :-). OFFOFF

[Birkesz 2010.01.29. 08:44:40](#)

[@pingwin](#): Csak látnék már Win skint. Nem olyant, ami úgy-ahogy lekoppintja, hanem teljesen azonost. Kár, hogy ez nem fog menni, mert valószínűleg le van védve a kinézet.

Plusz jó lenne, ha nem lennének kompatibilitási problémák, mint írtam feljebb.
Ezek megléte esetén lehetne váltani biztonságos környezetre.



[Viktus 2010.01.29. 08:56:05](#)

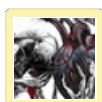
[@|Z|](#):

Megvéd a felhasználói környezetem, mert semmi ilyesmi nem történt az utóbbi 5 évben ...

[no mail, no problem 2010.01.29. 08:56:40](#)

[@Birkesz](#):

xandros? igaz, hogy fizetős linux, de mindenféle szempontból win klónt próbálnak gyártani, és benne ms applikációkat futtatni.
ne kérdezd, mi az értelme, én fel nem fogom.



[Viktus 2010.01.29. 08:58:16](#)

[@|Z|](#):

Tudod eleve utalás után még a kódot újra bekell pityegnem, majd betolja a tranzakciót várakozási listára ott megint látom jó helyre megy é bármi átakarná írogatni a KH rendszerébe kellene behatolnia ... mert még aznap átszoktam nézni számla információk, és egy telefonhívás bármelyik tranzakció törlése.

[Birkesz 2010.01.29. 08:58:50](#)

[@no mail, no problem](#): Nem ismerem, majd utánajárok. Azt, hogy mi az értelme, leírtam korábban: mivel a programok jó része Win alá készül, ezért feltétlenül szükséges, hogy a Linux is képes legyen futtatni azokat.



[igazi hős 2010.01.29. 09:05:16](#)

[@Birkesz](#): Ne mondd már, hogy ha nincs négyszínű zászló a képernyőn, akkor nem tudsz elindítani egy böngészőt! Eszem megáll, miféle kompatibilitási problémák? A Firefox és a Firefox között? Videószerkesztő programot vagy .Net fejlesztő rendszert nehezebb Linux alatt keresni, de az átlaguser böngészőt és office (szöveg- és táblázatkezelőt) használ. Mindezeket ingyenes szoftver van, ami egyformán fut a 2 rendszeren + 1 órási gyorstalpaló a fájlrendszerből, bár a Windows használók zöme nem ért semmit az NTFS-ből...



[pingwin • http://pingwin.blog.hu 2010.01.29. 09:05:34](#)

[@Birkesz](#): amugy szerintem pl a gnome skinek szebbek :)



[pingwin • http://pingwin.blog.hu 2010.01.29. 09:11:02](#)

[@kermi](#): probalj rtf-et



[pingwin • http://pingwin.blog.hu 2010.01.29. 09:12:24](#)

[@Birkesz](#): ebbol a hozzaszolosbol nekem ugy tunik, hogy te meg nem lattal linuxot kozelrol.

[Grigorij 2010.01.29. 09:12:36](#)

Eredetileg a íráshoz szerettem volna egy megjegyzést tenni, de a hsz-ek egy meghatározó csoportja kivágta a biztit nálam...

Írja már meg nekem valaki, hogy egyes "népcsoportok" - például az Apple hívők, német autó fanok vagy itt a linuxosok - miért ennyire kirekesztő, rasszista, alpári parasztok!?

Miért van az, hogy ezek a lények nem képesek az egymás mellett élésre? Miért van az, hogy ezek az alacsony IQ-jú majmok előszeretettel nézik le, szólják le, bélyegzik meg mindazokat, akik nem az ő elveik szerint élnek?

Miért gondolják, hogy a világ kizárólag az övék, hogy azok, akik bármit másképp gondolnak, azok megsemmisítendőkk???

A linuxos elfelejti, hogy az ő játékszere is csak EGY a világ IT termékei közül! Ugyanannyi jó és rossz tulajdonsággal, mint a többi...

És a világ - szerencsére - nem csak ifjú, zselés/copfós/rasztá kockás inges, szemüveges, kólavedelő és pizzazabáló webfejlesztőből, grafikusból stb. áll, hanem sok milliárd felnőtt emberből is!

[|Z| 2010.01.29. 09:17:03](#)

[@Viktus](#): Mindaddig, amíg a böngésződben látod azt, hogy mit hagysz jóvá, a böngésződben látod azt, hogy mit hagyál jóvá, a böngésződben futó kód azt jeleníti meg neked amit akarsz. Régebben ez elmélet volt ma már gyakorlat.

www.wired.com/threatlevel/2009/09/rogue-bank-statements/

[Birkesz 2010.01.29. 09:17:25](#)

[@igazi hős](#): Plíz, plíz, plíz, olvassad már vissza, miket írtam korábban. Nincs olyan sok komment. De hidd el nyugodtan, az átlag user lefagy attól, ha nem látja a négyszínű zászlót a jobb alsó sarokban, vagyis ha nem a megszokott kinézet fogadja. Nem a Firefox vagy a fejlesztői környezet a probléma, hanem pl az OpenOffice, ami nem képes teljesen 100%-os kompatibilitással megnyitni az MSOffice doksikat. Vagy vehetjük példának a játékok túlnyomó többségét: nem sok olyan van, ami alá nem kell emulátort futtatnod.

Pingwin: Nekem a Gnome menüje furá volt, számomra nem logikus (vagy csak kevésbé Windows-szerű) Nekem a KDE jobban bejött.

Aazami (törölt) 2010.01.29. 09:18:18

Nem értem ezt a Windows vs Linux vitát. Meg adathalászás. Már mindegyik banknál jó formán meg van az sms-ben küldött jelszó belépéshez, tranzakciókhoz. Ezt hogy is lopják el? Meg hogyan is tudnak utalni el a számlámról ha nekem jön az sms??? Akkor minek hardver kulcs?

Max. kártyával történő internetes vásárlásnál történhet gebasz, de ha időben jelzi az ember a banknak, hogy kártya visszaélés történt, a bankok általában megtérítik az összeget.

Na harcoljatok tovább a windows vs linux kérdésen.



pingwin • <http://pingwin.blog.hu> 2010.01.29. 09:18:53

@Birkesz: kde is szep :) talan az inkabb wines.

Birkesz 2010.01.29. 09:19:34

@pingwin: Láttam, rá is voltam kényszerítve hogy használjam (Windows alatt nem ment néhány program) de nem ragadtam le a Linuxnál. Egyrészt lustaságból, másrészt barátnő miatt, aki kategorikusan kijelentette, hogy nem hajlandó váltani. Innentől kezdve én sem erőlködök vele.

Birkesz 2010.01.29. 09:21:26

@Aazami: Nem mindegyiknél, sajnos. Pl. CIB bankban elég, ha tudod a jelszavakat és bent is vagy az Internetbankodban. Semmi HW kulcs, vagy SMS jelszó. Max egy üzenet, hogy beléptél.



pingwin • <http://pingwin.blog.hu> 2010.01.29. 09:24:33

@Birkesz: akkor jo regen lehetett, ha ilyenre emlekszel :)
cib-nel tenyleg nincs semmi, csak jelszo keres :/
pedig mindig mondjak milyen biztonságos, azt se tudom, hogy a java applet miatt mennyire az.



pingwin • <http://pingwin.blog.hu> 2010.01.29. 09:27:47

@Z: noscript

Birkesz 2010.01.29. 09:31:17

@pingwin: Mostanában nem figyeltem, hogy fejlődnek a szabad Office programok, pár éve még fennállt ez a probléma. De gyanítom, nem szűnt meg teljesen, mert az MSOffice is folyton változik, néha még annak is problémái vannak a saját dokumentumaival is :)

Az viszont biztos, hogy pár speciális program nem működik Linux alatt emulátor nélkül.

Aazami (törölt) 2010.01.29. 09:34:10

@Birkesz:

Az gáz. Én, mint banki IT-s nagyon nem hagynám a CIB IT vezetője helyében. De ez is csak addig fog menni náluk még nem kapnak egy fasza kis támadást mondjuk orosz honból, vagy a kínai teljesen baráti népköztársaságból :-)



igazi hős 2010.01.29. 09:36:36

@Birkesz: Részben igazad van a felhasználókat illetően (a jákékokat illetően pedig teljesen), de ismerek olyan helyet, ahol a rendszergazda azt mondta, hogy nincs IE, használj FF-t. 2 nap felháborodás (nemlehetdolgoznimegállazélet), aztán a felismerés, hogy ez nem rosszabb (sőt "beül a bohóc a sarokba és megmondja, hogy kint esik az eső!"). Ha mi is megtennénk mint a németek, hogy az államigazgatásban nincs MS Office, akkor heteken belül át tudnánk állni és nem kerülne többbe, mint egy éves MS licenz. (Persze a váltáshoz előbb ki kéne találni, hogy hogyan nyúljanak le sok pénzt egy ingyenes szoftverből, de én bízom a politikusainkban :-)



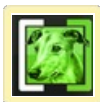
|Z| 2010.01.29. 09:37:08

[@pingwin](#): ööö, azt értem hogy a noscript miért segít abban hogy a kód ne kerüljön a gépedre, de hogy miképp segít abban, amikor natívan a böngésződben fut, azt már kevésbé értem. ja, és az átlag csipkártyás felhasználóról vitázzunk, ne a security paranoidról, aki 1%.



igazi hős 2010.01.29. 09:42:23

[@Aazami](#): Arról van szó, hogy te teljes nyugalommal utalod el az adódat, ami a sors (és egy távoli programozó) akaratából egy másik számlára érkezik meg. Pedig te csak egy cracket kerestél a múlt héten egy orosz honlapon...



// Gery Greyhound • <http://gerygreyhound.tumblr.com> 2010.01.29. 09:44:26

[@igazi hős](#): "az átlaguser böngészőt és office (szöveg- és táblázatkezelőt) használ."

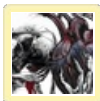
Vagy böngészőt és játékokat. Nem minden családban van irodai rabszolga, gyerek viszont annál inkább. Na, ők mit kezdenek a Linux-szal átlagfelhasználóként?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.01.29. 09:45:49

A legjobban az OTP SMS aláírása tetszik, ennek az értesítési telefonszámát CSAK személyesen lehet megváltoztatni. Vagyis ha kártyádat a telefonoddal lopják el, csak akkor bukó.

Viszont jó tudni, hogy a CIB-nél van lehetőség tokengenerátort kérni, és magára vethet, aki ezzel nem él. Mondjuk én nem választhatóvá, hanem inkább kötelezővé tenném, de ezzel megint itt vagyunk a biztonság VS kényelem kérdéskörénél. Nyilván engem az előbbi jobban érdekel, vélhetően viszont nem mindenkit.



Viktus 2010.01.29. 09:46:29

[@igazi hős](#):

Ahm , és a távoli programozó a teljes KH rendszert befolyásolja lásd. sms értesítés ... számla információ amit a KH központ ad le ...



pingwin • <http://pingwin.blog.hu> 2010.01.29. 09:46:45

[@Birkesz](#): nekem csak rtf-fel voltak problémáim.

a specialis programoknak lehet, hogy van native megfelloje -lehet, hogy nincs-

ha ebből: www.webupd8.org/2010/01/canonical-to-bring-closed-source-apps.html

lesz valami -> photoshop.deb? :)

az openoffice formatuma szabvány



pingwin • <http://pingwin.blog.hu> 2010.01.29. 09:47:37

[@Gery.Greyhound](#): vannak jó játékok linuxra is.

Aazami (törölt) 2010.01.29. 09:48:35

[@Viktus](#):

Ne én is ezt akartam írni igazi hősnek, csak elkéstem



pingwin • <http://pingwin.blog.hu> 2010.01.29. 09:49:51

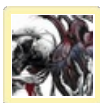
[@Z|](#): a noscript elvileg megakadályozza, hogy fusson, es csak az megy, amit engedsz, sztem így.

nekem szinte semmi nincs allando engedellyel, sokakat -pl család- idegesít, hogy allandoan engedelyezni kell, lehet, hogy tenyleg paranoid 1% vagyok, pedig atlag usernek hittem magam.

no mail, no problem 2010.01.29. 09:50:54

[@igazi hős](#):

na, ezt te komolyan gondolod, akkor szerintem neked se alapos gyakorlatod nincs mind az m\$, mind az open világban, továbbá vállalati IT-tse láttál belülről, vagy ha láttál is, az eléggé korlátos látás vagy IT volt. nem úgy van az, hogy pénteken legyakom a wint, hétfő reggelre meg minden ugyanúgy megy tovább linuxon, mint eddig. ez csak egy hagymázás délibáb egyesek fejében. ez a váltás sokkal bonyolultabb, mint hogy arra lehessen alapozni, hogy "nekem semmi problémám nem volt az ooo-val", és az "átlag jüzer csak wordot és excelt használ". és elárulom, hogy sokszor vagy nem is lehet, vagy nem érdemes váltani.



Viktus 2010.01.29. 09:54:26

[@no mail, no problem](#):

Sőt van sok olyan méregdrága program, amely még a következő win-el sem ügködik együtt rendesen.

no mail, no problem 2010.01.29. 09:58:18

[@Gery.Greyhound](#):

elvannak vele, mint befőtt. személyes tapasztalat. igaz, nálunk a számítógépes játszás nem töltött be se gyereknevelő, se időt agyonütő, se szülőket tehermentesítő szerepet. és a vérbölcsész gyerekeim máig linux felhasználó, aki agyfaszt kap egy windowstól.

no mail, no problem 2010.01.29. 09:59:49

[@igazi hős](#): pont az államigazgatás linuxra átállításával van a legnagyobb probléma.

|Z| 2010.01.29. 10:00:05

[@pingwin](#): "csak az megy, amit engedsz" . és mondjuk az a kód ami az egész gépedet uralja, az nem tudja felvenni magát noscript whitelistre? Meg azt sem értem miért feltételezzük, hogy a kód a böngészőben javascript alapon manipulálja a megjelenített html-t...



igazi hős 2010.01.29. 10:01:56

[@Gery.Greyhound](#): Gyereknek inkább konzolt, játékra jobb (persze meg kell venni a szoftvereket, ugye) vagy netes játékok.

[@Viktus](#), [@Aazami](#): Nem, csak és kizárólag a nálad levő appletet cseréli ki a sajátjára. Ez nem ördögösség.

[@no mail, no problem](#): Sőt még számítógépet sem láttam, csak halottam a Bélától, hogy nagyobb cégeknél olyan szinten nem lehet semmit telepíteni a gépekre, hogy egy image-ből húzzák fel az összes gépet, windowszal, office-szal, notes-szal, kismacskaival. Egyébként olyat közel sem írtam, amit te olvastál ki belőle, akkor azt mondtam volna, hogy ingyen van a váltás. 1 évnyi MS díj egy nagyobb cégnél milliókat, tízmilliókat jelent: ebből lehet oktatni, új policyt hozni, konvertálni, esetleg programokat átírni stb.



igazi hős 2010.01.29. 10:02:51

[@no mail, no problem](#): Mert az egész a MS zsebében van? e röhögtess, az "államigazgatás" elműködött BS2000 alatt is.

igazi hős 2010.01.29. 10:03:33



@igazi hős: "e röhögtesse"=Ne röhögtesse



pingwin • <http://pingwin.blog.hu> 2010.01.29. 10:04:07

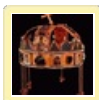
@no mail, no problem: francia rendőrségnek azért sikerült, meg nemetországban is.



pingwin • <http://pingwin.blog.hu> 2010.01.29. 10:05:44

@|Z|: miért uralja kod a gepemet?

ok, sztem legyen ez a vegszo :)



kitvalasztanal.hu - Választási tippért notebook! • <http://www.kitvalasztanal.hu> 2010.01.29. 10:07:11

@kermi: Nézd meg, hogy mikor írtam. Kora hajnali írásért csúfolódni nem vall sikeres emberre ;)

no mail, no problem 2010.01.29. 10:12:58

@Viktus:

ne is mondd. iszonyatos tapasztalataim vannak erről is. és a méregdrágát úgy kell elképzelni, hogy megvettek valami szart mondjuk többezer gépre, a licenc éves hosszabításban fizetendő, és 5-6 jegyű számokról beszélünk. dollárban, évente.

no mail, no problem 2010.01.29. 10:16:44

@igazi hős:

a vicc az, hogy valamilyen formában igen. tudok olyant, hogy egy cég ajánlatát a win->linux átállásról éveken keresztül arra használták, hogy árendeményt csikarjanak ki vele az m\$-tól. és gondolom némi megvesztegetést is, hogy mégis csak maradjon az m\$. komoly nyomás van ezen a piacon az m\$ részéről, csak nem látod kívülről.

Birkesz 2010.01.29. 10:18:10

@Csizmazia István [Rambo]: A CIB-es tokengenerálást nem említették, mint lehetőséget, amikor megnyitottam a számlámat náluk. Azóta pedig nem érdeklődtem utána, hogy bevezették-e. De köszi az infót, megyek is a bankba kérdezősködni.

Az átállás Linuxra főleg a szűkebb környezetben valósítható meg. Nagybátyám is lecserélte a biológiai laborban az oprendszeret debianra (ő is biológus egyébként) de ott max. 8 fő volt, akiket meg kellett győznie az előnyeiről. Nagyobb méretben ez már jóval nehezebb.

Az államigazgatásról és az állami tenderekről nem is beszélve.



igazi hős 2010.01.29. 10:20:19

@no mail, no problem: "komoly nyomás van ezen a piacon az m\$ részéről, csak nem látod kívülről." Sajnos. "A korrupció az amiből kihagynak."

no mail, no problem 2010.01.29. 10:27:08

@pingwin:

beszélj magyarországról, a francia rendőrség, meg a bonni önkormányzat kurva messze van. amiről én beszélek, ott nem lehet átállni, mert olyan egyedi fejlesztésű programok futnak, amelynek a fejlesztői konkrétan megtagadnak minden együttműködést, nem adnak ki semmilyen infó a programról, mert az számukra piacvesztéssel járhat. a program meg kell, törvény írja elő, hogy legyen. az új kifejlesztése évekre telik, és nincs rá pénz.

és sok olyan törvényt hoztak az elmúlt pár évben, amelyik határidőket szab eu-s jogharmonizációs (vagy hogy hívják) szoftverek üzembeállítására (egyes határidő már le is jártak), és semmilyen költségvetési erőforrást nem rendel hozzá. az

intézmény törvényis kötelezettséggel oldja meg, ahogy tudja, de természetesen az eddigi működését ne, csak költségvetését és létszámát csökkentse.

és akkor ott vannak az m\$ és ehhez hasonló gyártók, ahol saleseknek negyedéves terveket kell produkálni szoftver eladásra, mert különben kirúgják őket. na, onnét kurva nagy nyomás és hatékonyan megy a pénz elszívása.

Martian (törölt) 2010.01.29. 10:29:58

Hmmm... évek óta használok Windowst mindenféle direkt vírusvédő szoftver nélkül és még soha semmi rosszindulatú kód nem került a gépemre (egyébként főleg "kódhegesztésből" élek). Routeres tűzfal, script védelem és frissítőcsomagok persze fent vannak.

Ugyanakkor sok ismerősöm van, aki víruskergetőt is használ, mégis vírusos lett a gépe... nem értem.

no mail, no problem 2010.01.29. 10:30:34

@igazi hős:

köszí a bizalmat, de én nem azon a térfélen játszom, amelyiken részesülnek az osztás öröméből, ha érted, hogy mondom. de ettől még sugárban hányok tőle, hidd el.

Martian (törölt) 2010.01.29. 10:31:21

Szerintem általános irodai munkára a Linux sok esetben valódi alternatíva lehet.



pingwin • <http://pingwin.blog.hu> 2010.01.29. 10:32:55

@no mail, no problem: magyarországon is pl a rendorsegen sok linuxos cucc fut.



igazi hős 2010.01.29. 10:33:22

@no mail, no problem: Ilyet nem is feltételezek, legfeljebb ha az aláírásod mögött "államtitkár" vagy hasonló áll.

|Z| 2010.01.29. 10:35:33

@pingwin: mert a cikk arról szól hogy a felhasználók felénél fut ilyen kód...?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.01.29. 10:36:19

igazi hős:

Ez a korrupció az, amiből téged kihagynak, ez felejtethetetlen Hofi mondás.

Hogy az állami gépezet egyszer esetleg átálljon Linuxra, ahhoz szerintük kell majd egy Főbizottság, meg egy Sárkány Ellátó Vállalat, irodával, merdzsóval, gigászi költségvetéssel, stb.

Ajánlott olvasmány Moldova György örökbecsű Arrividerci Budapest című írása:

dydudu.hu/konyv/regeny/moldova/hivatal.html



kermi 2010.01.29. 10:40:11

A legnagyobb akadály állami szinten az átállás tekintetében szerintem a zseb. Milyen alapon várna a felső vezetés zsebpénzt egy ingyenes termék használata után? Magyarisztánban vagyunk. Itt kenőpénz nélkül a portás se köszön. Ez lehet a legnagyobb probléma.



igazi hős 2010.01.29. 10:49:04

@no mail, no problem: Érdekes, nekünk állami megrendelőknél a kódot letétbe kell helyeznünk (szerződösszegés meg egyéb

esetére). Bár nekünk is van olyan programunk, amiről nem tudnak elváltani (nem a mi hibánkból, egyszerűen belenőttek már), Linuxra meg horror áron portálnánk.

De a tömeg munkát át lehetne állítani nyílt szabványokra és programokra. Ha megtartasz néhány gépet (elég egy szervergép meg pár virtuális gép), akkor a speciális feladatokra is megmarad a megoldás. Tizenéve ugyanez ment: nyomda simán átállt Windowsra, de a levilágításra megmaradt a nagymaci.

Martian (törölt) 2010.01.29. 10:58:42

[@kermi](#): "Magyarisztánban vagyunk"

Euroisztán annyiban más, hogy ott csak nagy tételekkel dolgoznak zsebre... vagy eleve úgy alakítják a szabályozást, hogy zsebbe is pottyanjon valamennyi.



pingwin • <http://pingwin.blog.hu> 2010.01.29. 11:05:28

[@Z](#): ok

nam c kod fut :)



pingwin • <http://pingwin.blog.hu> 2010.01.29. 11:09:07

[@Z](#): winem alatt sztem nekem is fut



pingwin • <http://pingwin.blog.hu> 2010.01.29. 11:20:50

[@no mail, no problem](#): a francia rendorsegen, meg mas egyeb nemet allami szervnel biztos csak sztenderd dolgok mennek, es nincs semmi egyedi, mint ahogy a magyar rendorsegnek sem, de valahogy megis sikerul a fejlesztés.



igazi hős 2010.01.29. 11:33:28

[@pingwin](#): A magyar rendőrségen egy jól működő (értsd: az erőforrásokhoz képest jól működő) mainframe rendszer volt. Onnan (viszonylag) könnyű lett volna átállni egy másik platformra. (Csak azért viszonylag, mert egy évtizedekig fejlesztett rendszerben olyan aknák vannak, hogy ihaj. Párba mi is belefutottunk anno.)



Celtic 2010.01.29. 18:58:40

[@Birkesz](#): Es szerintem eleg is. Ha a jvm éppen nem kurva lyukas, akkor nagy bajod nem lehet (es persze nincs valami keylogger telepítve a gepedre)

Ennyiből a legstiztabb tenyleg egy livecd, elvegre a virtualis gepet hostolo gepen is lehet jo ki keylogger.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.01.29. 20:29:39

Egy kis Gartner a témához:

biztonsagportal.hu/fokozni-kell-az-internetes-bankolas-biztonsagat.html

Az Arrividerci, Budapest!-et elolvasta valaki?



gothmog 2010.01.31. 17:29:26

[@Martian](#):

És mennyire nyugodt szívvel mernéd ajánlani a saját módszeredet más egyszerű felhasználóknak?

[@Grigorij](#):

Mondd, te nem olvasod, amit írsz?



atomgoa 2010.02.01. 12:46:31

Windowst és Kubuntut használok, és csak annyit mondhatok, mindkét rendszernek megvannak a maga bajai. Linux alatt kompatibilitási problémák, Win alatt biztonságiak, ez van. A Win alatt sem használok root jogú fiókot, ennyit eltanultam linuxtól, ajánlom mindenkinek. Bank csak linux alól, ez sem 100% de közelebb van hozzá.

Aki pedig az állandó jelszóbeírkálást strapásnak érzi linux alatt, kíváncsi lennék, vajon az otthoni bejárat ajtaját is unja-e állandóan bezárogatni. Ugyanis mindkét dolog ugyanazért van: hogy nyugodt(abb)an alhassak.



röntgenszeműlány 2010.02.01. 13:36:03

@igazi hős: Értem, remek, és közben az egész tevékenységedet rögzíti egy keylogger. Igazán biztonságos.



gothmog 2010.02.01. 21:47:32

@atomgoa: Az "állandó jelszóbeírkálás" a végső érv a ms piárosaitól. Összességében egy ubuntu-júzer ritkábban ütközik bele, mint egy vista-júzer a figyelmeztető ablakokba.

Aki meg a kezelőfelület különbözősége miatt sír, az vesse már össze az xp felületét a win7-ével. Jajj-jajj, teljesen más a felület, hát hogy lehet ezt megszokni?

...



igazi hős 2010.02.01. 23:15:30

@röntgenszeműlány: Mármint azt logolja, hogy kattintottam egy ikonra? Nem bánom.

Vagy azt hiszed, hogy van olyan keylogger, ami a külső Windowson fut és a VPC eseményeit rögzíti? Nincs rá esélye.

Vagy a VPC-re települne fel a keylogger a külső gépből? Ez elég furcsa lenne.



Celtic 2010.02.02. 08:16:49

@igazi hős: Ikonra kattintva irod be a jelszavad? Mert ha billentyuzetrol, akkor tokmindegy, mennyire virtualis gepet hasznalsz. Vaeahogy a billentyuzet-host-virt.gep utvonalon el kell jutnia a leutesnek, nem fogja a host gepet atugrani.



igazi hős 2010.02.02. 08:34:11

@Celtic: Erre nem tudok érdemben reagálni, kérem kapcsolja ki, ovasson, tanuljon. Az érdeklődés/írástudás jelen esetben kevés.



röntgenszeműlány 2010.02.02. 11:51:49

@igazi hős: "Vagy azt hiszed, hogy van olyan keylogger, ami a külső Windowson fut és a VPC eseményeit rögzíti? Nincs rá esélye."

Hát pedig de, gond nélkül rögzíti. A virtuális gép ugyanúgy az operációs rendszeren keresztül éri el a hardvert, mint bármelyik másik program. Tess' szíves lenni kipróbálni, utána osztani az észet. Amit Celtic írt, az teljesen korrekt.

Az pedig, hogy egy biztonságtechnikai blogger ilyen tanácsot ad, az több mint ciki.



igazi hős 2010.02.02. 12:13:37

@röntgenszeműlány: Ilyen súlyú érvekkel ("Hát pedig de") nem tudok vitatkozni, feladom. Annyit azért javítanék, hogy ha:

- biztonságtechnikai blogger=biztonságtechnikai szakértő, aki blogot ír, akkor én nem vagyok az;
- biztonságtechnikai blogger=bárki, aki biztonságtechnikai blogba ír, akkor mindketten azok vagyunk és legalább az egyikünk téved. Ergo a színvonalat számonkérni nm szerencsés.



Celtic 2010.02.02. 12:15:49

@igazi hős: Nekem mindegy ugyan azt hallottam, hogy a hamis biztonsagerzet rosszabb, mitnha az ember tudja, hogy nincs biztonság, de nem szolok bele.



röntgenszeműlány 2010.02.02. 12:32:50

@igazi hős: Nem te vagy a blogger, és nem te adtad a tanácsot eredetileg, elég egyértelműen nem rád vonatkozott az a mondat. Te csak szimplán olyan kérdésekhez szólsz hozzá, amihez láthatóan kevés közöd van. Az érv pedig nem, hogy "hát pedig de", hanem a többi, amit Celtic írt, illetve én a komment többi részében írtam, és kegyeskedtél átugrani. Gondolom, mert halvány lila gőzöd sincs arról, hogy hogyan éri el egy virtuális gép a hardvert.

Ezért aztán nem szívesen terhelnélek olyan részletekkel, hogy bármelyik billentyű lenyomásakor keletkezik egy WM_KEYDOWN message, amit csak az a program nem kap el, amelyik nem akarja. Hogy emellett fut-e egy virtuális gép vagy sem, az tökéletesen irreleváns.

Mellékesen jegyzem meg, hogy ki is próbáltam.



igazi hős 2010.02.02. 14:02:15

@röntgenszeműlány: Nem mintha számítana, de nem mindegy, hogy hol vana te windowproc-od a "táplálkozási láncban", mert aszerint fogod látni vagy nem látni az üzeneteket. Azt mondd ki tudod próbálni, lássuk: ha ki tudod írni a windowsos programodból egy virtuális ablak handle-ját, már igazat adok neked és elhiszem, hogy van lehetőség az üzenetek logolására.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.02.03. 10:16:14**

Két dologra szeretnék reagálni. Az egyik a Linux kérdés. Abban a szerencsés helyzetben vagyok, hogy egyszerre használók háromféle rendszert: Win, Linux és Mac. A Linuxnak ez a driver kérdése tényleg nagyon gyenge láncszeme, érdemes csak a gyengébb ATI kártyások panaszait megkeresni a fórumokon. Egy XP vagy Win7-nél 100-ból százszor kapsz működő, 3D támogatást, itt meg sokszor csak a szenvedés van, az előzővel még ment, most nem megy, az előző disztribbel még ment, most fekete keret van, nem megy a 3d, stb. De TV kártyákkal, video digitalizálókkal is lehet hasonló kellemeseket szívni, egy idő után már az oprendszerhez érdemes vásárolni a megfelelő, kompatibilis hardvert.

A másik a VMware fertőzhetősége, támadhatósága, ebben röntgenszeműlány véleményét osztom, sajnos volt ilyen, van ilyen, lesz ilyen, még youtube videót is láttam róla, sőt vannak külön a shared folder kompromittálására is okosságok, tehát nagyon is kiszabadulhat a szellem a palackból, ha valaki elég okos hozzá. Érdemes tehát ebből is a frissítéseket, új verziókat haladéktalanul letölteni. Azt már csak zárójelben jegyzem meg, hogy olyan eset is van, mikor egy kutya közönséges 1.4 celeronra azt mondja a vmware player 3.x telepítője: "Error: This product can only be installed on a machine with CPU support for CMOV, PAE, TSC, and FXSAVE instructions" Ekkor vagy új gépet veszünk, vagy processzort cserélünk, vagy fogcsikargatva maradunk a támadható régi 2.x-nél :-(((



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.02.03. 10:20:12**

Vannak még Virtual PC, Virtual Box, stb. progik is. És még a VMware-hoz, ha a virtuális Windowst egy Linux hoston toljuk, akkor azért lehet reménykedni abban, hogy nyugalom lesz és a host tiszta marad. Windows alatt a Win esetében ez rizikósabb.

Face to Facebook avagy a svéd nekrofilok

2010.02.01. 19:20 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [adatvédelem](#) [facebook](#) [csalás](#) [csoportok](#) [kockázat](#)

A klasszikus Shakespeare idézet szerint ezt mondja Polónius: "No lend, and no borrow" (Arany János veretes fordításában "kölcson ne adj, ne végy!"). **Ha Polónius ma élne, intelmei között biztosan szerepelne valami ilyesmi is:** "És közösségi oldalakon vala ne csatlakozzál te semminemű csoporthoz, mert sosem tudhatod vala, mily szándékú halandók valának annak tagjai, és idővel milyen czélokat fognak követni".



Ma ismét adunk az *"Én egy egyszerű hétköznapi ember vagyok, ugyan mit tudnának nekem ártani a számítógépes bűnözők"* című tévészmének, közösségi oldalas történetekkel ismerkedhetünk. Meglepő módon azt is mondhatjuk, [csatlakozni egy Facebook csoporthoz kockázatosabb, mint egy direkt linken érkező kártevőre kattintani](#). De miért-e nagy maliciózus kijelentés? Bemelegítésnek mindjárt egy izgalmas Facebookos csoport jön, amelyik eredetileg magasztos és pozitív célok érdekében alakult: a Haiti földrengés áldozatainak gyűjtöttek adományokat. [Csalók azonban megváltoztatták csoport nevét Svéd Nekrofilek Egyesületévé](#), sőt még egy üzenetet is kiírtak a csoport weboldalára: "Ahogy mindnyájan tudjátok, a Svéd Nekrofilek Egyesülete 500 ezer koronát adományoz arra a célra, hogy a Haitiról visszahozott holttestek minél jobb állapotban legyenek, hogy közösülhessünk velük".



Egyáltalán nem vicces a dolog, és valószínűleg senkinek nem hiányzik, hogy a nevét leendő munkaadója egy ilyen tömörülésben találja meg. Egy érdekes felmérés szerint az **amerikai személyzetisek 70%-a** utasított már el állásra jelentkezőt amiatt, hogy negatív lett a közösségi oldalakról begyűjtött információ a jelöltől. [Figyelemreméltó naivság, hogy ennek ellenére a leendő álláskeresőknél mindössze csak a 7%-a gondolja úgy](#), hogy ezek az adatok egyáltalán befolyásolhatják a pályázatukat.



Volt aztán egy [Fan Check](#) nevű Facebook alkalmazás is, amely elméletileg profilunkon keresi meg, hogy mely ismerősünk írt/kommentelt a legtöbbet a dolgainkra. A gyakorlatban ehelyett azonban a kezdőlap összezavarását lehetett tapasztalni, és nem mindig jelenítette meg az új postokat sem, néha régieket tett előre, stb. Összefoglalva: "Elméletileg nincs különbség elmélet és gyakorlat között. Gyakorlatilag van." Nem egyedi eset azonban a Fan Check, [divat lett a dologból a Facebook kiegészítők háza táján](#), és ezekből a kártékony kisalkalmazásokból [egy egész csokorra valót nevez meg Roger Thompson](#), az AVG szakértője.



Éppen pár napja keletkezett egy vakriadó a Facebookon, amiben arra hívták fel a figyelmet, ha valaki egy "unnamed app", magyarul névtelen alkalmazás nevű holmit talál magánál, akkor azonnal törölje, mert az állítólag kémprogram. Persze nem az, de az már az ötletgazdák képzelőerejét dicséri, hogy a Google találatok kártevőkkel való mérgezésével rákészültek a szituációra, ha az egyszerű Facebook jüzer rákeres az "facebook unnamed app" kulcsszóra.



És végezetül ismét a csoportok, fan klubok kérdését vegyük elő. **Van-e értelme klubtagnak lenni? Mi is történik ilyenkor, nézzük meg.** Belépünk a Dr. Schön Ubul Ferencvárosi Szurkolói Körbe, vagy az "Új Élet" Koporsókészítő Kisipari Szövetkezet Barátai közé és nem tudjuk pontosan, kié a klub. **Nem tudjuk, kik a tagjai. De azt tudhatjuk, hogy mint ismerős, minden "csak az ismerősök láthatják"** adatunkat megnézhetik. **Van tíz, száz, ezer vadidegen ember, és mi Róbert bácsiként önként odaajándékozzuk nekik a bizalmas személyes adatainkat**. Nem tudjuk, milyen adatkezelési irányelveket vallanak magukénak, ha egyáltalán hallottak ilyesmiről. Nem tudjuk, milyen körülmények között tartják nyilván az adatainkat. **Nem tudjuk, eladják-e harmadik félnek, ha kapnak egy jó ajánlatot.** Nem tudjuk, nem lopják-e el egyszer tőlük, mert abc123 típusú jelszót választott magának a klubelnök.



Mire lehet használni ilyen személyes adatokat? Hát először is lehet szipkázni olyan infót, amivel jól válaszolhatunk a jelszóemlékeztető kérdésekre. De új típusú csalások is terjedőben vannak, például a személyes lapról kinézett barátok nevében Facebook üzenetet írnak az áldozatnak, hogy állítólag elvesztették a reptéren a mobiljukat, pénztárcájukat, útleveleket. Több alvázózat is ismeretes, de a lényeg, gyorsan egy kevés pénz segítséget szeretnének kérni, általában a Western Unionon keresztül. Ha valaki pedig segítőkész és bedől, keresztet vehet az ilyen átutalt pénzre.



A nemzetközi helyzet fokozódik, és kafferbivalybalamber egyik remek kommentjét idézve: **"Az optimista angolul tanul. A pesszimista kínaiul tanul. A realista lőni tanul."** Azt hiszem, emellett a személyes adatainkkal való bánásmódot pedig mindannyiunknak meg kellene már tanulni.



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



Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1720286>

Kommentek:

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



Ugyanezt eljátszották az egyik Jobbikos csoporttal. Csak ott valami undorító buzis dologra írták át a nevet.

Conficker a rendőrségen

2010.02.03. 19:00 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [microsoft windows usb rendőrség kulcs panda fertőzés féreg eset autorun vaccine conficker](#)

Nem, nem és nem, sajnos nem bilincsbe verve vádlottként került bekísérésre, de ott volt minden kétséget kizáróan. A Manchesteri rendőrség számítógépein, és ezzel kb. három napra meghiúsult a feltételezett elkövetők és a gyanús gépjárművek ellenőrzése.



Mintha egy korábbi posztunk támadt volna föl Főnix madárként, ahol a [buszsáv bírságok határidőre való kézbesítése szenvedett csorbát a Conficker féreg miatt, így a gyorshajtók megúszták](#). Lehet, hogy nemzeti játék lett a "Conficker férget az állami hivatalokba" öntevékeny mozgalom? Vagy csak véletlen? Vagy pedig a rendőrségi IT vizsgázott rosszul?



Mint az közzismert (mondaná Safranek) a Conficker egy olyan hálózati féreg, amely a Microsoft Windows egyik biztonsági hibáját kihasználó exploit kóddal terjed, gyenge admin jelszavak elleni támadással, **valamint az automatikus futtatási lehetőségén keresztül is terjed a fertőzés**. Bár az RPC (Remote Procedure Call) vagyis a távoli eljáráshívással kapcsolatos sebezhetőséghez már 2008. októberben kiadták az MS08-67 jelű Microsoft biztonsági javítócsomagot, amely elhárítja a hiba kihasználhatóságát, ennek ellenére **sok Windows alapú számítógépen nem fordítanak elég figyelmet a naprakész vírusvédelem mellett az operációs rendszerre is**, idézőjel bezárva.



A mostani esetben is nagy valószínűséggel **egy külső csatlakoztatott USB kulcs volt a bűnös**. A gépek megtisztítását és visszaállítását azóta elvégezték, a [közlemény szerint adatvesztés nem, csak hálózat forgalmi probléma](#) történt. (Az adatvesztés valószínűleg azt jelenti, hogy ők megtalálták mindent, ami eredetileg a gépeken volt, de arról nem szól a nyilatkozat, hogy az ő adataik kiszivárogtak-e.)



Arról is elfilozofálgattunk korábban, [miért jó, kinek jó, negyven évvel a Holdra szállás után egy ilyen Autorun nevű vírusról a Windows rendszerekben](#). Van egy olyan ősi dakota közmondás, miszerint "egy helyiségbe belépve a tetszetős belépővel szemben mindig fordíts nagyobb gondot a szerencsés távozásra".



Ezt jelen szituációra adaptálva Randy Abrams úgy mondja: "Jó lenne, ha a Microsoft csak fele annyi energiát áldozna az Autorun kérdésre, mint amennyit a WGA-ra (Windows Genuine Advantage)". Szerintem is kontrázva mehetnénk fel a Himalájára. Kicsit abszurd a helyzet, vagy inkább szégyen, mikor külsős cégeknek, független AV vállalatoknak kell közreadni [módszereket mint például az ESET hogyan kapcsoljam ki útmutató](#), vagy kifejleszteni olyan eszközöket, mint például a [Panda USB Vaccine, amelyik nem csak a helyi Windowsban, hanem a később a rendszerbe bedugott USB eszközökben is](#) lekapcsolja ezt kártékony automatikus feature-t.



Hé fiúk, halló Redmond, kapcsford, itt MZ/X vétel, kapcsoljátok már ki végre alaphelyzetben azt az átkozott Autorunt! Phfff, szerintem nem is hallják :-)

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [Akiknek a Captcha kinszenvedés](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1725178>

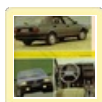
Kommentek:

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

[Aazami \(törölt\) 2010.02.04. 08:18:17](#)

Akkor ezek szerint az angol rendőrség nem egyforma verziójú op. rendszert használ? Szóval bárki bármilyen op. rendszert telepíthet, vagy mindenki teljeskörű admin jogosultságot kap a gépéhez, és saját maga választja mikor frissíti az op. rendszert vagy vírusirtót??

Szép!!!



[biturbo s - félázsiai bunkó állat](#) •

<http://oldfordworks.blog.hu> 2010.02.04. 08:27:35

Bármelyik m\$ oprendszer telepítőlemeze egyvalamire jó: megfogni, és behajítani a kukába. Aztán meg feltenni linuxot vagy bsd-t.

Az álca románca

2010.02.08. 19:50 | [Csizmazia István \[Rambo\]](#) | [12 komment](#)

Címkék: [windows frissítés](#) [hamis trójai](#) [ál antivirus](#)

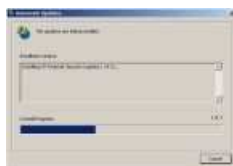
[Álcázás, hamisítás, csalás](#). Hányszor hallottuk már ezeket a szavakat? Ám ahogy a mondás tartja: "semmi sem állandó, csak a változás maga", egyre újabb és [trükkösebb átverésekkel jelentkeznek az ál-antivírus](#) készítőik csapata.



Ha valakinek esetleg nem volt eddig valódi vírusvédelem a gépen és pont [belegyalogolt egy hamis antivirusba](#), vagy csak érdekli a téma iránt, [fejest ugorhatott a How to Remove kezdetű](#) feljegyzésekbe.



Lassan már mindenkinek pavlovi reflexévé válik, hogy ismeretlen nevű antivirus vagy kémirtó programot ne telepítsen, vagy [előtte nézzon utána, valóban elnyerte-e a Cnet, PC World, vagy éppen a Softpedia Editors Choice díjat](#). Esetleg csak a [How to Remove díjat nyerte el](#). Éppen ezért ideje váltani - gondolták a trükkös fiúk, és azon tűnődtek, vajon mire kattint mindenki gondolkodás nélkül.



És igen, jutott eszükbe számtalan szebbnél szebb gondolat, míg állni látszott az idő. [Végül megoldották és megszületett a Windows biztonsági frissítési ablaknak látszó tárgy](#). Erre sokan, és mindenféle gyanakvás nélkül kattintanak az emberek, hiszen egy ilyen Microsoft frissítés olyan megbízhatónak látszik.



A végeredmény azonban sajnos ugyanaz, a naív felhasználó entert üt, [az ál-antivírus települ, a hamis riasztások jönnek, a teljes verzió reményében pedig az emberke a bűnözőknek fizet](#). A trükkre [mi mást is mondhatnánk, mint hogy: ügyes](#).

[Tetszik](#) [Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.](#)

[Megosztás](#) [+1](#) [0](#) [Tweet](#)

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés [trackback címe](#):

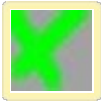
<http://antivirus.blog.hu/api/trackback/id/1739756>

Kommentek:



[nézz](http://www.ejatekok.com/) • <http://www.ejatekok.com/> 2010.02.08. 20:57:12

Svindlerek :)



[twollah / bRoKEn hOPe, sUppLeX](http://freewaresoftwarenews.blogspot.com/) • <http://freewaresoftwarenews.blogspot.com/> 2010.02.08. 21:00:03

Sok a naiv ember a vilagon.

Eleg ha beírja a keresobe, hogy spybot es a masodik talalat a roy
SpyBot-Search & Destroy.

Vagy ezen az oldalon (freewaresoftwarenews.blogspot.com/) beírjuk, hogy spybot es kidob egy rakat normalis eltavolitot.



[bandika57](#) 2010.02.08. 22:00:04

Használj Linuxot , OSX-et, Solarist és nem fenyegetnek ilyen marhaságok.

[Gyagyás Tóni \(törölt\)](#) 2010.02.08. 22:10:24

[@nézz](#): Akik ügyesek.

[Dr. Schwanzkopf Rudolf](#) 2010.02.08. 22:16:15

Én miért nem futok bele soha ilyen izékbe...

[Johnfive](#) 2010.02.08. 22:35:21

Ja, Solarist desktop OS-nek...Ilyen jótanácsok mellett nem is kell vírust telepíteni: a szopás garantált. (OS X, Linux detto)



[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu> 2010.02.09. 10:39:12

Johnfive:

Tetszik a hozzászólásod, és vicces is :-)

Solarist még sosem használtam, de az OS X-re és Linuxra állíthatom, nincs orális fixáció egyáltalán, sőt öröm és bódottá van helyette :-D

Egyébként meg: "Minden egyszerű, ha már eltöltöttél néhány évet a hozzászokással"



[atko](#) 2010.02.09. 19:16:40

[@Johnfive](#):

Virtualboxban most is futtatok egy Solarist Linux alól.

Alapból Kde 4.x.x -el települ. A napi használatban nem vettem észre, hogy más lenne, mint bármely Linux.

Ami otthon kell az van rajta mivelhogy KDE. Ha jól emlékszem talán még Gnome is van hozzá.

A post témájához meg annyit, hogy aki nem tudja miről van szó az ne csinálja.

Érdekes az senkinek sem jut eszébe, hogy miután megtanulta a sebtapaszt használatát műtéteket végezzen költségcsökkentés végett.



atko 2010.02.09. 19:36:13

[@atko](#): javítom:alapból Gnome.



gothmog 2010.02.09. 22:12:00

Jé, ilyenrel hozta a minap egy jó barátom a laptopját. Igaz, az nem XP internet securitynak nevezte magát, hanem valami security control centernek, de a grafikai elemei ugyan ezek voltak. Viszont nem engedett belépni a windowsba, amíg nem kattintottam a "buy full version" gombra. Kedves jószág.



gothmog 2010.02.09. 22:19:40

[@Johnfive](#): márpedig a Linux jóbarát. És ezt olyan windowst ismerőseim tanúsíthatják, akiknek az ilyen-olyan okból elpusztult winjéből valamely linuxos live-cd segítségével sikerült kimenteni fontos/pótolhatatlan fájlokat.



atko 2010.02.10. 14:59:00

[@gothmog](#): A live Linux cd-ről olvastam egyszer, hogy az olyan a wines felhasználónak mint halásznak a vízen járás.

Fertőző weboldalak is terjesztik a kártevőket

2010.02.10. 16:10 | [Csizmazia István \[Rambo\]](#) | [7 komment](#)

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

[Bármely weboldal kódjában lehet olyan rosszindulatú JavaScript kód](#), amely kártevőket kísérel meg letölteni a látogató számítógépére.



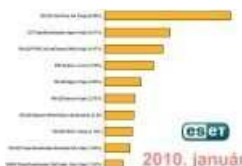
Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes kártevők toplistáját, melynek elemzése mindig tanulsággal szolgálhat a felhasználók számára. A tízes lista élmezőnyéből a régóta listatag Swizzor és Kryptik trójai kicsúszott, helyettük a még decemberben feltűnt Win32/Injector trójai és egy vadonatúj JavaScript kódú kártevő forgatta fel a helyezési rangsort.

A jelenleg második helyezett JS/TrojanDownloader.Agent trójai újonc a top listában. Általában kártékony weboldalokról érkezik, és további rosszindulatú kódokat kísérel meg letölteni a fertőzött számítógépre, amelyeket aztán el is indít. A JavaScript kód a felhasználó tudta és beleegyezése nélkül képes futni, és a trójai arról is gondoskodik, hogy az ablakát végrehajtás közben elrejtse előle.



Továbbra is a középmezőnyben foglal helyet a múlt hónapban felkerült Win32/Injector, amely a megtámadott gépen hátsó ajtót nyit, és a newvalarsrent.ru weboldalhoz csatlakozik. Innen további fájlokat próbál meg letölteni. Rootkit komponenssel is rendelkezik, működése során fájlokat rejt el a fájlkezelő alkalmazások elől (pl. EXPLORER, FAR MANAGER) még akkor is, ha ezek nem rejtett attribútummal rendelkeznek.

A listavezető Conficker féreg pedig már 2009 októbere óta őrzi az első helyét, aminek nagy valószínűséggel az az oka, hogy sok Windows alapú számítógépen még mindig nem fordítanak elég figyelmet az operációs rendszer frissítéseire, de a gyenge admin jelszavak, az automatikus Autorun funkció bekapcsolt alapállapota is jócskán felelőssé tehető. Emellett folyamatosan számtalan új variáns, módosított változat is megjelenik belőle, melyeknél a készítők rendre igyekeznek tesztelni és kijátszani a felismerést.



Végezetül következzen a magyarországi toplista. Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2010 januárjában az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. Ezek együttesen 35.8%-ot tudtak a teljes tortából kihasítani maguknak.



1. Win32/Conficker.AA féreg

Elterjedtsége a januári fertőzések között: 9.68%

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 eljárason keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.

Bővebb információ: <http://www.eset.hu/virus/conficker-aa>



2. JS/TrojanDownloader.Agent trójai

Elterjedtsége a januári fertőzések között: 5.01%

Működés: A JS/TrojanDownloader.Agent kártevőcsoport egyik fajtája a JS/TrojanDownloader.Agent.NRL trójai. Ez a károkozó általában kártékony weboldalakról érkezik, és további rosszindulatú kódokat kísérel meg letölteni a fertőzött számítógépre, amelyeket aztán el is indít. A JavaScript kód a felhasználó tudta és beleegyezése nélkül képes futni, és a trójai arról is gondoskodik, hogy az ablakát végrehajtás közben elrejtse előle.



A számítógépre kerülés módja: Fertőzött weboldalakon keresztül

Bővebb információ: <http://www.eset.hu/virus/trojandownloader-agent-nrl>



3. Win32/PSW.OnLineGames.NNU trójai

Elterjedtsége a januári fertőzések között: 4.47%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók 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/virus/psw-onlinegames-nnu>



4. INF/Autorun vírus

Elterjedtsége a januári fertőzések között: 3.76%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájl 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/virus/autorun>



5. Win32/Agent trójai

Elterjedtsége a januári fertőzések között: 2.80%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (például Temp mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/agent>



6. Win32/Injector trójai

Elterjedtsége a januári fertőzések között: 2.33%

Működés: A Win32/Injector trójai olyan Registry bejegyzéseket, illetve külön állományokat hoz létre a számítógép megfertőzésekor, amelyek egy esetleges újraindítást (bootolást) követően aktivizálják a kártevő kódját és gondoskodnak annak automatikus lefuttatásáról. A Windows System32 mappájában (alapértelmezés szerint C:\Windows\System32) található wsnpoem, illetve ntos.exe árulkodó jel lehet. A megtámadott gépen hátsó ajtót nyit, és a newvalarsrent.ru weboldalhoz csatlakozik, ahonnan további fájlokat próbál meg letölteni. Rootkit komponenssel is rendelkezik, működése során fájlokat rejt el a fájlkezelő alkalmazások elől (pl. EXPLORER, FAR MANAGER), még akkor is, ha ezek nincsenek ellátva rejtett attribútummal.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/injector-k>



7. Win32/Adware.WhenUSave alkalmazás

Elterjedtsége a januári fertőzések között: 2.24%

Működés: A Win32/Adware.WhenUSave működése során létrehozza a saveupdate.exe nevű állományt. Az ilyen, nem kifejezetten kártevő, hanem inkább a veszélyes vagy nem kívánt programok kategóriába tartozó kénytelen reklámprogramok sok esetben élnek olyan trükkökkel, hogy különféle további könyvtárakban is létrehoznak magukból másolatot. Ennek kettős célja van: egyrészt egy esetleges vírusirtást követően egy eldugott helyen megmaradhatnak a fertőzött állományok, másrészt helyi hálózatokban, megosztott könyvtárakban, peer 2 peer hálózatokban is képesek terjedni. Futása során megkísérel a web.whenu.com weboldalhoz kapcsolódni, ahonnan kénytelen reklámokat, valamint saját programfrissítéseit tölti le. A fertőzött gépen aktív böngésző esetén linkeket, időjárás-jelentést és más kénytelen reklámokat jelenít meg.



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

Bővebb információ: <http://www.eset.hu/virus/adware-whenusave>



8. Win32/VB.EL féreg

Elterjedtsége a januári fertőzések között: 2.13%

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/virus/vb-el>



9. Win32/TrojanDownloader.Bredolab.AA trójai Elterjedtsége a januári fertőzések között: 1.95%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, mely távoli oldalakról további kártékony kódokat tölt le és hajt végre. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságítámozgatás-szolgáltató (SSPI - Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.



A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: <http://www.eset.hu/virus/trojandownloader-bredolab-aa>



10. WMA/TrojanDownloader.GetCodec.gen trójai Elterjedtsége a januári fertőzések között: 1.43%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámlablakokat jelenít meg a számítógépen.



A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: <http://www.eset.hu/virus/trojandownloader-getcodec-gen>

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Tízből öt kártévő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Nyári tanácsok utazáshoz](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1745022>

Kommentek:

[tdk.112 2010.02.10. 17:03:27](#)

NoScript. :-)

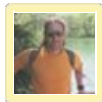


[samcro 2010.02.11. 23:29:12](#)

[@tdk.112](#): Ja, tökjó a NoScript, kivéve ha whitelisten lévő oldal fertőz.

[kdeurhj 2010.03.03. 17:43:42](#)

Szia! A jelszó ellopását ki tudom úgy védeni, hogy mindig egy pendriveről másolom be?



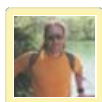
[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu>](#)
[2010.03.06. 12:38:27](#)

Szia Kdeurhj!

Ez sok mindenben múlhat, a kérdés pedig rövide, és nem is tér ki mindenre. A lényeg szerintem nem csak az, honnan veszed elő, hanem hogy hova gépeled/kopipasztázod be. Ha már beírtad, akkor ugyanúgy ott van, mintha kézzel írtad volna be. Az előttem szólók már jól megdicsérték a Noscriptet, és igazuk van, sokat lendít a dolgokon, de sok átlagjuzernek sajnos nincs hozzá türelme állandóan kattintgatni. Ha én lennék a Mozilla, ezt a noscriptet gyárilag már rég beleépítettem volna a termékbe, aztán aki nem akar vele élni, kapcsolhassa ki.

[kdeurhj 2010.03.22. 00:29:15](#)

[@Csizmazia István \[Rambo\]](#): Kösz! Banki belépésnél szerettem volna elkerülni a jelszólopást. Talán a Linux LiveCD a legjobb megoldás, a RAM-ból remélem nem lehet ellopni.:) Azt mondják, hogy a Linux biztonságosabb, bár nem értem, hogy a tűzfal miért nincs alapból bekapcsolva és az Eset is készíti már vírusírtót, biztos ami biztos. A noscriptet és nem bírtam sokáig használni, de érdemes megnézni, hogy mennyi minden akar "betöltődni". Internet használat biztonságára mennyire jó a Sandbox? Az elkülönített részből tényleg nem tudnak "kijönni" a fertőző elemek?



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu>](#)
[2010.03.22. 11:13:55](#)

Linux Live CD-nél vagy Windsows alatt virtuális gép alól indított Linux alól szerintem kiválóak az esélyeid a biztonságra, úgy gondolom, nem tudnak "kijönni" :-)

[kdeurhj 2010.03.22. 11:37:08](#)

[@Csizmazia István \[Rambo\]](#): Kösz!

A fű zöld, a másolók másolnak

2010.02.11. 18:25 | [Csizmazia István \[Rambol\]](#) | [7 komment](#)

Címkék: [kaspersky](#) [virustotal](#) [vírusfelismerés](#) [szignatúra](#) [kártevőelemzés](#)

Eredetileg valamilyen [Valentin napi virtuális képeslapos figyelmeztetést](#) gondoltam írni, de aztán valami eltérített az eredeti szándékomtól. Sebaj, a legtöbb ilyen [fertőzött linkkel rendelkező képeslap amúgy sem magyar nyelvterületen](#) csörgeti láncait, és már írtunk is hasonló tárgykorben [korábban néhány szösszenetet](#).



Szóval nagyban zajlik az élet az Aprajafalvi víruslaborban. Először Álmodozó szól kávéscsészével a kezében, hogy megérkeztek a honeypotos kártevő minták, **aztán Ügyi jelenti, hogy a vírusminták a VirusTotalról is itt vannak már**. Dulifuli figyelmezteti Ügyifogyit, hogy ezek között sok ám a sérült, működésképtelen minta, és arra nagyon kell vigyázni, hogy csak valódi, életképes kártevőre történjen a riasztás. Okoska **már készített egy olyan jó kis programot, ami egy adott könyvtárból felolvasva automatikusan teszteli a mintákat**, így már csak az marad hátra, hogy a maradékot Törp Papa utasításai szerint kiosszák és elemezzék.



Kérdés csak az, van-e hasonlóság a törpök és valódi szereplők között. Eddig tart az idilli kép, a dolog akkor vehet izgalmasabb fordulatot, ha például az egyik csapat azt látja, hogy saját felismerési adatbázisát mintha túl gépiesen követné egy vagy több másik antivírus motor. Egy korábbi történetben már szoltunk arról, [hogyan pirított rá Harun Al Rasid vagy Mátyás Király módra a Malwarebytes az IObitre](#). Most a Kaspersky csapat érezte úgy, megrendezi az igazság pillanatát. Kicsit vitatható módon tették ezt - hasonló erkölcsi aggályok merülhetnek fel, mint [a BBC botnet bérlése](#) vagy az [Amerikából jöttem, mesterségem címere: Csalószivató](#) című cikkben korunk Robin Hoodjainak néha újságcikket és bankszámlát is hamisítaniuk kell a gaz spammerek móresre tanításánál.



A Kaspersky Lab úgy gondolta, megleckézteti a versenytársakat, és 20 teljesen ártalmatlan állományt feltöltöttek úgy a VirusTotal oldalra, hogy szándékosan hamisítva kártékonynak jelezte őket a saját motoruk. Kis idő (10 nap) elteltével aztán 14 további antivírus is riasztott már ezekre (mint az közismert, ugye a mintákat minden AV labor egy idő után megkapja elemzésre). [Ekkor borították a bilit](#), és Moszkvában újságírók előtt bemutatták, a blogjukban pedig megírták a leleplezést.



Félreértés ne essék, az addig egy teljesen logikus és indokolt lépés, amikor egy gyanús fájl a hétköznapi ember, vagy a kártevő elemző bedob a VirusTotalba. Inkább az lehet a történet egyik tanulsága, hogy ne bambán, érdemi elemzés és gondolkodás nélkül minősítsenek egy állományt kártékonynak. Ez a nehezebb út, de az érdekesebb is, olyan sikerekkel kiköveve, mint [Mark Russinovit](#) [Sony rootkites leleplezése](#) például.



Néhányan, köztük David Harley az ESET laborjából kritizálta a vitatható módon végzett kísérletet, többen pedig a publikus helyszínen való beszámolót nehezményezték [a szakmán belüli, pl. AMTSO elintézési mód helyett](#). A történet jó reklám a Kasperskynek, de a valódi megoldást a laboroknak a minták tényleges elemzéseinek elvégzése adja. A [VirusTotal sem tartotta korrektnek a lépést](#), bár

természetesen tisztában voltak azzal [az inkorrekt gyakorlattal is, amely ellen ez az akció történt](#). Mindenesetre látszik, **a vírusvédelmet nem pótolhatja egy ilyen kártevő elemző weblap, és annak eredménye sem szentírás**. Ahogy azt [VírusTotal weboldal szövegeinek magyarázója :-\)](#) frappánsan megfogalmazta:



vagy kicsit másképp: "A gravitáció nemismerete nem mentesít a zuhanás alól".



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](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1749481>

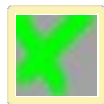
Kommentek:

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](#).



[DanZi 2010.02.12. 00:17:08](#)

Csizi, van egy humorod :) remélem már rég Mac-et használsz otthon :)



[twollah / bRoKEN hOPe, sUppLeX • http://freewaresoftwarenews.blogspot.com/ 2010.02.12. 04:28:04](#)

Tokenes virusirto nincs.
Inkabb legyunk gyanakvoak.

[tom sailor 2010.02.12. 06:12:26](#)

[@twollah / bRoKEN hOPe, sUppLeX](#): Dehogyan nincs. Format c:
:)

[Ajtony 2010.02.12. 07:32:52](#)

Sziaztok! Az egyik gépem nagy csinnadrattával torolt egy vírus az irtó program, a neve: microsoft eredetiség ellenőrző "akarmi" volt. :-)



[Krajcs • http://uralicowboy.blog.hu 2010.02.12. 08:55:20](#)

[@Ajtony](#): Már a warez verziók sem a régiéek... ;)

[különvélemény 2010.02.12. 09:08:50](#)

Már épp ideje volt.

Egyes remek vírusirtók szó nélkül törölnek olyan állományokat, amik nem tartalmaznak vírust, csak bizonyos cégek úgy gondolják így harcolnak a warezolás ellen.

Bár szerintem az algoritmus sem lehet túl bonyolult:
keygen.exe -> Generic.dx Trojan

Üzenném az ilyen remek vírusirtóknak, mint pl a mekkáfé, hogy elég csak a fájlnévet ellenőrizni, felesleges belenézni az állományba, így azzal is villogtathatnák hulladék terméküket, hogy mennyire gyors.

különvélemény 2010.02.12. 09:30:44

[@tom sailor:](#)

A bootvírusok, bár nem túl népszerűek mostanában, túléltek a formacét.

Az a lényeg, hogy ragadjon a bélyeg

2010.02.15. 20:50 | [Csizmazia István \[Rambol\]](#) | [4 komment](#)

Címkék: [microsoft xp frissítés kékhálál](#)

Mindent próbálnak a [hamisítani, megtévesztéshez felhasználni](#). Nincs ez másképp a [Microsoft Essentials](#) programmal sem. De előtte még egy kis ungabunga ;-)



Ugyanis első közelítésben más aspektusban jutott eszünkbe a Microsoft, [lévén az egyik gépünk beleesett a szokásos frissítés keretében előállt lefagyásos-újraindulásos népi játékba](#), pedig semmilyen kártevő vagy rootkit nem szerepelt rajta. A tanácsolt remedy-eket követve eleinte semmilyen eredményt nem sikerült elérni, **szinte a Blaster féreg sebességével indult mindig újra és újra a gép**.



A "felejtethetlen" Lugossy Béla helyett a felejtethetlen Blaster

Gépet indítjuk, nézegetjük mi van - hopp újra indul. Gyorsan a másik linuxos gépen [a HUP cikke alapján keresgélünk](#), ahol egy forrás [az XP atapi.sys kompromittálódására esküszik](#). Próbálkozzunk: **Recovery CD betesz, atapi.sys expandál, gép restart, és várjuk az eredményt. Helyette hibaüzenet, hopp megint újraindul**. Bill Gates felmenői ijesztően barbár, alpári stílusban és kontextusban tolnak ajkainkra.



Stratégia váltás és újabb, ezúttal saját elmés ötlet jön. "A leghosszabb utazás is egyetlen lépéssel kezdődik" jegyében apró lépésekkel haladunk céljaink felé: megpróbáljuk a gépet egy korábbi rendszerállapotra visszaállítani. Indítás után a rendszer visszaállítás keresése, hol is lehet, hol is lehet - hopp a gép újraindul. Restart után gyorsan a Programok - Kellékek - Rendszereszközök - Rendszer-Visszaállítás ikonját a Startmenüre ejtjük, és máris hopp, újraindul a rendszer. A következő újraindulás után már így gyorsan tudjuk indítani a start menüből, **hadd szóljon az a korábbi február 8-a**. A visszaállítást szerencsére átvészeli a gép, és nem kell már senki anyját szidjuk, végre helyre áll a rend és a béke. Az igazsághoz tartozik, hogy **több különböző vírusvédelmi programmal is átvizsgáltuk a gépet, és semmilyen állítólagos rootkit vagy kártevő nem volt rajta**, az egyetlen bűne talán az lehetett, hogy Fujitsu a gép típusa ;-)



Visszakanyarodva hosszára nyúlt bevezetőnk után mai mondandónkra, **a biztonságért folytatott küzdelemben talán a félműveltség a legnagyobb veszély**. Erre példa a mai ál-vírus irtó is, hiszen aki abszolút nem ért a géphez, az nagy valószínűséggel megkérdezi, megkér valakit, aki jobban ért hozzá, hogy segítsen. Aki viszont fél füllel már hallott ezt-azt, és úgy gondolja, már mindent tud, [és emiatt ismerősen cseng neki a Security Essentials 2010, annak pechje van](#).



Ez ugyanis nem a Microsoft Security Essentials, de a név választása szándékosan hajaz az MS alkalmazás nevére. **A legviccesebb az egészben, hogy az ingyenes MSE helyett ezúttal egy fizetős SE2010-et ajánlanak fel**, és aki ezért aztán fizetni is hajlandó, az duplán

rosszul jár.



[A semmiért fizet és fertőzött is marad](#), esetleg a kártyaadatai is komprimittálódhatnak, és pluszban a "neves" szoftver helyett, amire azt gondolta, aham ezt ismerem, egy semmitértőt kap. Tisztára, mint a kínai piacon az Adidas cipő helyét az Adadis.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

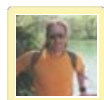
- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1760435>

Kommentek:

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



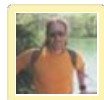
**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
2010.02.17. 13:50:41**

Hackers "fix" XP BSoD rootkit:
blogs.zdnet.com/hardware/?p=7349



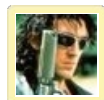
[Yann Le Pentrec](#) • <http://lnk.bz/t7c> 2010.03.04. 08:01:34

Egy parancssorban kiadott shutdown -a időlegesen megoldja az újraindulási problémát, legalábbis ennek segítségével könnyebb keresgélni a megoldást. :)



**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
2010.03.06. 13:27:32**

Ezt a -a paraméteres anti shutdown Barba trükköt nem ismertem, de köszönjük az olvasók millióinak nevében :-)



[Yann Le Pentrec](#) • <http://lnk.bz/t7c> 2010.03.09. 14:54:24

Szívesen, pontosan ezért osztom az észet. :P

Felmérés a személyes adatok védelméről

2010.02.15. 15:05 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [személyes felmérés adatok](#) [osa](#) [védelme](#)

Figyelem, szolgálati közlemény. A BROAD projekt (Broadening the Range Of Awareness in Data protection) **kérésének teszünk eleget, amikor a felhívásukat közreadjuk**. Remélhetőleg az Antivírus Blog szakmai olvasói között is sokan vannak, akiknek a véleménye fontos lehet egy ilyen vizsgálat szempontjából.



idézet ON

"Jelenleg folyik Magyarországon az a nemzetközi felmérés, amely az informatikusoknak a személyes adatok kezeléséről alkotott véleményét kívánja megismerni. A témáról sok szó esik hazánkban is, de az adatkezelő rendszerek kialakításában meghatározó szerepű informatikusokat és főnökeiket eddig nem kérdezték meg erről.

A felmérés egy online kérdőív segítségével történik, amely a kutatás holland vezetői által felügyelt rendszeren fut, magyarul vagy angolul lehet kitölteni.

A felmérés első szakaszában intézményi azonosítókkal (tokenekkel) lehetett részt venni a vizsgálatban a meghívott intézmények (szakmai szervezetek, felsőoktatási intézmények) érintett kollégái számára - többen már ebben a minőségükben találkozhattak is a kérdőívvel. Szeretnénk azonban, ha nem csak a „hivatalos” informatikus társadalom tagjai vehetnének részt, hanem mindazok, akik nem tartoznak a fenti körbe, de tevékenységük, elhivatottságuk alapján informatikusnak tartják magukat, vagy informatikus kollégáik irányítójának. Külön érdekessége lehet a felmérés eredményének, ha a két nagy csoport tagjainak véleménye eltér egymástól.

A kérdőív ezért nyitottá vált bármely magyar informatikus számára, aki korábban nem töltötte ki azt intézményi keretek között. Címe: <http://vortex.uvt.nl/survey>

A vizsgálat neve: IT Professional survey

A kérdőív neve: BROAD"

idézet OFF

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

• [1 trackback](#)

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1760258>

Trackbackek, pingbackek:

Trackback: [Felmérés a személyes adatok védelméről](#) 2010.02.20. 11:12:19

Figyelem, szolgálati közlemény. A BROAD projekt (Broadening the Range Of Awareness in Data protection) **kérésének teszünk eleget, amikor a felhívásukat közreadjuk**. Remélhetőleg az Antivírus Blog szakmai olvasói között is sokan vannak, akiknek a véleménye...



Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Divatos a PDF-es fertőzés

2010.02.18. 12:20 | [Csizmazia István \[Rambol\]](#) | [9 komment](#)

Címkék: [pdf növekedés](#) [exploit](#) [scansafe](#)

Az összes [exploit között 80% a PDF állományok aránya](#) - állítja egy 2009 évvégén készült felmérés. Úgy tűnik, **a kártevő terjesztők kedvenc módszerévé avanzsált** a preparált Portable Document Format.



Számos weblap, e-mail melléklet vagy üzenetben küldött link tartalmaz manapság kártékony PDF-re mutató hivatkozást. A ScanSafe adatai szerint rohamosan romlik a helyzet, **a 2009 év elejei adatok a mostani 80% helyett még "csak" 56 százalékos arányt mutattak**. Ha még korábbról kezdjük vizsgálni, például a [CVE \(Common Vulnerabilities Exposures\)](#) adatai szerint 2006-ban még csak 35 bejelentett sebezhetőség szerepelt, 2008-ban már 58, **míg 2009-ben ezek száma már 107 volt**.



És bár végre megérkezett a várva várt Adobe frissítés, amely orvosolja például [az Adobe Readerbe épített Flash lejátszó hibáját, ami miatt azt tetszőleges kód futtatásra lehetett](#) kihasználni, **sajnos véglegesen biztosan nem lélegezhetünk fel** és mondhatjuk, hogy "it's over John". Hanem sajnos Rambosan azt kell válaszoljuk: "Nothing is over, nothing".



Idegentől továbbra se fogadjunk el tudatmódosító cukorkát, sem pedig [ismeretlen PDF állományra mutató kéréstlen linket](#) emailben vagy közösségi oldal üzeneteként.



Mindazonáltal a South Park rajzfilm bevezetőjéhez hasonlóan [az Adobe Reader szoftvert semmilyen korosztálynak nem ajánljuk](#) ;-)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- ["Szösölmédia" és nyaralás](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1768151>

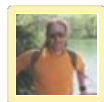
Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.02.18. 15:01:17](#)

Már maga a név is kezd egy nagy viccé válni: hordozható dokumentum formátum. Anno azt szerettem benne, hogy ha elküldtem/vittem, akkor az mindig mindenhol ugyanaz volt. Ez ma már annyira igaz, mint a word.doc



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu 2010.02.18. 15:51:07](#)

Szia Atko!

Mint régi motoros, aki DOS-on, Ékszeren és World Perfecten is tolta még a Windows előtt, és annak hajnalán, én értékelem a PDF-et, mint ami nagyjából egyformán megjeleníthető egy Windows, Linux és Macintosh környezetben. Még engem is kihúzott a bajból, amikor előadás előtt kiedrült, másik, nem sjaát Wines gépen kell lejátszani a Linuxon és Open Office-on készült PPT bemutatót, ahol a betűk szétestek, a hosszú ő és ú betűk vagy nem látszóttak vagy négyzet volt a helyükön. Nos ilyenkor az okos kismalacka már 4-kor kiment a répa földre és PDF-be is renderelte a fóliát ;-) és mosolyogva előad abból.

A nagyobb gond szerintem inkább a vaddisznó méretű fatwarre hízott ilyen alkalmazásokkal van (Accrobat Reader 2 még 1.4 MB, viszont az Adobe Reader 9.2 már 24.9 MB) amikben ráadásul lassított felvételszerűen javítják a réseket. A mai világban aki Internet Explorerrel böngészik, Outlook Expresszer levezik, és Adobe Readerrel olvas doksit, az a lehető legsebezhetőbb eszközökkel veszik körbe magát.



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu 2010.02.19. 16:17:59](#)

Kis adalék még:

threatpost.com/en_us/blogs/security-skeletons-adobes-closet-021910

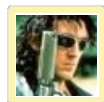


[atko 2010.02.20. 18:18:59](#)

Lassított felvétel :-) és a WP is ismerős.

Igazad van, valóban nem a formátum hibája az ami körülötte történik.

Hogy miért ilyen az Adobe hozzáállása nem tudom, de remélem ébrednek és gyorsítanak.



[Yann Le Pentrec • http://lnk.bz/t7c 2010.03.04. 07:14:11](#)

No ezért kell nem Adobe által gyártott PDF-megjelenítőt használni. Ez itt a reklám helye, bár ingyenes termékről van szó (ám van belőle fizetős is, meg mindenféle csoda editor): Foxit PDF Reader a válasz. Kicsi, praktikus, biztonságos.

zslaci 2010.03.06. 09:56:23

Mi a francnak egy reader-be flash lejátszó?

Nem vagyok paranoiás, de mintha eleve egyetlen biztonsági rést írnának manapság program néven. Lassan már nincs olyan elterjedt alkalmazás ami ne lenne valamilyen veszélynek kitéve...



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.03.06. 12:42:56

@Yann Le Pentrec:

Ahogy a Biblia fogalmaz, az vesse rá az első követ közületek, aki bűn nélkül való. Sajnos van azért exploit a Foxitre is, és bár nem kerestem, de a Sumatrara gondolom ez ugyanúgy igaz. A programozás órán mi azt tanultuk, hogy "hibátlan program nem létezik, csak olyan, amelyik eddig hiba nélkül futott le". Ennek szellemében tehát mindenre létezik, de ha a brutális programméreteket nem is nézzük az Adobenál, a sebezhetőségek óriási száma, és a "Technocolba mártott csiga" tempójú frissítések miatt én is a Foxitet meg a Sumatrát szoktam kiváltó programnak javasolni Windows alatt.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.03.06. 13:20:44

@zslaci:

Jó kérdés, nyilván mezők, gombok testreszabása volt az eredeti cél, csak hát nyitott ajtón aztán bejött minden. Szerintem is meg volnánk ilyen híján, mármint világlátott emberek határozottan állítják, kikapcsolt JavaScript-tel is lehet teljes értékű emberi életet élni ;-)



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.03.09. 15:00:18

Sumatra ma jött szembe épp egy programcsomag részeként, de nem vizsgáltam be - ezek szerint érdemes foglalkozni vele szintén. (Így viszont maga a PDF formátum hordozza magában az exploitok lehetőségét, ha minden reader "lyukas"?)

A Twitterre költöztek és élvezik

2010.02.22. 19:50 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [link twitter viagra kártevő kéretlen adathalászat klubtagság](#)

A vajonkik újabban egyre sűrűbben teszik tiszteletüket, és terítik kéretlen levélszemetüket, kártevővel terhelt linkjeiket a közösségi portálokon, többek közt a nagy forgalmú Twitteren is.



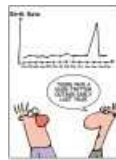
Mint azt az [Adathalászni könnyebb, mint csajozni](#) című cikkből is láthattuk, [egy közösségi oldalon éppen az a jó](#), hogy az ott lévők kevésbé gyanakvóan jobban megbíznak a küldeményekben, a linkekben. A Hancu féle történet pedig **mindennél jobban bizonyítja, hogy a social engineering történetek szépen működnek**, [száz barát négy nap alatt, és hasonló akciók](#) mindig meghozzák a szükséges mennyiségű ismeretlenül is ismerős balekot. Persze ez a látatlanban visszaigazolom, ha [Pamela Anderson feje van, mosolyog, a kamerába néz és nem iszik közben alkoholt](#) című dolog csak egy mellék szál, a fő probléma inkább a tereppel van: egyre sűrűbben küldözgetnek itt mindenféle Canis mergat. A hétvégén például egész nagyüzem volt "Lol. this is me??", "lol , this is funny." és "Lol. this you??" üzenetekből.



Amik valljuk be, amúgy is sűrűn előfordulnak itten kérem tisztelettel, de [ezúttal a bzpharma.net kínált twitter szerű hamis belépési oldalt, amely valójában adathalász link volt](#). Az account begépelése után **még ál-bálna is jött, hogy "Twitter is over capacity"**. Vagyis ebben a kontextusban ez valamiféle Moby Dickes összeesküvés volt ;-), mindenesetre úgy tűnik, a megszerzett és kompromittált azonosítokról ezekután elkezdtek áradni a [Viagrás kéretlen üzenetek](#) is.



Persze **attól sem kell mindig hanyatt esni**, [ha újabb követőnk akad. Aki ha már a korábbi cikkekben is említve egy csinos hölgyemény fotójával van felvértezve](#), még mindig vezethet a weblap linkje egy orosz társskereső oldalra, és meggyőződhetünk, nem az üzeneteink iránti kíváncsiág vezette, hanem az, hogy mi majd hátha kattintunk neki.



Nem könnyű tehát az **egyre gyarapodó ocsút az értékes búzától elválasztani** a Twitter mátrixában sem, és ráadásul a különféle közösségi oldalakon [a rengeteg ismeretlen összetételű klub tagság](#) ezt még megtévezve teljesen átláthatatlanná teheti. Ha ezt a klubban egyszer elmeséljük...

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Informatikai biztonság az egészségügyben](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szösölmédia" és nyaralás](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1781437>

Kommentek:

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



Kontárblog • <http://kontar.blog.hu/> **2010.02.23. 22:42:18**

tetszik, jól összeszedted!

Chuck Norris megváltoztatja az életed!

2010.02.25. 12:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [linux](#) [chuck](#) [hálózat](#) [norris](#) [jelszó](#) [router](#) [modem](#) [féreg](#) [dsl](#)

Nem kell megijedni, nem ránt azonnal a Total Gym edzőpadjára mindenkit. De az eset édes-bús emlékeket ébreszt, és a [jelszó kezelési módszereinket sem árt immár sokadjára felülvizsgálni](#) miatta.



Idősebbek és a katonaviseltek biztosan emlékeznek arra az SQL Slammer nevű kártevőre, amelyik a korábbi szokásos, mackós tempójú fertőzésekkel szemben **egyszerre csak villámgyors terjedéssel jelentkezett**. Az okok között persze már akkor is ott szerepelt az elhanyagolt, biztonsági frissítésekkel el nem látott vállalati környezet, de **volt még egy fontos momentum, ami érdekessé tette ezt a világméretű fertőzést**. A kártevő nem fertőzte meg a gépet, legalábbis nem a szó hagyományos értelmében, nem fűzte magát hozzá állományokhoz, nem volt megtalálható a merevlemezen, **hanem csak és kizárólag a memóriában futva volt jelen**. A szervert **ki-bekapcsolva (hehe) könnyen el lehetett távolítani**, de persze alapos tervszerű mentés, frissítés nélkül a fertőzött hálózati megosztásokon minduntalan visszatért. Ez az emlék idéződött fel, miután most 2010 elején kutatók észlelték a csak routereken és DSL hálózati eszközökön (modem) terjedő fertőzést.



Mit lehet tenni, hogy megelőzzük a bajt? A dolog **gyökere a szofisztikált jelszó választásban rejlik**. Ez legyen erős, egyedi, és [semmiképpen se a gyári alapértelmezett](#). Aki esetleg eddig nem tett még látogatást [az alapértelmezett jelszavakat tálcán kínáló](#) weboldalon, most elgondolkodhat kicsit a dolgokon. A megelőzés tehát a használatba vételkor azonnal [alkalmazott jelszó](#) csere saját erős jelszóra, a beállítások közt pedig tiltsuk le a távoli elérés lehetőségét. **Ha jelent meg új firmware (nem biztos), akkor frissítsük is az eszközt**.



Ha viszont a jelszó az alapértelmezetten állt, vagy szótár alapon könnyen kitalálható volt, akkor az eszköz beállításait, különös tekintettel a DNS szerverekre, a féreg átkonfigurálja. Miért jó ez neki? Ez a kulcs ahhoz, hogy **a levelezést elhappolja, banki, közösségi és egyéb jelszó adatokat szerezhesen meg, a netes forgalmat eltérítse, de emellett folyamatosan keres mindig további fertőzhető eszközt is a hálózatban**. Vagyis megéri a bűnözőknek. Szakértők mindazonáltal jelenleg csak kis méretű fertőzésről beszélnek, tehát szó sincs róla, hogy a fél világ már elesett volna, de a veszély ennek ellenére valós, odafigyelni érdemes. Például az is érdekes részlet, hogy [a kód a D-Link routerek egy ismert biztonsági hibáját is megkísérli kihasználni](#).



Mégis, **mit lehet tenni, ha már Chuck Norris odabent van**, és csörgeti a nunchaku láncait? Először is kapcsoljuk ki, és indítsuk újra routert, modemet. Ugye mivel csak a memóriában létezik a féreg, ettől eltűnik, de rögtön ezután érdemes megnézni, hogy van-e új firmware, és ha van, haladéktalanul frissíteni. Ezek után - mivel a beállításaink mérgezetten lehetnek - egy **teljes reset, és a konfiguráció beállítások alaphelyzetbe hozása szükséges**, valamint [a már emlegetett jelszó csere](#). A netes beállításainkat ismét el kell végezni és érdemes minden, **a hálózatban működő számítógépen ezek után egy alapos vírusvizsgálatot is elvégezni**, hátha előzékenyen besegített ezt-azt a fertőzés. **Továbbra se hagyjuk magunkat átverni, becsapni, és routerünket Chuck Norris által orvul lekaratélyozni!**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:



- [Gyerek-barát netezés](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Akiknek a Captcha kinszenvedés](#)
- [A jelszó érték, vigyázzunk rá](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1788918>

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.

Kulcs a lábtörlő alatt

2010.03.03. 21:20 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [twitter](#) [közvetítés](#) [pleaserobme.com](#)

[Már a Sarah Palin esetnél látszott](#), nem célszerű ész nélkül minden személyes adatot túlzottan ki tacepaozni a közösségi oldalakra.



Manapság, amikor az izraeli hadsereg azért fúj le egy tervezett akciót, mert [egy katonája kibeszéli a twitteren a rajtaütés részleteit](#), nem lehet az sem meglepetés, hogy az óvatlan kitárulkozás **nem célszerű viselkedési forma** az interneten (sem). A [Pleaserobme.com honlap egészen érdekes dolgot mutat meg](#): nagyon sokan interurbán [realtime közvetítésként osztják meg](#) életünk minden apró rezdülését a nagyérdeművel.



A [mellékelt keresési javaslattal élve magunk is meggyőződhetünk arról](#), hogy éppen ebben a pillanatban is milyen sokan közlik a pillanatnyi helyzetüket. [Nem kell GPS vagy okostelefon póráz a munkaadónak](#), de a betörők is minden bizonnyal örülnek az ilyen nüanszokra kihegyezett részletes online közvetítésnek, mert frankón [látszik, hogy lesz még idő kivinni a plazma Tv-t is a teherautóba](#). Pláne, ha még a "nyaralni mentünk Mallorcára, hurrá" kezdetű blogpostot is olvasták.



Ehhez képest öröm és bódottá, hogy **Franciaországban már emberrablást - saját magunk ál elrablását - is megrendelhetjük potom 900 euró áron**. Amiről a Rejtői életmű ismerőinek a [Bradley Tamás visszaüt című örökbecsű klasszikusa kell, hogy eszébe jusson, ahol kiderül](#) hogy még az ilyen bombabiztosnak gondolt forgatókönyv is elsülhet balul.



Ha épp nem akarjuk elraboltatni vagy kiraboltatni magunkat, **óvatosabban kéne a bárki által olvasható információkat magunkról csepegtetni**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/1806772

Kommentek:

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

[totasnick \(törölt\) 2010.03.25. 20:41:12](#)

Szerinted hány ember kapcsolja össze a lakcímét a twitterével?

Hátsóajtó az Energizer elemtöltő szoftverében

2010.03.08. 18:30 | [Csizmazia István \[Rambol\]](#) | [7 komment](#)

Címkék: [fertőzés](#) [trójai](#) [backdoor](#) [cert](#) [symantec](#) [hátsóajtó](#) [energizer](#) [arucer.dll](#)

Megfelelő hozzáállás, ha már semmin nem lepődünk meg. Valljuk be, néha azért kiesünk a szerepünkől, de vigasztaljuk magunkat azzal, hogy a kivétel erősíti a szabályt. [Ezúttal az Energizer szolgáltatotta mindehhez a muníciót.](#)



A CERT is megerősítette a felfedezést, hogy az **Energizer Duo szoftverében trójai programot találtak**. Az arucer.dll nevű állomány az elemek állapotának ellenőrzése helyett (vagy mellett) **hátsó ajtót nyitott, azaz távoli hozzáférést biztosított a kompromittált géphez.**



A CERT vizsgálódása - és ebben a Symantec víruslaborja is segédkezett - bebizonyította, hogy **egy kártevő a 7777 porton hallgatózott, és onnan távoli utasításokat** volt képes végrehajtani.



A bejelentés után az elemgyártó cég **törölte a weboldaláról a fertőzött alkalmazást**. Az esettel kapcsolatos [teljeskörű leírást a CERT oldalán olvashatják el](#) az érdeklődők.



És ami a legszomorúbb, **ez a felállás minden valószínűség szerint már 2007 óta így volt**, vagyis aki csak azóta letöltötte, használta, mind áldozat lehetett. Úgy tűnik, időnként mindenféle hullanak ki csontvázak különböző szekrényekből, és meg van ennek a diszkrét bája itt a számítástechnika berkeiben is.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Ez történik a weben egy perc alatt](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/1818402>

Kommentek:

العربية (törölt) 2010.03.09. 18:03:13

hehe :D ez király :D



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.03.09. 21:24:38

Eleve mekkora agyament hülyeség, hogy egy elemtöltőnek bármiféle köze és kapcsolata legyen egy személyi számítógéppel. Szerintem eddig is megvolt az emberiség efféle sületlenségek nélkül. :)



ergerberger 2010.03.12. 00:31:13

@Yann Le Pentrec: "eddig is megvolt az emberiség efféle sületlenségek nélkül."

Mint például a laptop?



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.03.14. 17:46:06

Mondom elemtöltő, nem laptop, az megint egy másik történet. Ne tessék kiforgatni a mondanivalót.



ergerberger 2010.03.17. 01:25:02

@Yann Le Pentrec: laptop = PC + akku + akkutöltő.

Merthogy szerintem agyament hülyeség, ha egy akkutöltőnek bármi kapcsolata van egy PC-vel.

Érted.



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.03.20. 21:40:34

Én eddig is értettem, hogy te mire gondoltál, de én az USB-s akkutöltőre + szoftverre, amiről a cikk szól, ezt találok sületlenségnek.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.03.22. 11:18:34

Tegye fel a kezét, aki látott olyan embert, ha már látott olyan embert, aki feltelepített a gépére egy ilyen elemtöltő vezérlő programot. Ez már szinte a perverzió egy különös formája, bár a Hairból kimaradt. Mindenesetre a gyártó ennek ellenére sáros, és tanulnia kell a figyelmetlenségéből. Elég lett volna egy cikk a Blikkben, hogy brit tudósok szerrint ha valaki a PC-s programmal tölti az elemeket, azok 110%-al több áramot adnak le, és kétszer annyi ideig tartanak, és milliónyi letöltés lett volna azonnal. Ezt a meg nem valósult véletlent is bele kell látni az esetbe, amely szerencsére nem történt meg :-)

Az Adobe a legvonzóbb célpont

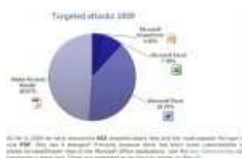
2010.03.11. 18:40 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [reader](#) [adobe](#) [pdf](#) [támadás](#) [exploit](#) [f](#) [secure](#)

Az F-Secure vizsgálatai szerint is az Adobe programjait támadják leginkább különböző exploitokkal - erről szólnak a biztonsági cég 2009-es információi.



A kétes értékű staféta botot a Microsoft szövegszerkesztői állományoktól ragadta el az Adobe, amely nem csak a Flash állományok lejátszóját, de a **Portable Document Format** fájlok megjelenítésére alkalmas **Adobe Readert** is készíti. [Ha az F-Secure 2009 adatait nézzük](#), a sebezhetőségek **már 49%-ban a PDF olvasót érintették**, míg a Microsoft Word érintettsége "mindössze" 39% volt ugyanebben az időben. Az átrendeződés következtében az Excel, Powerpoint, stb. egyéb Office állományok kihasználása is csökkent. [Az Adobe Reader egyébként már jó ideje a célkeresztben áll](#), ehhez talán a **könnyű támadhatóság és a fejlesztők sztochasztikus frissítési gyakorlata** is nagyban hozzájárulhatott. Korábban **mi is ismertettünk hasonló kimutatásokat**, és ha a számokban volt is valamennyi különbség, tulajdonképpen a [Scansafe adatai szerint is eljött az áttörés](#).



Ezekhez [az eredményekhez még két további dolog járulhatott hozzá](#). Egyfelől valóban **egyszerű találni PDF exploitot**, számuk is egyre jobban növekszik és azt alkalmazva állományokat e-mailben küldeni, vagy weboldalra kihelyezni. Másrészt **a felhasználók frissítési szokásai sem mindig megfelelőek**. Ha van is, aki legalább az antivírus és a Windows biztonsági frissítését több-kevesebb rendszerességgel elvégzi, az otthoni felhasználók között rengetegen meg is állnak itt. [Az összes felhasználói alkalmazás napra készen tartása sziszifuszi munka](#), emiatt aztán sokaknál ez már **nem valósul meg, vagy csak jelentős késéssel**.



Akit érdekel, a márciusi és áprilisi PC Worldben részletesebben is fogjuk boncolgatni, körüljárni ezt a frissítési problematikát: miért nehéz, milyen buktatók vannak, mennyiben segítenek a programfejlesztők, és rejthet-e ritkán veszélyeket is akár egy frissítés.

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](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1831474>

Kommentek:

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



[Skunkworks 2010.03.12. 00:40:00](#)

Tényleg egy hülye gondolat, de akkor az Adobe miért nem csinál semmit? Legalább valamit gerjesztene, hogy ne nyomják fel a cuccaikat. Mondjuk nem értek hozzá, ez igaz.

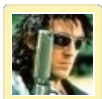
[zeneigénius 2010.03.12. 08:48:14](#)

Az adobe egy vicc.

Feltalálták a postscriptet - Indesign-ban sokáig nem lehetett normális PDF-et írni, csak ha Distillálod. Most belerakták a 3d-t tök feleslegesen, stb, stb, stb.

Minek kell indi, illus, photoshop? Miért nem elég erre 1 proggi???

Lol. Remélem az adobe eltűnik mihamarabb



[Yann Le Pentrec • http://lnk.bz/t7c 2010.03.14. 17:49:28](#)

Sajnos nem úgy néz ki, mint ami eltűnni készül, sőt, ők vásárolják fel a kisebb cégeket a nekik kellő technológiák végett. (pl. Macromedia)

Autoruntól sújtva

2010.03.12. 09:40 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

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

Bár a Conficker féreg szinte bebetonozva áll első helyen már hónapok óta, a trójai programok mellett **a külső eszközök automatikus futtatása szaporítja** tovább a felhasználók gondjait.



Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melynek elemzése mindig tanulsággal szolgálhat a felhasználók számára. **A magyar lista első helyén tavaly október óta a Win32/Conficker áll**, amely eddig leggyakrabban az operációs rendszer frissítésének hiányát és a gyenge admin jelszavakat kihasználva terjedt.

A Conficker azonban egyre többször kerül a számítógépre úgy, hogy egy másik, **a Windows automatikus futtatási lehetőségét kihasználva terjedő kártevő tölti le az internetről**. Miután az autorun típusú vírus megfertőzte a külső eszköz automatikus indítófájlját, az USB kulcs számítógépbe való illesztésekor már a Conficker is letöltődik az internetről, és megfertőzi a számítógépet.

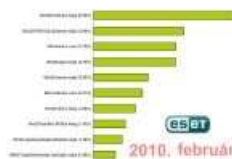


A Conficker azonban nem egyedi példa, úgy tűnik, hogy a bűnözők előszeretettel használják ki, hogy **a legtöbb felhasználó nem tiltja le az automatikus futtatást** a Windows operációs rendszerek alatt. A februári toplistán így több olyan kártevő található, mely ezt a funkciót használja ki. Az ESET szakértői szerint éppen ezért fontos, hogy a felhasználók megtanulják letiltani, hogy a Windows automatikusan lejátssza a külső eszközök – például USB kulcsok – tartalmát, amikor azokat csatlakoztatják a számítógéphez.

A lista **második helyét az online játékok jelszavainak megszerzésére és továbbítására specializálódott**

Win32/PSW.OnLineGames.NNU trójai tartja. Ez a kártevő billentyűleütés-naplózával (keylogger) rendelkezik, és gyakran rootkit komponense is van, ami jelentősen megnehezíti a kártevő detektálását.

A jól ismert szereplők mellett pedig ezúttal is találunk **egy újoncot a tízes listán, ez pedig a Win32/AutoRun.IRCBot trójai**, amely a megtámadott gépen a Windows könyvtárban egy állományt hoz létre, majd a Registryben gondoskodik annak automatikus lefuttatásáról. Működése során **hátsó ajtót nyit a megtámadott számítógépen**, ezzel pedig veszélyezteti a felhasználó adatait, jelszavait.



Végezetül következzen a részletes toplista. Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikája szerint **2010 februárjában az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban**. Ezek együttesen 28,26%-ot tudtak a teljes tortából kihasítani maguknak.



1. Win32/Conficker féreg

Elterjedtsége a februári fertőzések között: 6.50%

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 eljárason keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.

Bővebb információ: <http://www.eset.hu/virus/conficker-aa>



2. Win32/PSW.OnLineGames trójai

Elterjedtsége a februári fertőzések között: 4.08%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók 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/virus/psw-onlinegames-nnu>



3. INF/Autorun vírus

Elterjedtsége a februári fertőzések között: 3.72%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájl 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/virus/autorun>



4. Win32/Agent trójai

Elterjedtsége a februári fertőzések között: 3.70%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (például Temp mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat, illetve .exe kiterjesztéssel hozza létre.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/agent>



5. Win32/Injector trójai

Elterjedtsége a februári fertőzések között: 2.46%

Működés: A Win32/Injector trójai olyan Registry bejegyzéseket, illetve külön állományokat hoz létre a számítógép megfertőzésekor, amelyek egy esetleges újraindítást (bootolást) követően aktivizálják a kártevő kódját és gondoskodnak annak automatikus lefuttatásáról. A Windows System32 mappájában (alapértelmezés szerint C:\Windows\System32) található wsnpem, illetve ntos.exe áruklódó jel lehet. A megtámadott gépen hátsó ajtót nyit, és a newvalarsrent.ru weboldalhoz csatlakozik, ahonnan további fájlokat próbál meg letölteni. Rootkit komponenssel is rendelkezik, működése során fájlokat rejt el a fájlkezelő alkalmazások elől (pl. EXPLORER, FAR MANAGER), még akkor is, ha ezek nincsenek ellátva rejtett attribútummal.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/injector-k>



6. INF/Conficker vírus

Elterjedtsége a februári fertőzések között: 2.21%

Működés: Böngészés során, amennyiben az autorun.inf fájl valamely egység főkönyvtárába kerül, a betöltő eléri, hogy a kártevő kódja induljon el. Vagyis az INF/Confickernek az a szerepe, hogy betöltse magát a Win32/Conficker kártevőt.



A számítógépre kerülés módja: fertőzött weblapról, vagy külső eszközön keresztül.

Bővebb információ: <http://www.eset.hu/virus/conficker>



7. Win32/VB.EL féreg

Elterjedtsége a februári fertőzések között: 1.89%

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/virus/vb-el>



8. Win32/Autorun.IRCBot féreg

Elterjedtsége a februári fertőzések között: 1.43%

Működés: Az interneten vagy lokális hálózaton terjedő kártevők elsődleges célja, hogy egy másik számítógépet fertőzzenek meg. Nincs ez másként a Win32/Autorun.IRCBot trójai esetében sem, amely a megtámadott gépen a Windows könyvtárban egy állományt hoz létre, majd a Registryben gondoskodik annak automatikus lefuttatásáról. Működése során hátsó ajtót is nyit a megtámadott számítógépen. Ezzel a támadók teljes mértékben átvehetik a számítógép felügyeletét, így akár alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.



A számítógépre kerülés módja: fertőzött weblapról vagy külső eszközhöz keresztül.

Bővebb információ: <http://www.eset.hu/virus/autorun-ircbot-aj>



9. Win32/TrojanDownloader.Bredolab.AA trójai

Elterjedtsége a februári fertőzések között: 1.29%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, mely távoli oldalakról további kártékony kódokat tölt le és hajt végre. Futása közben a Windows, illetve a Windows/System32 mappákba igyekezik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságítámozgatás-szolgáltató (SSPI - Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.



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

Bővebb információ: <http://www.eset.hu/virus/trojandownloader-bredolab-aa>



10. WMA/TrojanDownloader.GetCodec.gen trójai

Elterjedtsége a februári fertőzések között: 0,98%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kérértlen reklámlablakokat jelenít meg a számítógépen.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/trojandownloader-getcodec-gen>



 Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Akiknek a Captcha kinszenvedés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- ["Szösölmédia" és nyaralás](#)
- [25-ször több a mobilos kártevő](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/1832450

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

668 százalékos növekedés

2010.03.16. 18:30 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [statisztika](#) [online](#) [fbi](#) [kaszinó](#) [növekedés](#) [számítógépes](#) [bűnözés](#)

Igen, fűtyenthetünk elismerően, ez nem semmi. Sajnos az tippelt jól, aki szerint ez biztosan nem a tavalyi magyar GDP-ről szól, és valóban: az FBI partnerszervezete, az **Internet Crime Complaint Center (IC3)** statisztikáit ismerhettünk meg a számítógépes bűnözésről.



Kissé a **Moore törvényekre** emlékeztet, de itt nem processzorok teljesítményéről, hanem a [számítógépes bűnözők teljesítményéről van szó](#): de mitagadás évről évre tudnak **duplázni ők is**, sőt már évek óta [több a bevétel ebből, mint a kábítószerkereskedelemből](#). A főcímbe **emlegetett** egészen pontosan [667.8 százalékos növekedés a 2001 és a 2009 évek internetes bűncselekmények számainak összevetéséből](#) adódott.



A tételeken végigszaladva **nincs is olyan, amiről itt a blogban már ne írtunk volna** rengetegszer: az [álfertőzésekkel riogató hamis antivírus](#) iparág, a pénzért [zsaroló hamis bérnyíl](#), a gazdasági trükkökön át [a tőzsdei árfolyamok manipulálásán](#) át egészen a [hamis álláshirdetésekre, ahol kevés munkával nagy fizetést ígérve](#) a számítógépes csalók pénzét kell továbbutalni különböző számlákra, azonban **a börtönbe végül mégis mi, a naív strómanok megyünk**.



Most egy újabb vonal is megerősödni látszik, ez a [számítógépes fogadások, kaszinók és az illegális szerencsejátékok](#) területe. Az ilyen [szürke zónába tartozó területén is megjelentek már](#) **csalók által üzemeltetett oldalak, ahol tömegesen fordulnak elő például személyiség lopások**. Számtalanszor fordul elő, hogy a kéretlenül terített és különféle online kaszinókat reklámozó spam levelek mellékletei, illetve az abban szereplő linkeken található **letölthető program nem online játékokra alkalmas, hanem valamilyen trójai, amely megfertőzi a számítógépet**, és hátsó ajtót nyitva rajta távolról vezérelhető zombigéppé változtatja azt.



Ez pedig sajnos **nem a felhasználónak szerencse, hanem csakis a botnetek irányítóinak**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártya bűnözők kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kényszerűsége](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [25-ször több a mobilos kártevő](#)



A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1844158>

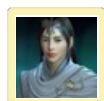
Kommentek:

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



[Mike36 2010.03.17. 03:55:06](#)

látom az FBI még több pénzt akar



[Csore60 2010.03.17. 06:38:51](#)

Most majd megint jön valaki, aki hülye kockafejűnek fog nevezni, de muszáj megjegyeznem, a fentiek miatt használok Linuxot.

Tudom, hogy ettől a többség nem fog lemondani a jó kis kényelmes, bár időnként összeomló Windowsról. A Linux használata tényleg kicsit bonyolultabb, de könyörgöm, a Win. biztonsági szempontból egy nagy kalap xar. Nem véletlenül épült rá biztonsági iparág. / Hogy mennyi volt ebből az alkotók eredeti szándéka, azt nem tudhatom.:) /

[különvélemény 2010.03.17. 09:21:33](#)

A kábítószer kereskedelmi hasonlatot a befektetett pénz vs nyereség miatt szokás emlegetni, aminek semmi köze sincs az árbevételhez, vagy az éves növekedéshez.

A pelenkaeladásból is tutira nagyobb a bevétel, mint a kábcszerekből.

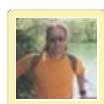
A százalékos éves növekedés pedig mindig attól függ, honnan indultunk.

Persze jól hangzanak a magas százalékok.



[xaba99 • <http://landf.blog.hu> 2010.03.17. 09:47:35](#)

@Csore60: az egység sugarú felhasználó a linuxból is 5 perc alatt zombigépet, mer vírustenyésztőt csinál. aki meg ért hozzá, az windows-on sem kap be vírust.



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu> 2010.03.22. 11:26:32](#)

Szia Különvélemény!

A bűnözés módja keveredik is az internetes fomákkal, hiszen sokan kábcszert árulnak az interneten, és amit aztán csomagfutárral szállítatnak.

Részbe igazat adok neked: lehet a pelanka, sajtoskifli, Pitralon arcvíz, dohány-tabak és gyarmatárú függvényében nézni vagy nem nézni és a statisztika ugye mindig olyan, amilyenné a készítő tenni akarja.

Részben azért vitázok is: mert amire utal a dolog, az igaz: egyre jobban érdekesebb ezzel foglalkozni, mert a pénz kijön a cső végén, viszont a lebukás - a kábcszer biznchez képest is - szinte elenyésző, és ez a tendencia csak erősödik.

A CKM olvasó kérdez 1.

2010.03.18. 15:05 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [vírus kémkedés](#) [kémprogram](#) [ckm családtag](#) [terjedés](#)

Vendégszereplésen jártunk a CKM Magazinban, egészen pontosan egy vírusvédelemmel, internet biztonsággal foglalkozó cikksorozatunk kezdődött el ott. Mivel nem mindenki olvas CKM-et (bevallom én magam sem), viszont az ott felvetett olvasói kérdések-válaszok esetleg másoknak is érdekesek, tanulságosak lehetnek, így arra gondoltunk, ezeket itt a blogban is rendszeresen közzétennénk. Az első rész következik.



[Tetszik](#) [Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.](#)

[Megosztás](#) [+1](#) [0](#) [Tweet](#)

Ajánlott bejegyzések:

- [Akiknek a Captcha kinszenvedés](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Nyári tanácsok utazáshoz](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés [trackback](#) címe:

<http://antivirus.blog.hu/api/trackback/id/1849458>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 Twitter blokkolja a rosszindulatú linkeket

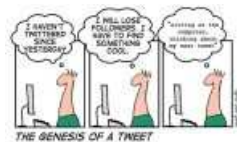
2010.03.19. 11:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [link hivatkozás](#) [twitter szűrés](#) [kártékony adathalászat](#)

Az e-mailben küldött kéretlen linkeknél mindig is veszélyesebbnek számítottak azok közösségi üzenetek vagy vagy bejegyzések, amelyben szintén hivatkozások szerepelnek, de **mindenki úgy gondolja, ezek valamiért megbízhatóbbak**. A [rossz hír hogy ab ovo ez nem igaz](#), a jó hír, hogy [a Twitter megpróbál tenni valamit ellene](#).



Úgy gondolták, hogy mivel [a felhasználók már eleve óvatlanabbak a közösségi oldalakon](#), legalább a linkek tekintetében **megpróbálják megelőzni a kártékony kódok terjesztését**. Mostantól szűrik a hivatkozásokat, ami igen hasznos lehet, [hiszen csak adathalász támadásból rengeteg indul innen](#), a további kártevőkről, trójaikról, kémprogramokról nem is beszélve. Előfordul az is, hogy [hamis antivírus programra mutató linkeket küldenek Twitteren keresztül](#), és akinek nincs valódi védelmi programja vagy tapasztalatlan felhasználó, ebbe az utcába is be tud sétálni.



Remélhetőleg [a linkek helyzete mostantól jobbra](#) fordul, a [felhasználók alapvető naívsága azonban továbbra is "kezelésre" szorul](#).

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/1851822

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Fél kiló domaint kérek

2010.03.22. 14:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [domain](#) [.ru szigorítás](#) [reisztráció](#)

Nincsenek véletlenek. A kártékony kódokat, spameket terjesztő weboldalak **mindig olyan országokban érik el a Gauss görbe csúcsát, ahol elégtelen a törvényi szabályozás** az ilyen bűncselekmények üldözésére és/vagy a domain regisztráció túlzottan liberális.



Most úgy tűnik, [a .ru legfelsőbb szintű végződés esetében javulás állhat be, az eddigi "benyögök bármit és enyém a domain" korszaknak vége](#). Látványos változást hozhat, mivel **mostantól a magánszemélynek személyi okmányt (például útlevelet), cégeknek pedig működési, bejegyzési iratokat kell bemutatni** az ügyintézéshez. Másképpen fogalmazva az ember szinte nem is érti, miért is nem így történt ez a kezdetektől fogva, miért lehetett eddig könnyedén ismeretlen személyeknek mindezt megtenniük. Na mindegy, a szokásos és elvárt gyakorlathoz történő közeledéstől **a szakemberek mindenesetre a spamek, a botnet irányító szerverek számának csökkenését várják**.



[Ha varázsütésre nem is tűnik el minden kártékony oldal, talán lesz javulás. Kínában éppen a múlt hónapban vezettek be hasonló lépéseket](#), igaz ott a fő mozgató rugó inkább az online pornó elleni küzdelem lehetett. Majd meglátjuk az eredményeket pár hónap múlva, [hátha kevesebb viagrás levél lesz-e a postafiókokban](#).



Jó hír tehát, hogy a két nagyot most végre megzabolázták, de azért tudni kell, még bőven marad választásuk a spammereknek, csalóknak, hiszen közben Vietnám, Indonézia és néhány hasonló országban továbbra is a túlzottan engedékeny bejegyzési szabályokat alkalmazzák. De sebjaj, **a leghosszabb utazás is egyetlen lépéssel kezdődik :-)**

 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](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/1858908

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 kell-e írni mindent a homlokunkra?

2010.03.24. 14:20 | [Csizmazia István \[Rambol\]](#) | [4 komment](#)

Címkék: [email információ felesleges publikus antivírus](#)

Ez az egész világnak a tudomására hozom, megosztom hát mindenki vel feeling igazán kimehetne a divatból. Ennek praktikus okait néhány aspektusból már sokszor nézegettük, most pedig újabb nézőpontokkal gazdagítjuk e látványt.



A korábbiakban elemeztük, miért [nem praktikus dolog percre kész twitter üzenetekkel részletesen beszámolni pillanatnyi helyzetünkről](#), ez szinte felhívás keringőre, gyere és törjél be hozzám. Aztán a wifi kapcsolatokról szóló elmélkedéseink közben is felmerült, ha már neten kinderspiel elérni az összes hálózati eszköz gyári jelszavát, akkor az "okos pilóta alagútban nem katapultál" mintájára kevésbé szerencsés [alapértelmezetten hagyni a jelszót](#), vagy **Dlink, Linksys, Dr. Kovacs III.2. neveket adni a WiFi kapcsolatunknak**. A legjobb valamilyen semleges (txk15), vagy az üres, de láttunk már a belvárosban "Vége az ingyen netednek te kecsge" nevet is.



Az antivírusokkal kapcsolatban is van pár elgondolkodni való. Ebből az egyik érdekesség, mennyiben hasznos a különböző AV cégek bevett gyakorlata, amely referencia listákat tesz közzé a weboldalán, ezen ügyfeleink használják a mi megoldásunkat. Mint az közzismert, minden etikus hackelés (penetration teszt, audit de a valódi rosszindulatú célzott támadások többségénél is) úgy kezdődik, hogy **első lépésként feltérképezik az adott cég infrastuktúráját, hálózatát, az interneten elérhető publikus konkrétumokat**. Ahogy [az Aurora eset kapcsán is írták](#): "kiválasztják célpontjukat és alaposan tanulmányozzák azt: utánanéznek milyen és mennyire sebezhető alkalmazói programokat futtatnak a cégnél, mely gyártó(k) vírusvédelmet alkalmaznak, hogy azok megkerülésére kézzel tuningolt, "láthatatlan" támadó-kódot (ún. exploit-ot) és kártevőt készítsenek". Látható, hogy **egyáltalán nem előny ilyenkor, ha mindent biztosan lehet tudni, hiszen ezzel municiót szolgáltatunk** arra nézve, milyen válogatott exploitokat érdemes keresni egy esetleges támadáshoz.



Hasonló a helyzet amikor a levelezésünkben szerepelnek azok a záró sorok, hogy az XY antivírus 123456 adatbázissal ellenőrizte ezt a levelet. **Ha ez minden kimenő levelünkben szerepel, ezzel is felesleges információkat osztunk meg** mindenki vel. Az [ingyenes antivírusoknál valószínűleg mindez nagyobb gondot okozhat](#), ha a nyilvánosságra került sebezhetőség és az azt befoltózó biztonsági javítás reagálási sebességét nézzük. De még a fizetősök esetében is gondolkodhatunk úgy, nem kell a ház homlokzatának vagy a kerítésének hivalkodónak lennie, elég ha mi tudjuk milyen biztonságos és szép a lakásunk belülről. Ahogy [a Sarah Palin esetről is sokan "nem gondolták úgy"](#), hogy az ilyen talkative magatartásból bármilyen hátrányuk származna, sokan szórják ezt az alapértelmezetten bekapcsolt opciót minden címzettjük számára.



Összefoglalva: dolgozzon csak meg a feltörő, ha akar valamit, ne mi nyújtsuk a fejünket tálcán. Amikor amúgy is [túl sok adatot tárolnak rólunk](#), mi magunk ne könnyítsük meg ezt. Másképpen fogalmazva ahogy Moldova György írja: **"a saját akasztásunkra ne vigyünk kötelet, legyen a hóhérnak is valami rezsije"**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)

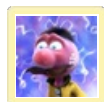
- [Ez történik a weben egy perc alatt](#)
- ["Szövmédia" és nyaralás](#)
- [Nyári tanácsok utazáshoz](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1864691>

Kommentek:

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



Zizidor 2010.03.24. 15:38:23

"XY vírus 123456 adatbázissal ellenőrizte ezt a levelet"

Ez a hülye szokás egyébként sem ér semmit. Mi van ha kézzel írta oda a feladó, miután elhelyezte az üzenetben a trójait? Nem ellenőrizhető, hiteltelen, megbízhatatlan.



atko 2010.03.25. 08:30:58

[@Zizidor](#): + a telepített vírusirtó nem olvassa el csak azért, hogy ne ellenőrizze. :-) Ha meg nincs telepítve akkor tök mindegy mit nyitsz ki.



xaba99 • <http://landf.blog.hu> 2010.03.25. 11:01:39

"XY vírus 123456 adatbázissal ellenőrizte ezt a levelet"

ez nem minősül kéréstlen reklámnak?



atko 2010.03.26. 13:01:56

[@xaba99](#): Igen annak számít akkor ha az utcán járva egy házon olvasva azt, hogy építette xy arra gondolsz: "Basszus ez egy kéréstlen reklám!"

De az tény, hogy a kiírás nem azért született, hogy bízz a levélben, hanem ez egy jó reklám.

A logikája érdekes, mert ha a gépem van vírusirtó, akkor a levelem miért lenne vírusos? Ha nincs rajta, akkor miért írta oda magát? Ergo a kimenő levél vírusellenőrzése olyan fricska ami engem nem véd semmitől, más helyett meg miért én fizessek? dolog.

Facebook jelszó érkezh-e exe-ben?

2010.03.26. 18:40 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [spam](#) [facebook](#) [jelszó](#) [phishing](#) [spoofing](#) [adathalász](#)

Itt a tavasz, [IWIW üzenetek szállnak a széllel](#), de a Facebook felhasználók is megkapják a maguk hivatalosnak látszó municióját.



Ugye amikor spamet válogatunk - már mint utólag szemmel, mert remélhetőleg a rabszolga munka nagyját már mindenki valamilyen automatikus szűrővel végezteti - **első pillantásra ordít, ha a nemkívánt levél feladója** Alonso Hillary, Eduardo Lenin, Jesus Sanchez, Approved Viagra vagy Csing Csang Csung: ez mehet is azonnal a kukába. Ennél egy fokkal szofisztikáltabb, apró gondolkodásra készíthet, ha maga a nagyhatalmú Mailer Daemon, [egy nemzetközi bank](#) vagy [éppen mi magunk szereplünk](#) az elektronikus üzenetek feladójaként. **És megint kicsit más a helyzet, ha valóban felhasználói vagyunk egy szolgáltatásnak, például a Facebook pont egy ilyen hely.**



Itt már jó eséllyel írhatnak olyan megtévesztő leveleket, aminél az átlag nem szisszen fel rögtön (nem fél, mert nem is banktól jön). Sőt még milyen kedvesek is, hogy [a jelszováltoztatásra, új jelszó megerősítésére figyelmeztetnek, szóval rendesek :-\)](#) A levél aláírása pedig: a Facebook csapata.



Ami **nem szokványos viszont, hogy egy új jelszó az e-mail üzenet mellékleteként érkezzon exe vagy zip fájlként az üzemeltetőktől.** Ez kizárt. Ha ez önmagában **minden felhasználónak azonnal szemet szúrna, már jobb lenne a világ.**



A sors fintora, hogy [kevés, ha valaki nagyon erős jelszót használ](#) (fgGj/8893!%!'_ö9Gz5"), de közben ezt pedig lefuttatja. A folytatás pedig [valószínűleg az adózási időszak beköszöntével fog majd megjelenni, gyors hatékony adóvisszatérítés](#), csak most, csak önnek, 24 órán belül visszautaljuk a kétszeresét, ajándékba örökélet plusz két év, ingyen sör, csak kattintson már végre, esdeklünk, köszönetet kérjük...

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kinszenvedés](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1870237>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.03.26. 19:57:18](#)

Nekem van egy tuti fakebook jelszavam. Nem regisztrálok iwiw és face és egyéb book oldalakra. A twitter miatt még az amúgy jól indult webisztánt is elfelejtettem örökre. Aki hülye haljon meg. Ez több millió éve bevált! Miért változtassunk épp most rajta? Éljen az evolúció!

Kétélű fegyver a webkamera

2010.03.29. 18:35 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [webkamera](#) [kukkolás](#) [féreg](#) [kártevő](#)

A fekete és fehér, a jó és a rossz, a jin és jan, valamint a biztonság és a kényelem vívják már egymással évezredek küzdelmüket. Zen buddhista példák helyett mi most **webkamerával kapcsolatos újabb fejleményekről fogunk beszélni**: egyre több mozgólódást lehet tapasztalni a rosszul értelmezett felügyelettel kapcsolatban, valamint **növekvő érdeklődés övezi** a témát a kártevő terjesztők részéről is.



Akik az [antivirusblog](#) [tweetjeit is figyelemmel szőtták kísérni](#), emlékezhetnek arra a februári esetre, amikor [egy philadelphiai \(USA\) iskolában a diákok használatra adott noteszgépeivel kapcsolatosan felmerült a webkamera jogosulatlan használata](#). Ez úgy derült ki véletlenül, hogy a gépeket üzemeltető iskola több esetben figyelmeztette a diákokat, hogy **"otthon helytelenül viselkedtek"**, és ez ne forduljon elő többet.



A dolog pikantériáját az srófolja még feljebb, hogy a nyomozás megerősítette: [a tanárok valóban képesek voltak távirányítással aktiválni a tanulók webkameráját](#), ám erről a lehetőségről [a diákok és a szülők szerint egyáltalán nem tájékoztatták őket](#). Az ilyen behatolásból 14 hónap alatt negyvenkettőt biztosan végrehajtottak a vizsgálatok szerint.



További fejlemény, hogy [Graham Clueley szerint észlelhető érdeklődés egyes kártevők részéről a webkamera](#) használatba vétele iránt. A Sophos vezető munkatársa a Peeping Tom/Rbot-GR féreg kapcsán nyilatkozta, hogy **találtak benne olyan tulajdonságokat, amely titokban a webkamerát és a mikrofont aktiválta**, illetve ezeket az adatokat kísérte meg egy távoli gépnek elküldeni. Ha külső kamera egységről van szó, **húzzuk ki bátran, amikor épp nincs használatban**.



Megnyugodhatunk, **egyelőre csupa egyedi, ritka, és elszigetelt esetről van szó**, de ha már szigetelésről van szó: biztos ami zicher, **szígszalagot a noteszgép nem használt webcamjére**, és akkor tutira nyugi lesz.



De azért látni kell, elindult itt itt egy új irányzat, amire az antivirusoknak és a felhasználóknak is **érdemes lesz majd a jövőben jobban odafigyelni**.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1876833>

Kommentek:

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

Higany 2010.03.29. 21:56:25

Az utolsó kép igen találó :) A hőskor!



Dyrtyho • <http://panelarc.blog.hu> 2010.03.30. 20:55:57

Mindig is tudtam, hogy 1x még veszélyes lehet az emberiség számára a webkamera, ha ez a módszer elkezd fejlődni, akkor az ember már sehol sem lesz biztonságban, és az emberek úgy fognak élni mint a valóságshow szereplők

Foxhound 2010.04.10. 11:00:12

Jin és jang

Hello, Steve Terence vagyok.

2010.03.31. 14:30 | [Csizmazia István \[Rambol\]](#) | [10 komment](#)

Címkék: [spam](#) [hoax](#) [rulett](#) [csalás](#) [hihetetlen](#) [szemétleve](#) [lévél](#) [kéretlen](#) [pénzeső](#)

Szól a kéretlenül kapott e-mail. Én meg nem. Na mindegy. Ha valaki pont Steve Terence, ez lehetne ugyan egyéni szociális probléma is, de sajnos most már nem az, **hiszen egy spam üzenet keretében megosztották mindezt velünk. Vajon most kaptunk egy titkos varázsmódszert a 10.8 százalékosra emelkedett munkanélküliség,** és pénzügyi kilátástalanság leküzdésére?



Akik nem szeretnék tovább olvasni, annak akkor előre eláruljuk, a pincér a gyilkos, és valóban ő tette a nyomravezető lószórt a bárszekrénybe;-) Illetve ja igen, és **valószínűleg nem jó az emlegetett varázsmódszer sem.** Az állítólagos Steve Terence-nek a Google keresőben kevés a nyoma, számunkra már ez sem túl jó előjel. A szerényen csak pénzeső.com oldal idén, **2010 januárjában került domainbejegyzésre,** csak ettől persze még lehetne hiteles, sikeres, és hasonló. Ennek ellenére már **a hamis antivírusok weboldalairól ismert** áradozó álolvasói levelek is övezik: Steve, Maggi, Krisztina köszöni, Emánuel hálás, **Malyomváry Armandó egy nap leforgása alatt megduplázta a családi konyhapénzt,** Kovács Brezsnayke pedig már fel is mondott munkahelyén, a Fogaskerek Fogatlanító Kisszövetkezetben és már ebből éli fényűző életét, e hálálkodó levelet is a Jaguárja bőrkormányán pötyögte be a gyémántokkal kirakott Blackberryjébe ;-)



Le hát a kizsákmányoló unalmas hétköznapi munkával, keresse meg mindenki mostantól a forradalmi online kaszinózással a betevőt, vagy mellékést, de akár napi 400 EUR, azaz kábé 106 000 HUF-ot. Zsebpénzre pont elég is lesz, ha kicsit összehúzzuk magunkat :-)

Ehhez elég mindössze mindig a feketére vagy a pirosra tenni zsetonjainkat, folyamatosan duplázni, amíg az adott szín nem veszít, aztán váltani, és kész is, höhő...



Ki vagy te, ez tényleg jó kérdés. Vajon ha öreg, kopasz, szemüveges és csúnya lenne, akkor is tódulnának az emberek, vagy csak így, ha egy jósvádájú mosolygós NCIS helyszínelő ábrázat néz szembe velünk?

Elég olvasgatni [Nemere István: Szélfhadosok könyvéből](#), vagy csak elővenni a józan eszünket, hogy **feltegyük a nyelvtanilag selejtes, de már szinte közhelyszerű "és akkor ezt így hogy" kérdést.** Ilyen nyerő, bombabiztos szisztéma nem létezik. Még ha logikai feltételezésként lenne is ilyen, **elhiszi-e bárki, hogy ha valaki egymaga százmilliókat nyerhetne, akkor majd a titkok tudója csak úgy megosztja az egyszerű plebejusokkal a becses titkot?** Mégis, ha az olvasók közül bárki ebből tartja el magát és családját, kommenteljen nekünk bátran, szeretünk a jó hírekről is beszámolni.



Bár a [dubai MLM kiemelkedő nyertesei sem jeleztek vissza eddig felhívásunkra,](#) **de ez biztos csak az APEH miatti félelmükben nem tették :-).** Ha pedig [valaki esetleg matematikus,](#) és szemléletesen bebizonyítaná az olvasóknak az említett szisztéma lehetetlenségét, őt is szeretettel várjuk még bátrabb kommentelésre.



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szösölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1883735>

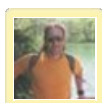
Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.03.31. 14:31:53](#)

Úristen én meg már évek óta nem nézem meg a spam mappám a gmail-ben!
Mennyi pénztől eshettem el eddig! A francha!
Amúgy Húsvétra minden jót!



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu 2010.04.01. 10:56:09](#)

Szia Atko!

Kösz a jókívánságokat, Neked is és minden Olvasónak Boldog Húsvéti Ünnepeket kívánok.

[cworm \(törölt\) 2010.04.01. 13:27:09](#)

Hali, a többi pcworld-ös cikked is elérhető pdf formátumban valahol?



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu 2010.04.01. 14:03:51](#)

Szia Cworm!

Itt van balra egy bazi nagy oldaldobozban az összes.

[cworm \(törölt\) 2010.04.01. 14:57:24](#)

...facepalm...:)

[Lord Bundi 2010.04.02. 19:47:51](#)

Ez már igen régóta ismert trükk
nagyon egyszerű
ha mindig duplázod a pénzed akkor ha mindig veszítesz is, ha legalább 1* nyersz akkor is 1 forinttal többet nyertél mint amennyit előtte veszítettél...
(egyszerű...2es számrendszer (ugyebar abba mindig a duplája a köv szám az előtte lévőnek és az összes előző összege 1el kisebb mint a köv szám))
Ez nem nagy trükk meg milliárdos módszer ez ezer éves...

[actonic 2010.04.12. 16:46:38](#)

Tényleg egyszerű. Ha duplázod a pénzed, és valamikor nyersz, az a veszteségednél mindig több lesz a nyereséged.

Mi van ha pl. 7 veszteségig van pénzed, és pirossal játszol, majd mindig piros lessz még a 8. -on is. Ezt nevezik szerencsejátéknak. Elveszted az összes pénzed, ami sok lehet.

Egyébként logikailag jó.

A kétkedőknek meg írták, hogy próbálják ki demó módban az egészet, aztán rájönnek hogy tetszik vagy nem.

Én két dolog miatt nem csinálom. Nincs most kezdőtőkém ehhez, és kicsit majrás vagyok annak ellenére hogy jó ötletnek tartom. Meg elég sokszor kell szerencsésnek lenned, hogy összejöjjön valami. Na meg hogy mivan a túl sokszor piros vagy fekete.

Valaki okosabb nálam?

Csinálja?

emailcímet a honlapon nem láttam. :(

Ja és félni kell ezektől az oldalaktól,, a kaszinóstól, meg a banki oldalaktól vírusvédelmileg?

Kösz

Robi

actonic 2010.04.12. 17:02:07

@Lord Bundi: Mi a véleményed a antivirus.blog.hu/2010/03/31/hello_steve_terence_vagyok -on amit írtam? Kíváncsi vagyok a véleményedre.

Te játszanál?

Kösz

Robi



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.04.12. 18:57:15**

Szia Actonic!

A kaszinóstól kártevőileg nem kell okvetlenül félni, ha szeretsz játszani, bár átverős, fertőző oldal mindenhol lehet. Aki nem játszik, az bátran bekapcsolhatja a kéretlen, veszélyes, stb alkalmazások szűrését, és akkor az ilyen nem fertőző, de reklámokat kéretlenül adó cuccokat szűri.

A valódi bankos oldalaktól nem kell félni, csak a hamisítottaktól. Figyelni kell, tanúsítványt ellenőrizni, internet biztonsági csomagot használni, OS-t frissíteni, kéretlen linkekre nem kattintani, kb ilyenek.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.04.12. 18:59:08**

Lord Bundi, Actonic:

Jah igen, a sakk játék feltalálója is kért jutalmul egy búzaszemet az első kockába, kettőt a másodikba, és mindig a dupláját a következőbe. Nem sikerült öt kifizetni, mert a 64. kockába már a Földgolyó több évi termését kellett volna tenni :-D

Teljes biztonságot nyújtó Registry bejegyzések

2010.04.01. 13:00 | [Csizmazia István \[Rambol\]](#) | [7 komment](#)

Címkék: [móka](#) [április elseje](#)

Érdekes felvetéssel állt elő két olasz tudós. A számítógépes kártevők évekig tartó alapos viselkedés elemzése után öt olyan rejtett (hidden), és ezáltal nem megváltoztatható, nem törölhető Registry bejegyzést készítettek, amivel 100%-osan meg tudták védeni kísérleti laboratóriumokban tetszőleges Windows alapú számítógépet bármilyen vírustól, féregtől, hamis antivírustól vagy trójaitól.



A teszteredményeket független laboratóriumok többszörös ellenőrzések után is igazolva látták, bizonyítva ezzel a módszer hibátlan működését. Kártevők millióit vizsgálták éveken keresztül, viselkedés analíziseik eredményét mesterséges intelligenciát is magában foglaló rendszerrel dolgozták fel, amíg sikerült leszűkíteni azokat a kulcsfontosságú elemeket, amelyek alapján sikerült elérniük ezt a meghökkentő, de nagyon is sikeres eredményt. A teljes antivirus szakma is kiemelt figyelemmel kíséri Alfonso Scimmia és Henry Lippopotamo váratlan felfedezését, amelyet a kutatók ígéretük szerint először velük ismertetnek majd.



Kísérletük eredményéről a nagyközönségnek jövő hónapban számolnak be majd teljes részletességgel a *Computer Scientist de Aprile Otale* című szaklapban, de amint ismertek lesznek a részletek, az online sajtó is hírt ad majd róla, így várhatóan mi is.

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

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [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/1886279>

Kommentek:

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

[pete_r 2010.04.01. 13:10:01](#)

Április elseje van! Szép jó napot kívánok mindenkinek.:D

[cworm \(törölt\) 2010.04.01. 13:21:48](#)

A címet elolvassa azt mondtam, "nocsak, érdekes lehet", de aztán a második mondat elolvasása után világossá vált a tréfa.:)

[nyos 2010.04.01. 16:46:26](#)

Tenyleg lehet olyan registry bejegyzést csinálni, amivel a rendszer működése teljesen valik, ezáltal kártevók részére is tamadhatatlan. (persze használhatatlan is, de ez részletkerdes)

Apr. 1-et felreteve, a registry és a biztonság között tenyleg van kapcsolat: amelyik gépen egyetlen registry bejegyzés sincs (mert olyan OS, amin nincs), az általában biztonságosabb.

[Sixx! Anyád is nyugger? 2010.04.01. 19:07:47](#)

Továbbá brit tudósok megállapították... :D

[Sixx! Anyád is nyugger? 2010.04.01. 19:09:10](#)

@nyos: bocsi, amit írtál, az valahol kapitális ökörség. Pl. VMS-en is van registry-szerűség, de arra nem mondanám, hogy nem biztonságos.

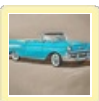


[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.04.02. 08:38:39](#)

Sajnos nincs ilyen varázs Registry kulcs, ezért nem zárnak be az antivirus cégek, és nyergelnek át terítők és díszműárak terjesztésére ;-)

Ha valaki vette a fáradságot, és az újság címét, meg a "tudósok" neveit megnézte translate.google-lel magyarul, az Registry függetlenül szagot kellett, hogy kapjon :-)

Nekem egyébként a csopaki webcamera tegnapi képe tetszett a legjobban :-D
antivirus.blog.hu/media/image/201004/apr1_2.jpg



[Sam. Joe • http://www.matchboxmemories.hu](#) **[2010.04.09. 10:04:02](#)**

Nekem az "Aprile Otale" volt az a pont, ahol leesett a tantusz és röhögtem egy nagyon jót! Szép volt Rambo, jedi vagy még az Alderaanról!!! De tudod mi a kemény?

A TurulMeme.com április kilencedikei - azaz mai - értesítőjében a harmadik helyen szerepelt a hír! Szóval elég sokan beugrottak neki, bár kicsi késéssel. 8-)

Hogyan szűri a Google a kártékony linkeket?

2010.04.06. 14:10 | [Csizmazia István \[Rambol\]](#) | [4 komment](#)

Címkék: [google spam kártevő találatok adathalász keresési ellenőrzése](#)

Azt, hogy a weboldalakon keresztül történő fertőzések hogyan jutnak el az internetezőkhöz (csukott szemmel begépelnek _akármit_ a böngésző címsorába ;-), többször is körbejártuk már. **Áramlanak ezerral az adathalász weboldalak, és üzemszerűen mérgezik a Google keresések találatait is** az éppen aktuális trendek, események, [katasztrófák](#), [sportesemények](#), [botrányok](#), tragédiák, díjátadók, [sztárok valós vagy kitalált haláleseteinek megfelelően](#). Joggal vetődik fel hát a címadó kérdés, a válasz pedig az, hogy bár **mindent időben kiszűrni lehetetlen, azért rajta vannak az ügyön**.



Folyamatosan több millió oldalt vizsgálnak át naponta. Ez az elemzés a hatalmas meglévő és keletkező mennyiség miatt - a víruslaborokba ömlő napi sokezer mintához hasonlóan - nem emberi, hanem **automatikus feldolgozást jelent**. [Elsőként azt nézik meg, hogy egy adott URL tartalmazza-e a "bank" vagy a "login" szavakat](#), illetve szerepel-e benne **domain név helyett gyanakvásra okot adó IP cím**, nem szokatlanul hosszú-e az URL sor - ezek mind adathalász gyanús jelek lehetnek.



A továbbiakban aztán ellenőrzésre kerül, **tartalmaz-e jelszó nevű űrlapmezőt, megnézik a host szerverek területi információit**, stb. Utolsó lépésként pedig az adott oldal esetleges **spamgyanús visszajelzéseit ellenőrzik**, a kétes domain host, és hasonlóké. Ezek az összetett információk adnak aztán egy végső képet, ami alapján ha a Google szükségesnek látja, feketelistára teheti a linket.



Nyilván **az otthoni gépünkön csak egyedül erre az elemzésre támaszkodni helyi biztonsági programok helyett badarság lenne**, de azokat ha némi késéssel is, de **jól kiegészítheti**. Az automatikus ítélet miatt elvélve előfordulhat időnként hamis riasztás, de szerintük az ilyen false pozitív esélye csekély, 1 a 10000-hez.



Több olyan weboldal fordult már meg a kezeink között, [amely "Bejelentett támadó webhely" címkét kapott](#), de ezek közül nálunk **még egyetlen olyan sem volt, amelyik ezt indokolatlanul kapta volna**: végül [mindegyikben megtaláltuk azt az iframe vagy javascript elem](#) amely valóban gyanús kínai vagy orosz oldalakra mutatott.



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:



- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1898263>

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](#).



Morci úr • <http://suttyok-ket-kereken.blog.hu> **2010.04.06. 17:52:45**

A női portál noiportal.hu
Többször is le volt tiltva a google által.
Aztán másnap helyre állt.
Az véletlen lenne. Többnyire csajos témák vannak rajta.

[tommybravo](#) 2010.04.06. 17:54:37

Egy elég durva false positive-ot azért tudok mondani: az origo egyes aloldalait rendszeresen rakta tiltólistára a google, és általa a Firefox is. Ha jól emlékszem valamelyik tracking code-ot nem szerette a kereső, de aztán megoldották valahogy.

[repecs](#) 2010.04.06. 19:13:23

nehogy már hozzá lehessen szólni:
index.hu/kulfold/2010/04/06/igy_lottek_helikopterrol_az_irakiakat/

[Nyelvész Józsi](#) • <http://szleng.blog.hu/> 2010.04.06. 19:54:12

[@tommybravo](#): Nem false positive volt, hanem iframe-en keresztül bejutott malware. És tényleg megoldották. :)

Neve? Besorolása? Felismeri? Válaszoljon!

2010.04.08. 14:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [blog](#) [david](#) [trójai](#) [abrams](#) [féreg](#) [randy](#) [harley](#) [kérdézz](#) [felelek](#) [nevezéktan](#)

Az ESET threat blogban nemrég [szerepelt egy bejegyzés, amelyben olvasók beküldött kérdéseire feleltek](#). Mennyire törekednek a különböző antivirus cégek az egységes kártevő elnevezésekre, és hogy lehet hogy például a VirusTotal oldalon **egy adott kártevő az egyiknél féreg, míg a másiknál trójai**? A felvezetőt és a válaszokat olvasva láttuk, hogy a kérdések izgalmasak, és talán másokat is érdekelhetnek, így **mi is közreadjuk ezeket**.



Kérdés: Mennyire fontos, hogy a kártevőknek pontos, egyedi neve legyen?

David Harley: Az észlelés és eltávolítás szempontjából ez nem annyira lényeges és az antivirus gyártók névadással ezt nem is tudják időben követni, hiszen a heti százezer új kártevő megjelenésével ez egyenesen kivitelezhetetlen. Az azonnali osztályba sorolás ezzel szemben tényleg kulcsfontosságú. A különböző antivirusok által használt egységes elnevezés bármennyire jó lenne, lehetetlen. Amíg egy adott kártevőt az egyik program felismer, egy másik talán nem, vagy még nem, és sok esetben egy adott kártevőket terjesztő weboldal is sokféle formában terjeszt egy adott kártevőt: visszafejtést gátló exe tömörítőkkal újracsomagolva, a kód szándékos összezavarásával a felismerés megnehezítésével kínálja letöltésre ugyanazt a kórokozót.



Randy Abrams és David Harley

Aki a témában további részletekre kíváncsi, az alábbi dokumentációkban olvashat erről bővebben:

<http://www.eset.com/resources/white-papers/cfet2009naming.pdf>

<http://www.eset.com/resources/white-papers/Harley-Bureau-VB2008.pdf>

Randy Abrams: A pontos elnevezés kiemelten fontos, ha egy adott kártevőről és annak viselkedéséről beszélünk. A legtöbb esetben azonban a védekezéshez nincs szükségünk a konkrét névre.



K: Szükséges-e, hogy az egyes kártevők konkrét nevei, illetve az egyes antivirus gyártók kórokozó elnevezései szinkronban legyenek?

DH: Az egységes nevezéktan nem szükséges, az esetleges kivitelezése pedig egyenesen lehetetlen. Vannak persze kezdeményezések, amik legalább fő vonalakban egységesítené a nevezéktani szabályokat - például a [Common Malware Enumeration \(CME\)](#) - de ehhez folyamatosan nagy erőfeszítések kellenének kivétel nélkül minden egyes gyártó részéről.



RA: Szinte lehetetlen ennek a megvalósítása. Ha naponta csak 200 minta feldolgozását vesszük - ami messze csak a töredéke a napi beérkező mennyiségnek - a nevezéktani egyeztetések feladatait már egy külön főállású munkatársnak kellene végeznie, aki csak ezzel foglalkozna, és ugye ezt minden egyes AV cégnél egyszerre kellene végezni. Nem érné meg a ráfordítás. Az elnevezéssel kapcsolatos teendők másodlagosnak tekinthetők a sokkal fontosabb és lényegesebb feldolgozás, felismerés, megelőzés, mentésítés mögött.



K: Sokszor látok hasonló nevű kártevőket, amik az egyik gyártónál mint féreg, a másiknál pedig mint trójai szerepel. Hogy lehetséges ez, és akkor ez pontosan mit jelent?

DH: A terjedése lehet olyan, mint egy féreg, de ezenfelül rendelkezhet olyan jellemzőkkel, mint a trójai programok, amelyek látszólag

valamilyen hasznos programnak látszanak, de valójában kártékonyak.



RA: Néha, az is előfordulhat, hogy a vírusirtó cégek tévednek. Egy fégnek valóban lehetnek trójai tulajdonságai, de persze nem minden fég trójai, és a trójaiak többsége nem fég. Van olyan cég is, amely egy Javascript férget VBS fégnek nevez.



K: Ha egy antivírus minél több különböző kártevőt különböztet meg, akkor ez egyben azt is jelenti, hogy egyben sokkal precízebb is a mentesítési képessége?

DH: Nem, semmiképpen. A generikus felismerés és mentesítés napjainkban a legfontosabb feladat, és ez sokkal inkább megvalósítható, mint minden egyedi minta vagy alváltozat elkülönítése. De persze a végrehajtás előtti felismerés és blokkolás még mindig jobb, mint az utólagos tisztogatás.



RA: A több megkülönböztetett kártevő név nem okvetlenül jelent több felismert kártevőt is egyben. És persze az egyedi felismerési név még nem garantálja a problémamentes eltávolítást. Egy kártevő észlelése egyáltalán nem jelenti annak sikeres eltávolítását, és a mentesítés egyúttal azt is jelenti, hogy kompromisszumot kötünk a biztonság rovására. Aki számára a biztonság végletesen fontos, az nem mentesít, hanem ilyenkor újrahúzza a gépet mentésből. Hiszen egy adott kártevő észlelése nem jelentheti automatikusan azt, hogy százszázalékosan minden összetevőt, fertőzési komponenst sikerült ezzel felfedezni. Ezt akkor értettem meg igazán, amikor a Microsoftnál dolgoztam, ott valóban minden incidensnél újratelepítették a gépeket.



K: Az olyan antivírus motorok, amelyek komolyan támaszkodnak a heurisztikus felismerésre - mint például az ESET is - ezeknél mondhatjuk, hogy az eltávolítási képességeik kevésbé erősek, mint azoknak a programoknak, amelyek inkább a szignatúra alapú detektálásban erősek?

DH: Attól függ, mit nevezünk sikeres eltávolításnak. Láttam már olyan tesztet, ahol az eltávolítási képességet lepontozták amiatt, hogy maradtak hátra olyan összetevők, amik már semmilyen veszélyt nem jelentettek. Az én olvasatomban a sikeres eltávolítás az, amikor annak elvégzése után már semmilyen utólagos probléma nem jelentkezik. Lehetnek a mentesítésnél olyan speciális esetek, amikor egy generikus felismerés nem lenne annyira sikeres, mint egy egyedi alváltozatra kidolgozott eljárás, illetve az is okozhat időnként problémát, ha az ilyen teljesen egyedi variáns vagy közeli alváltozat felismerése, azonosítása hibásan történik. A lényeg, hogy a fejlett heurisztikus felismerés és a viselkedés analízis segítségével még az esetleges fertőzés előtt sikeresen detektálhatunk olyan kártevőket, amelyek még nem is szerepelnek a szignatúra adatbázisban. Amint kapunk bővebb információkat az egyes veszélyekről, úgy bővítjük a felismerési és mentesítési részeket. A heurisztikának nem az a célja, hogy a szignatúra alapú felismerés helyébe lépjen, hanem ez egy olyan technika, amely egyáltalán nem csökkenti a vírusadatbázis fontosságát.



RA: Ahogy David is jelezte, különféle megközelítések léteznek a mentesítésre. Nem ismerek olyan specifikus tesztet, amelyet jelentős mennyiségű és változatos kártevő mintán végeztek volna el. Vagyis ezt az elméletet - miszerint mely program hatékonyabb a mentesítésnél - semmilyen tudományos bizonyítékkal nem tudjuk egyelőre eldönteni. Ami biztos, hogy a felismerési képesség - legyen az szignatúra alapú vagy akár heurisztikát használó - valóban nem azonos az eltávolítási képességgel, és nincs egyenlőségjel ezek között.



K: Mi a különbség a "trojan dropper" és a "trojan downloader" elnevezések között?

DH: Egyszerűen fogalmazva a trojan dropper telepít és elindít egy másik programot (ami nem okvetlenül rosszindulatú, de sokszor trójai, azaz titkolt funkcionálást hajt végre). Régebben a dropper szót olyan értelemben is használták, mint hogy egy kártevő saját magából további kártékony kódokat csomagolt ki és indított el. Ezzel szemben a trojan downloader letölt valamilyen további kártékony kódot, amit

azonban nem okvetlenül telepít is, illetve futtat le. Valójában nincs olyan egységesen elfogadott szabatos meghatározás, amely egységesen jellemezné a különböző antivírusgyártók leírásait, és sok esetben tovább bonyolítja a helyzetet, hogy az antivírus cégek víruslaboratóriumában dolgozó kutatók és a marketing osztályon dolgozó munkatársak is különbözőképpen használják ezeket a kategóriákat. A biztonsági kutatás nehéz terep, és elkerülhetetlen, hogy az osztályozás, besorolás, meghatározás folyamatában viták legyenek, persze ehhez a kártevők egyre növekvő komplexitása is hozzájárul.



RA: Igen, a dropper szócska utal arra, hogy az adott - jellemzően trójai - program "kidob" magából valamilyen másik, többnyire kártékony kódot. A legelső Access makró vírus is ilyen volt, azonban a készítője egy pitiáner szintaktikai hibát vétett, így a dropper funkció meghiúsult benne. A downloader kategória pedig az internetről, esetleg egyéb hálózati kapcsolatról további kódokat letöltő funkcionalitást jelent, és ez igen jellemző a mostani kártevőkre.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [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/1903791>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Hatásos és eredményes mód a személyiséglopás

2010.04.12. 15:10 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [arizona lopás](#) [csalás](#) [hamis adóbevallás](#) [személyiség](#)

A [kockázatok ismertetésénél](#) többször is szó esett már az úgynevezett [identity theft](#), azaz [személyiséglopásról](#), de [ennek jelentőségét valószínűleg sokan rendre alulértékelik](#), úgy vélik, olyan ez, mint a közlekedési baleset vagy a vakbélgyulladás: velünk soha, mindig csak mással fordulhat elő. Hát nem így van, a mostani bűnöző csapat pénzügyi eredményeit látva talán sikerül ehhez egy kis "Aha élményt" okozni.



Ugyan mit árthatnak nekem, hiszen én csak egy egyszerű hétköznapi ember vagyok. A most horogra akadt arizonai csapat bevétele vastagon rácáfol az ilyen álnaív megközelítésre. Mi az hogy, nem csak hogy lehet, de ráadásul igen sok pénzt lehet így szerezni, **már ha 4 millió dollárt annak tartunk ;-)** A [bűnszervezet kifinomult trükkökkel hamis adóbevallásokat nyújtott be ellopott azonosítókkal, illetve elhunyt személyek adataival visszaélve](#).



A nyomozás adatai szerint **legalább három éven keresztül végezték üzelveiket**, és ehhez számos nevet, társadalombiztosítási számot, cégnevet és adóazonosító számot használtak fel. A mintegy 1900 benyújtott hamis adóbevallásból úgy tudtak pénzt csinálni, hogy az ottani gyors reagálású **elektronikus bevallási rendszer szerint lehetőség van az adóvisszatérítést rövid időn belül bankkártyára visszautalva megkapni**, és az ilyen kérelmekből óriási mennyiséget kell viszonylag rövid idő alatt tömegesen feldolgozni - és mindezt érdemi ellenőrzés nélkül.



Most a börtönben ülve gondolkozhatnak el az 5.5 millió dolláros büntetésen, de **vélhetően nem azt sajnálják majd, amit elkövettek, hanem csak azt, hogy végül lebuktak**. Tegyük azért hozzá, **ha valaki rendezetlen szabályozású országokból (Kína, Ukrajna, Vietnám, stb.), többszörösen láncolt proxykon keresztül hajtja végre jól eltervezett cselekményeit, jó eséllyel megúszhatja**.



A [lebukási ráta sajnálatos módon még mindig roppant alacsony](#), a **bizonyítási procedúra pedig - különösen nemzetközi vegyes bűnelkövetői kör esetén - elképesztően körülményes**. Ebben a konkrét esetben a szervezetbe beépült titkosügynökök tették lehetővé az áttörést a nyomozásban, illetve segítették elő a leleplezést, és a vádemelést.



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



Tweet

Ajánlott bejegyzések:

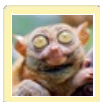
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [A jelszó érték, vigyázzunk rá](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1913919>

Kommentek:

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



[DeToXXX 2010.04.12. 17:02:32](#)

ha nem lennének kapzsik le sem buknának :P

Nagy a forgalom a közösségi oldalakon

2010.04.14. 16:00 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam facebook csalás twitter közösségi oldalak kártevő](#)

Egyre többen használják a közösségi oldalakat. A felhasználók megnövekedett száma [a tettekre kész családokat, spammelőket, kártevő terjesztőket sem hagyta állva](#), egyre sikeresebben alkalmazkodnak és élnek az új lehetőségekkel.



Van aki csak passzióból, van aki munkahelyi kapcsolata miatt kénytelen, és csak nagyon kevesen utasítják el teljesen a közösségi oldalakat. A magyar Iwiw, a roppant népszerű [Facebook a maga 400 milliós felhasználói táborával](#), a Myspace, Skype, vagy akár [a Twitter 75 millió tagjával](#) teljességében új helyzetet teremtett, különösen a fiatal felhasználók táborában. Egy amerikai felmérés szerint [a 12 évesnél idősebb gyerekeknek már a fele \(48%\) tagja a közösségi portáloknak, és azt naponta többször is használja](#). Ez az a korosztály, akik szerint a lassú és körülményes e-mail már csak a nyugdíjasok ódivatú csigalassú kispolgári csökevénye, és a tájékozódásban is jelentős mértékben támaszkodik erre a hihetetlen tempóban növekvő, és villámgyors web2 lehetőségekre.



Ha valaki nézte az április 11. választások napján az Origó címlapját, az érzékelhette, milyen tempóban keletkeztek posztok, szinte az átlagfelhasználók ütőerén tarthatta az ember a kezét, **realtime-ban jöttek a vélemények, hozzászólások**, felismerések, viccek (*Aki ma tulipánt rajzol a szavazólapra, annak a Voksán Virág lesz; Orbán Viktor szerint ma egy új országban ébredünk. Az időjárásból kiindulva ez Anglia :-D, és hasonlók*). Mivel még nincs vége a kampányidőszaknak, [a Twazzup.com oldalon még bele lehet lesni az ilyen pörgő, gyorsan frissülő gyűjtő boksokba, ha ott kereső szónak megadjuk például "#valasztas OR #valasztas2010 OR #voks2010 OR #voks OR #voks10 OR #kampanycsendkiraly" sztringet](#).



Ezek az informálódásban valóban tényleg jó perspektívákat nyújtó lehetőségek, ám emellett az is szükséges, hogy [a veszélyekkel az ember tisztában legyen](#). Ez mindent jelent, a nekünk küldött üzeneteket [éppúgy, mint a gyanús telepíthető "gyári" applikációkat](#), továbbá hogy [nem szükséges életünk minden egyes másodpercéről beszámolnunk](#).



Ahogy az internet világában, vagy az e-mail küldők táborában, **itt sem mindenki az akinek mondja magát, vagy éppenséggel Grál lovag**. [Az adathalászat főtétele éppen az, hogy a nagyszámok törvénye miatt érdemes próbálkozni](#), hiszen a megtévesztett 1-5% már meghozza a konyhára a szükséges profitot, és itt több százmilliós felhasználó táborról beszélünk!



Folyamatosan változnak maguk a közösségi oldalak is. Ugye lassan kiderül, [hogyan csinálták azt a bizonyos első milliót, amit nem illik később firtatni](#). Aztán amikor felfut a cég, jól fut a szekér, [akkor jönnek vele a kérértlen reklámok, hirdetések is](#). Szerencsére [az SMS spam nem érte el \(még?\) a komolyan zavaró küszöböt](#), de a közösségi oldalakon küldött kérértlen reklámok, kártevőre mutató linkek, csalások azonban már nagyon jelen idősek, és tucatjával próbálják megtéveszteni a felhasználókat.



Éljen hát az egészséges gyanakvás, óvatosság, **a terep megváltozott, de a mögöttes szándékok és az emberi természet viszont nem.**

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Informatikai biztonság az egészségügyben](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [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/1920203>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Harmadik típusú hamis antivírusok

2010.04.15. 16:30 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [csalás](#) [hamis jogi licence](#) [szerzői scareware](#) [viola violation](#)

A hamisítás, a csalás lényeges eleme, hogy úgy operáljon, úgy jelenjen meg nagy magabiztossággal, határozott fellépéssel, mintha igazi lenne. [Lehet ez ál rendőr](#), ál rendőr igazolvány, [hamis Dakar rali kíséző kamion](#), banktól [érkező levél vagy bármi](#). A tavalyi év [drákói szigorúságú RIAA szerzői jogi pere](#)i új inspirációt adtak a bűnözőknek.



[Pont tegnap volt szó arról, a széles merítés a felhasználók óriásira duzzadt táborában](#) és a mindig palira vehető 1-5% gyanútlan és naív ember [rendre kifizetődővé teszi a csalásokat](#). Most egy olyan új konstrukció kezd kibontakozni, amely várhatóan [a hamis antivírus csapás mellett sok pénzt fog hozni](#) a kiagyalók konyhájára. Azért mellett, mert a számítógépes [kártevők és csalások világában az evolúció](#) nem azt jelenti, hogy valami fejlődik, és a régi megszűnik, hanem az egyre újabb kockázatok a régiekkel párhuzamosan egyidőben jelennek meg.



Az új találmány neve: [hamis szerzői jogi büntetés](#), de mi hívhatjuk Szerzőijogi Violának is :-)) A naív ügyfél letölt valamit a Bittorrent hálózatról, és ezek után a felugró Javascript ablak nem álfertőzésekről tájékoztat, hanem illegális letöltésről, ejnybejnyéről, pénzbüntetésről. Valódinak lázó hivatalos pecsétben, flepniben nincs hiány, és az állítólagos svájci székhelyű ICCP Foundation felszólít a csak most, csak nekünk összesen négyszáz dollár befizetésére, és így elkerülhetjük az esetleges sanyarú pert a maga zord következményeivel: 5 év börtön, 250 ezer USD helyett.



Bár az ICCP azt sugallja, munkakapcsolatban áll a valódi jogvédő szervezetekkel (RIAA, MPAA, stb.) ez nem igaz. Sőt berezelní sem kell, és szintűgy nem javasolt turkálni a Visa vagy Mastercard kártyánk után, mert ez az egész egy ordas nagy csalás. Ha először csak a domaint nézzük, már kilóghat a lóláb. Mert mi is a sansz arra, hogy az állítólagos nagyhírű komoly svájci alapítvány honlapját oroszok jegyezzék be [idén február 24-én és üzleti emailcímük az info@rustelekom.biz legyen](#)? Ugye ennek az esélye kb. akkora, mint vizilónak az epsomi derbin. A weboldal egyébként már nem is jön be, a Google azonban [emlékét kegyelettel megőrizte a hálásszívű utókornak - egyelőre](#).



A kártevő egyenesági leszármazottja a [hamis antivírusoknak \(scareware\)](#), ugyanaz a csapat fejlesztheti napi nyolc órában, és az orosz illetőségű főnök is valószínűleg ugyazzal a vizilóbörkorkorbaival hadonászva rendeli meg tőlük az új funkciókat a szerzői jogi kamu programban, amivel előtte a hamis antivírusnál a rendeléseit leadta.



A program fertőzés esetén [sok helyen belegányol a rendszerbe](#), kiirtása - különösen ha nem volt a gépen előtte semmilyen vírusirtó - nehézkes, sziszifuszi munka. Szerencsére már nem kell nulláról kitalálni a levakarás mikéntjét, [megtették ezt már helyettünk mások, elég követni a részletes útmutatójukat](#).



Gyaníthatóan a **"hogyan szerezzünk pénz munka nélkül"** eme módszerével fogunk még többször is találkozni az idei évben.



Ez az egész egyben erős készítés is lehet arra, hogy a **védelmi programunkban** a kéretlen alkalmazások, veszélyes alkalmazások, és **hasonló kategóriákat végre mindenki bekapcsolja detektálásra** - jogi okokból ezek alapértelmezetten nem kerülnek keresésre -, és irtsa még az irmagjukat is.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1922867>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Böngészési előzmények, mint közpréda

2010.04.19. 14:04 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hirdetés](#) [vírus](#) [pornó](#) [facebook](#) [deep előzmény injection](#) [packet targeting](#) [böngészési](#)

Folyamatosan új utakat keresnek (pl. targeting, [Deep Packet Injection](#)) a legális cégek éppúgy, mint a kártevőterjesztők. Épp a minap számoltunk be arról, hogy a hamis antivírusok [után most a hamis szerzői jogi büntetés dívik](#), de megjelent már egy olyan vírus is, amely a pornó oldalak látogatóinak böngészési előzményét teszi ki büntetésül közszemlére.



Egy adott oldal keresési előzményeire épített, és célzott hirdetési módszer nem újkeletű, bár személyiségi jogok szempontjából azért okozhat ez is nehéz perceket. Ha valaki **csak egyszer is rákeres az Amazonban például a dildo-ra** (igyekszünk óvatosan fogalmazni, és persze természetesen csakis kizárólag a szomszédja nyomatékos kérésére teszi ezt az illető), az nyilván nem akarja, hogy ettől kezdve az áruházba lépve az ő személyes profilja csupa ilyen termék akciós reklámjával borítsa be a kezdő-üdvözlő képernyőjét.



Ha pedig az adott áruházat netán az egész család minden tagja látogatja, úgy szintén szalonképtelen ötletnek lehet ezt minősíteni.



Most a [Facebook készül állítólag a böngészési előzményt is figyelembevevő testreszabott](#) reklámokat megjeleníteni, mert ugye kell a pénz. Egyelőre ennél [pontosabb részleteket nem lehet tudni a szerdai bejelentés előtt](#), de az ezzel kapcsolatos félelmek már javában élnek.



Talán Svédországban volt olyan korábban, hogy **publikus weboldalon webkamera mutatta a bordélyházak bejárati ajtaján belépő és onnan távozó vendégeket**, akiket a nyilvános szerepelés nyilván kevésbé tett boldoggá, viszont az intézkedés célja a képmutatás és a prostitúció elleni eredményes harc volt. Egy családos parlamenti képviselő munkaidőben látogatott, és bukott meg így. Picit erre hasonlít a [bevezetőben említett kártevő, amely Japánban jelent meg, és egy fájlmegosztó oldalról történő erotikus tartalom letöltése esetén igyekszik megzsarolni a felhasználót](#) azzal, hogy a kiolvasható összes adatát előzményekkel együtt közszemlére teszi, a levételért pedig pénzt kér: [ez 400 dollárba kerül a delikvensnek](#).



Félő, hogy hasonló kártevők máshol is meg fognak jelenni, ezáltal aztán a warez oldalak, de akár pártszimpátiák, betegségek, látogatott banki oldalak és más bizalmas, személyes adatok a későbbiekben bárki által olvashatóan nyilvánosságra kerülhetnek municiót szolgáltatva a bűnözőknek személyiséglopáshoz, zsaroláshoz.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:



- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1933738>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Kevésbé foglalkoztatott ... etikus hackerek

2010.04.19. 11:50 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [személyes adásvétel adatok hacker kretén lopott etikus kevésbé foglalkoztatott bébiszitterek](#)

A [halhatatlan, de papírmájában sajnos már megszűnt Kretén magazin](#) egyik kedvelt rovata volt a "Kevésbé foglalkoztatott bébiszitterek". Abszolút alkalmilag, ritkán vagy esetleg soha többé - most mindenesetre **mi is bemutatunk egy hasonló testvérrovatot, aztán ki tudhatja, mit hoz a jövő, lesz-e téma**, ami az utcán hever majdan.



Az etikus hacker nem fából vaskarika, hanem egy [komoly technikai felkészültséget igénylő, és elfogadott szakmává nőtte ki magát, amelyet számos vállalkozás üz. profi módon](#), oktatása is hasonlóan színvonalas keretek között történik [például a Netakadémia szervezésében](#).



Ezúttal következzen egy kevésbé etikus hacker hirdetése :-D, linket azért már mégse, de képet igen lehet :-)



 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1933529>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 (törölt) 2010.04.19. 15:25:19

Hát ez a hirdetés elég béna...)

Jelen esetben pedig egy l-lel kell írni a halhatatlanságot.)



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.19. 15:31:25

- Milyen a hallása?
- Római katolikus.
- Nem a vallása, a HALLÁSA?
- Ja, az kitűnő :-)

Köszí Cworm, javítottam

Conficker a csúcson, újoncok a páston

2010.04.20. 10:04 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

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

A Conficker féreg hónapok óta **bebetonozva őrzi vezető helyét** a magyarországi vírustoplistán. Új kártevők azonban márciusban is megjelentek: **két trójai és egy féreg került fel** sereghajtóként a listára.



Az ESET **minden hónapban összeállítja a Magyarországon terjedő** számítógépes vírusok toplistáját, melynek elemzése tanulsággal szolgálhat a felhasználók számára. **A magyar lista első helyét 2009. október óta a Conficker féreg tartja**, amely az operációs rendszer frissítéseinek hiányát, a gyenge admin jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed.



A márciusi toplistán **második helyén lévő INF/Autorun vírus szintén régi szereplő**. Ez a kártevő kizárólag az automatikus futtatás lehetőségét használja ki a terjedéséhez. Mivel **a legtöbb felhasználó nem tiltja le** ezt a funkciót a Windows operációs rendszerek alatt, és sokan nem figyelnek oda a vírusirtó szoftverük frissítésére, a kártevő zavartalanul terjed.



A listán új szereplő a nyolcadik helyre felkapaszkodó Win32/Boberog féreg, amely **képes hátsó ajtót nyitni** a megfertőzött számítógépen. Számos manipulált rendszerleíró adatbázis bejegyzést is készít, ezek teszik lehetővé, hogy **a kártevő a kommunikációja során a tűzfal védelmét is kikerülhesse**. A program ezután folyamatos kapcsolatot nyit a támadónak, aki így az IRC csatornán távolról átveheti az uralmat a megtámadott gép felett.



Kilencedik helyen bukkant fel a Win32/Tifaut trójai, amely fájlokat hoz létre, és azok automatikus lefuttatásához külön Registry bejegyzést is készít. Működése során különféle weboldalakhoz kísérel meg csatlakozni, és **azokról további kártékony kódokat tölt le** a megfertőzött számítógépekre.



Tizedikként szerepel a **Win32/TrojanProxy trójai**, amely nevéhez hűen valóban **rejtett funkcionálissal bír**. Futása közben megváltoztatja a HKLM\SOFTWARE\Microsoft\Internet Explorer\Main Registry bejegyzést, valamint hátsó ajtót nyit a fertőzött gépen, majd megkísérel távoli webhelyekre csatlakozni.

Végül következzen a magyarországi toplistán. Az ESET **több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere** szerint 2010 márciusában az alábbi 10 károkozó terjedt a legnagyobb számban. Ezek együttesen az összes fertőzés 25.28%-ért voltak felelősek.



1. Win32/Conficker féreg

□**Elterjedtsége a márciusi fertőzések között: 5.95%**

Működés: A Win32/Conficker egy olyan hálózati férgek, 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 férgek módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válnak a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható a külső meghajtó fertőzött Autorun állománya miatt.

Bővebb információ: <http://www.eset.hu/virus/conficker-aa>



2. INF/Autorun vírus

Elterjedtsége a márciusi fertőzések között: 3.63%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájl 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/virus/autorun>



3. Win32/Agent trójai

Elterjedtsége a márciusi fertőzések között: 3.35%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (például Temp mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/agent>



4. Win32/TrojanDownloader.Bredolab trójai

Elterjedtsége a márciusi fertőzések között: 3.13%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, mely távoli oldalakról további kártékony kódokat tölt le és hajt végre. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is kulcsokat készít, illetve módosít a biztonságítamogatás-szolgáltató (SSPI - Security Service Provider Interface) szekción. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.



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

Bővebb információ: <http://www.eset.hu/virus/trojandownloader-bredolab-aa>



☐ INF/Conficker vírus

Elterjedtsége a márciusi fertőzések között: 2.23%

Működés: Amennyiben böngészés során az autorun.inf fájl valamely egység főkönyvtárába kerül, akkor a betöltő eléri, hogy a kártevő kódja induljon el. Vagyis az INF/Confickernek az a szerepe, hogy betöltse magát a Win32/Conficker kártevőt.



A számítógépre kerülés módja: Fertőzött weblapról, vagy külső eszközön keresztül.

Bővebb információ: <http://www.eset.hu/virus/conficker>



6. Win32/PSW.OnLineGames trójai

Elterjedtsége a márciusi fertőzések között: 2.19%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozóknek rootkit komponense is van, amelynek segítségével igyekeznek állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. 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/virus/psw-onlinegames-nnu>



7. Win32/VB.EL féreg

Elterjedtsége a márciusi fertőzések között: 1.85%

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/virus/vb-el>



8. Win32/Boberog féreg

Elterjedtsége a márciusi fertőzések között: 1.20%

Működés: A Win32/Boberog féreg egy olyan kártevő, amely képes hátsó ajtót nyitni a megfertőzött számítógépen. Első lépésként fájlokat hoz létre a C:\Windows\System, illetve C:\Windows\System32 könyvtárakban, ezek automatikus lefuttatásáról pedig külön Registry bejegyzésekkel gondoskodik. Emellett számos manipulált rendszerleíró adatbázis bejegyzést is készít. Ezek lehetővé teszik például, hogy a kártevő kikerülje a tűzfalt azáltal, hogy a létrehozott állományokat a tűzfal szabályai között megbízható fájlként regisztrálja. A féreg futása során folyamatos kapcsolatot tesz lehetővé a támadónak, aki az IRC csatornán távolról átveheti az uralmat a megtámadott gép felett.



A számítógépre kerülés módja: Fertőzött weblapról, e-mail mellékletben, vagy külső eszközön keresztül.

❑**Bővebb információ:** <http://www.eset.hu/virus/boberog-m>



9. Win32/Tifaut trójai

Elterjedtsége a márciusi fertőzések között: 0.89%

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 Registry bejegyzést is készít. 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/virus/tifaut-a>



10. Win32/TrojanProxy trójai

Elterjedtsége a márciusi fertőzések között: 0.86%

Működés: A Win32/TrojanProxy trójai a nevéhez hűen rejtett funkcionalitással bír. Futása közben megváltoztatja a HKLM\SOFTWARE\Microsoft\Internet Explorer\Main Registry bejegyzést, valamint hátsó ajtót nyit a fertőzött gépen, és titokban megkísérel távoli webhelyekre csatlakozni.



A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: <http://www.eset.hu/virus/trojanproxy-wopla-nae>

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1935517>

Kommentek:

nyos 2010.04.20. 12:40:25

Ha ennyi vírus/trojai van, ami távoli weboldaltól tölt le újabb kódot, akkor miért nem kapják el azt, akinek az oldalára a URL mutat? Gondolom nem biztonságtechnikai kutatók oldalán van fent a kártevő többi része (ha ott lenne, könnyen arrebbszerezhetné), hanem valami black hat fickó oldalon.

A víruskészítők a fenti elkerülése érdekében miért nem p2p hálózatról töltik le a továbbiakat? Esetleg a frissítés is mehetne ilyen elven, elvileg már van olyan botnet, ami p2p elven kap parancsokat, szóval nem lenne nehéz implementálni.

Ha technikai okokból mégis a webhez ragaszkodnak, akkor közbeiktathatnának egy plusz reteget. Mondjuk letarolnak a vírus kódjába 10-20 egyedi keresőszót, és egy egyszerű webklienst + parsert, ami a guglin rákerek az adott szavakra, és ha találat van, akkor az oldalról letölti azt a programot, amit szintén a kódjába egészítve megtalál. Így a vírusírók a későbbiekben is el tudják érni, anélkül, hogy addig a lebulást veszélyeztetnék.

Tíz gyanús jel, hogy zombi-e vagy

2010.04.22. 13:15 | [Csizmazia István \[Rambol\]](#) | [57 komment](#)

Címkék: [fertőzés jelek](#) [zombi botnet](#) [sysinspector](#) [gyanús](#)

A legfrissebb [negyedéves Symantec összefoglalóból](#) az derült ki, hogy Magyarország a 9. helyet foglalja el a botnet fertőzött országok sorában. Ha ez így van, érdemes lenne több figyelmet fordítanunk a védelmünkre. Az [ESET egy listában foglalta össze, mikor kezdjünk el gyanút fogni](#), hogy mégsem mi vagyunk a főnökök a saját számítógépünkön.



Jöjjön akkor a **lista a leggyakoribb jelzésekről**. Ha ezek közül többet is, vagy akár mindet ismerősként üdvözölhetjük, akkor **érdemes lehet egy alapos vírusellenőrzést végrehajtani**.

1. Túlágosan sokszor pörögnek fel ok nélkül a hűtőventilátorok jelezve azt, hogy erősen dolgozik a gép, akkor is, amikor éppen nem is dolgozunk rajta. Persze ez még önmagában nem jelent semmit, lehet hogy éppen most tölti le és telepíti a gép a Microsoft frissítéseket, illetve a poros számítógép belső is okozhat intenzívebb ventilátor tevékenységet. Mindenesetre azért ez egy elég feltűnő jel, amire érdemes odafigyelni.



2. Minden ok nélkül túlágosan sok ideig tart, amíg a gép kikapcsol (shutdown), vagy ez nem is sikerül neki. Ez a pont is hasonlít az előzőre abból a szempontból, hogy ezt is okozhatja számos dolog, ami lehet kártevő is, de lehet rosszul megírt meghajtóprogram, kevés lemez hely, és még sok minden más. Természetesen a szokásos havi második kedden végzett frissítéssel egybekötött kikapcsolás egy teljesen más térszta, de ott ki is van írva mindez. De az összes többi esetben ez is egy jelzés lehet a sok közül.



3. A Facebook üzenő falon hosszú tömött sorban állnak a látszólag nevünkben küldött üzenetek. Érdemes haladéktalanul Facebook jelszót változtatni, és új erős, teljesen egyedi jelszóra cserélni, végül a számítógép teljes kártevő ellenőrzése is szükséges ilyenkor.



4. A programjaink igen lassan (mint a Technocolba mártott csiga) futnak. Ez persze adódhat a gyenge harver miatt, vagy ha valóban több ezer állományt kell feldolgozni. A pontosabb megfogalmazás így inkább a szokatlanul lassan **az eddigiekhez képest** lehetne, ez már jól fedi a lényegét.



5. A rendszer nem engedi letölteni a legfrissebb Microsoft frissítéseket. Ez szintén eléggé jellemző szimptóma, ezzel igyekeznek megakadályozni a kihasználható sebezhetőség befoltozását. Azért ha lopott Windowst használunk, akkor ennél a pontnál ne csak botnetre gyanakodjunk elsősorban ;-)

6. A rendszer nem engedi letölteni a legfrissebb vírusadatházist, illetve egyes vírusvédelmi weboldalak nem is jönnek be a böngészőben. Ez már egy nagyon jellemző tünet, például a [Conficker féreg esetében üzemel is egy ilyen teszt weblap](#), ami pontosan ezekre támaszkodva mutatja ki a fertőzést.



7. Rövidebb-hosszabb ideig az internet sebessége drámaian lelassul. Mivel a fertőzött zombi gépek gyakran vesznek részt távoli DoS támadásokban, hatalmas mennyiségű spam levél kiküldésében, ezért a bejövő-kimenő forgalom figyelése, hirtelen megváltozása ugyancsak érdekes lehet. Egy állandó internetforgalom figyelő diagram a tálcán vagy az asztalon, illetve a tűzfal naplófájlok rendszeres ellenőrzése segíthet ilyenkor a nyomozásban.

8. A barátok, családtagok, ismerősök azt jelzik, leveleket, üzeneteket kaptak tőlünk, pedig mi nem is küldtünk nekik semmit. Ez utalhat botnetre, de emellett előfordulhat más kártevő fertőzése, illetve előfordulhat a postafiókunk feltörése is. A haladéktalan jelszó csere, és az alapos vírusellenőrzés mellett könnyen ellenőrizhetjük ez utóbbit például a Gmail esetében, ahol azt is meg tudjuk nézni, hogy legutóbb milyen IP címekről léptek be postafiókunkba.

9. Hirtelen popup ablakok kezdenek el megnyílni, reklámok jelennek meg, akár úgy is, hogy a böngésző el sincs indítva. Ez a jelenség valamilyen reklámmal kapcsolatos bot kártevő jelenlétéről árulkodik.



10. A Windows Feladatkezelőben furcsa nevű programok, folyamatok tűnnek fel. Ez megintcsak nem egy kizárólagos jellemző, hiszen számos hardver illetve szoftver komponens használ ilyeneket. Sőt megfelelő programozó tudással láthatatlan folyamatok készítése is könnyen lehetséges. Ennek ellenére sokszor láthatóak ezek, és vannak igen jellegzetes nevűek, ahol könnyen következtethetünk konkrét kártevőre.



Az alaposabb nyomozásban jó szolgálatot tehet az ESET SysInspector modulja, amely pontosan ezekről a futó programokról, futó folyamatokról képes igen árnyalt képet mutatni, veszélyes komponensekre figyelmeztetni.



Remélhetőleg a részletes útmutatóval **segítettünk valamit abban**, hogy a szebb jövőben majd némileg kedvezőbb, **zombimentesebb pozícióban találhassuk** Magyarországot.

 Tetszik  26 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [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/1941835>

Kommentek:

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



[szavazzfasszal](http://szavazzfasszal.blog.hu) • <http://szavazzfasszal.blog.hu> 2010.04.22. 14:18:00

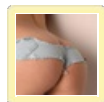
Na asszem én pl zombi vagyok.



[Hümüzhümümüz](#) 2010.04.22. 14:21:11

Nálam egyik tünet sincs. Avast, Ad-Aware és Defender fut a gépeimen.

Viszont kimaradt a szórásból, hogy fél évente telepítsük újra magát az op. rendszert. Na jó, legalább évente! :) Van egy haverom, akinek 5 éves (!!!) gépén a vásárláskor telepített XP fut. :D 3-4 perc alatt bootol be neki és állandóan kékhalál. :P



[pillantás](http://www.eloszto.hu/) • <http://www.eloszto.hu/> 2010.04.22. 14:21:46

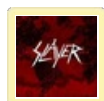
Én még nem vagyok :)

[Piréz Vitéz](#) 2010.04.22. 14:26:13

kva blogmotor... na nem írom újra az egész

"A barátok, családtagok, ismerősök azt jelzik, leveleket, üzeneteket kaptak tőlünk, pedig mi nem is küldtünk nekik semmit."

Ne terjesszük már a hülyeséget. Spammerek előszeretettel használnak valós címeket küldéshez, lehetőleg olyat, amit ugyanonnan gyűjtöttek, mint a címzettet. Pl. levlistáról kipécéznék egy címet, a többi levlista tagnak meg a nevében küldik a szemetet. A sok barom meg óbégat, hogy tegyen már fel egy víruskeresőt, mert jaj megfertőzi őket is.



[MajdnemAraya](http://ubuntuwallpapers.blog.hu) • <http://ubuntuwallpapers.blog.hu> 2010.04.22. 14:26:47

Nekem meg Ubuntu fut a gépemen...

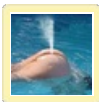


[Lord_M_](#) 2010.04.22. 14:37:22

[@MajdnemAraya](#): Nekem meg Commodore Basic V3.5 65535K Bytes free...

READY.

[]



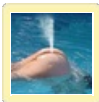
[□sirparaszt scene/buckalakó tahó/fotelrokker 2010.04.22. 14:37:29](#)

@Piréz Vitéz: Pontosan.

Már 5 éve is ezért hisztizt sok jól képzett ismerős, pedig akkor Mac-ról neteztem.

[Flaggx 2010.04.22. 14:39:39](#)

Én zombi vagyok... de megnyugodtam, legalább a gépem nem az.:)



[Zsirparaszt scene/buckalakó tahó/fotelrokker 2010.04.22. 14:41:52](#)

Most látom a bannert.

Respect a Wizard of Wor-ért! :)



[Lord_M_ 2010.04.22. 14:44:51](#)

```
10 CLRSCN
15 SCREEN 9
20 BOX(0,0)-(320,240),1
30 LOCATE(1,1)
40 PRINT "BONGESZO"
50 LOCATE(2,1)
60 INPUT "ADJA MEG A KERESETT CIMET:","A$
70 IF A$="" THEN GOTO 50
80 OPENURL (A$) FOR INPUT AS 1
90 B=LOF(1)
100 C$=SPACE(B)
110 GET #1,,C$
120 PRINT C$
130 CLOSE
140 END
```



[eloszto • http://eloszto.hu 2010.04.22. 14:51:26](#)

A merevlemez állandó kerregése is ilyen jel lehet.



[Lord_M_ 2010.04.22. 15:01:34](#)

Az a baj amúgy, hogy még hozzáértőként is nehéz időnként ilyeneket felfedezni a csodálatos windows vista és 7 esetében. Szerencsétlen XP elzörgött 14 rendszerfolyamat mellett is, de 19-nél már minden stabilan működött. Ez egy új win7 esetében is 30 körüli / feletti feladatot mutat a feladatlistában, és akkor ugye a services.msc-t még nem is néztem ... Egy hétköznapi felhasználónak meg még több gondja van ezzel. Mit lát ő a feladatlistában... scvhost-ból hatot... és már nem is tudja hogy mit keres...

Arról meg ahogy a cikk is írja, a Windows is tehet, hogy időnként a rendszer belassul, vagy éppen ő dolgozik a háttérben...

HDD kerregés: okozhatja a fájlok töredezettsége is, meg a telítettség is... a memória totális használata...

Nem tudunk igazán behatárolható jelenséget adni a felhasználók kezébe amivel megérti hogy most éppen nem ő uralkodik.

Mondjuk az segíthet, ha valamely addig használt rendszerfunkció egyszer csak "a rendszergazda letiltotta" üzenettel tagadja meg a használatot, pl dátum idő, feladatkezelő... különösen ha addig éppenséggel mi magunk voltunk a rendszergazdák...

A hozzáértők írják a kártékony programot(is), a nem hozzáértőktől meg elvárjuk hogy tudjanak védekezni és / vagy ismerjék fel a problémát...

[Orbán a magyar nép ópiuma! 2010.04.22. 15:07:45](#)

Nagy dolog, az ország 2/3-a zombi.

shred 2010.04.22. 15:08:14

Ettől nem lettem okosabb... marad a gyakori vírusellenőrzés és a ház rendszeres porszívózása.

Skatulya bácsi megmondta 2010.04.22. 15:09:56

Rambo nagy C64 rajongó! Talán neki van/volt nagy C64 proggyűjteménye is!

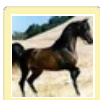


Miliko Enoki 2010.04.22. 15:26:10

Hát én nem vagyok zombi, de a gépem az.

Két nappal ezelőtt-munkámból kifolyólag- bejelentkeztem azon a bizonyos "ügyfélkapun"... láss csodát, hát nem beengedtem a Trójait!!!

Csak azt nem értem akkor minek ez a sok sz@r vírusirtó, meg védekezés, szerintem legközelebb gumióvszert használok:(



ColT • <http://kilatasgaleria.blog.hu/> 2010.04.22. 15:33:04

Hát, ezért nem kell winnyózt használni, ha nem muszáj.

Linux-szal nehezebb zombivá lenni :)



PizkosFreddy 2010.04.22. 15:54:37

Vitaminy jó ezellen...???

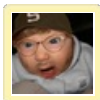
guszt 2010.04.22. 16:05:00

Kimaradt, hogy érdemes letiltani az autorun-t a mobil drive-okon. TweakUi install letölt (genuine windozzal az ms-ről, warezzal valahonnan máshonnan, vagy havertól), felrak, autorun funkció letilt. Az egész művelet sor 1 percen belül végigjátszható, és nagyon hasznos, szerintem a windozos gépek elég jelentős hányada fertőződik meg így, egy kisebb munkahelyi géppark is simán azonnal visszafertőződik a pendrive-okról, mire végigér a gazdi az összes gépen, kezdheti újra az egészet.

Ezzel együtt az is egyértelműen gyanús jel, ha a pendrive-on van egy autorun.inf - azt érdemes azonnal shift+del-lel lezúzni. (Rejtett file, át kell állítani az intézőt/totalcommandert, hogy azokat is mutassa.) Akkor van gáz, ha ez a file nem volt rajta, mielőtt a te gépedben járt, vagyis ott került rá. Ekkor azonban már könnyen lehet hogy nem tudod felrakni a TweakUi-t sem.

guszt 2010.04.22. 16:13:32

Ja igen, az oktalannak tűnő hosszas HDD aktivitás egy mai gépen simán lehet normális, 4 giga ramot kikesselni nem pár másodperc, szóval ha nyitva van jópár dolog - a gép még bőven bírja, azért van annyi ram meg akkora proci benne - és elkezd a háttérben rendezkedni a rendszer, az hosszú percekig tekerheti a winsit, anélkül, hogy épp frissítést töltené le, vagy egyáltalán rá lenne dugva a netre.



szamojéd szomszéd 2010.04.22. 16:25:14

Nálam 10ből egyik sem. Viszont ha kikapcsolom a pc-t (XP SP3-mal) és a modemem (scientific atlanta) nem áramtalanítom utána, akkor érdekes módon pár perc múlva újraindul a gépem.

A modem áramtalanítása esetén ez nem történik meg.

Erre valaki tud mondani valamit?? Kösz!



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.04.22. 16:43:33

[@Piréz Vitéz](#): Szia!

Teljesen igazad van ha csak az emailt vesszük. Pontosan emiatt nem érdemes figyelmeztetni a feladót, hiszen fiktív, és BÁRMI lehet odaírva.

Én inkább az akármilyen üzenetekre gondoltam, pl. MSN, a Skype-on is lehet naponta botoktól orosz szexoldalas üzeneteket kapni, és pont tegnap gyalogolt bele egy ismerős valamilyen Facebook nyavalyába, és elkezdte ontani az ismerősöknek az automata angol nyelvű üzeneteket.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.04.22. 16:44:59

[@Lord_M](#): Hehe, azt tudod hogy voltak vírusok C64-en is? Még vírusirtó is volt a kezem között, például a BHP (Bayerische Hacker Post) Viruskiller :-D



norbert79 • <http://norbert79.deviantart.com> 2010.04.22. 16:45:24

[@Lord_M](#): Nem oda Buda! C64:
**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM 38911 BASIC BYTES FREE

READY.
[]

Commodore Plus-4 esetén pedig:
COMMODORE BASIC V3.5 60671 BYTES FREE
3-PLUS-1 ON KEY F1

READY.
[]

Szóval a tied vagy egy cartidge-os gép volt, vagy valami saját hack :)

Drótmalac • <http://blob.blog.hu> 2010.04.22. 16:46:13

[@szamojéd szomszéd](#):
tiltsd le a BIOS-ban a a Wake Up on Lan-t.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.04.22. 16:46:41

[@Zsirparaszt scene/buckalakó tahó/fotelrokker](#): Szia!

Hát ja, eredetileg hangmérnök akartam lenni, de aztán bejött a stúdióba 81-ben a Kóbor, hóna alatt egy Londonból frissen hozott ZX81-gyel, és akkor minden megváltozott :-)



norbert79 • <http://norbert79.deviantart.com> 2010.04.22. 16:46:42

[@Csizmazia István \[Rambo\]](#): Pontosabban csak önmagát másolni képes vírus, pusztítani tudtommal nem tudott. A 1541-es kódjába írta be magát, olyan track illetve sector eléréseket művelt ami miatt nem lehetett csak úgy leírtani, de elpusztítható volt, s kevesebb fejfájással járt, mint egy későbbi CIH vírus.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.04.22. 16:48:27

[@Lord_M](#): Köszí ezt jó kis kommentet, ez a mondatod überkirály módon összefoglalja a lényegét:

"A hozzáértők írják a kártékony programot(is), a nem hozzáértőktől meg elvárjuk hogy tudjanak védekezni és / vagy ismerjék fel a problémát"



**Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.22. 16:50:11**

@Skatulya bácsi megmondta: Hát igen, a jó öreg C64, brühühü. Amúgy a www.commodore64.hu gyűjtemény régen tényleg megvolt, de ma már csak emlék... Emulátor azér néha még beficcen.



**norbert79 • <http://norbert79.deviantart.com> 2010.04.22.
16:50:13**

@Csizmazia István [Rambo]: És mikre nem lel az ember!

noname.c64.org/csdb/release/?id=49101



**Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.22. 16:54:38**

@Miliko Enoki: 100 %-os védelem nincs, pl. betörés biztos (megfizethető) zár sincs, ha ilyet veszél, akkor lukat fúrok a tetőn. Szóval minden megkerülhető, de azért érdemes védekezni. A helyzet romlásához az is nagyban hozzájárult, hogy profik fejlesztik a kártevők jó részét a kiemelkedő haszon, kémkedés reményében pl. RBN, Kína, stb.



**Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.22. 16:59:58**

@ColT: Ha nem vagy kötve a Windows világhoz (Autocad, SAP, Macromedia, játékok, stb.) akkor egy magán embernek jó választás lehet egy Linux, és a kártevő fronton is sokkal jobb a helyzet. De nem 100% ott sem, jó tűzfal ott sem árt, chkrootkit, rkhunter, ismeretlen programok telepítése ott is veszély forrás, tudatlanul (PEBKAC) trójai kodeket ott is le lehet tölteni. A fő gépem nekem is Linux, akkor váltok Windowsra, ha a kártevőket akarom bizgetni :-)



**Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.22. 17:02:38**

@guszt: Az igazi megoldás inkább az lett volna, hogy maga a Microsoft tiltja már le évekkal ezelőtt az összes verzióban az Autorunt. De akkor sérült volna "a felhasználói élmény" és azt nem akarták. Évekig ment ugyanez a szívás a makróvírusoknál is, míg nagy kegyesen lépni méltóztattak.



szamojéd szomszéd 2010.04.22. 17:07:22

@Drótmalac: Kösz, megpróbálom!



**Gépember • <http://gepembernaploja.blog.hu/> 2010.04.22.
17:41:48**

Csak egy kis segítség, hogy a megnyitott feladatkezelőben tudd, hogy melyik folyamat mit jelent:

gepembernaploja.blog.hu/2010/04/07/mi_fut_a_gepemen_startup_info



**anyádbogár • <http://www.apadhuzzonafaszara.com>
2010.04.22. 17:46:46**

én meg asszem a zombieland-ből van a cikk végén a kép :-)



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.22. 17:56:48

@anyádbogár: Meg az elején is, Woody Harrelson bácsi arat :-D

kvadrillio 2010.04.22. 19:12:22

Mindenki tudja, hogy tele vagyunk kártevőkkel, állandóan beteszik a kárjukat mindenhova , ahova lehet.
Írtani kell őket rendületlenül ! :O)



anyádbogár • <http://www.apadhuzzonafaszara.com>
2010.04.22. 19:34:56

@Csizmazia István [Rambo]: pedig tényleg... csak a pontokra reflektáltam, így a kezdőkép kimaradt.

totálendi 2010.04.22. 19:58:26

Ha lekurvaanyázod újságíróként az olvasóidat, akkor zombi vagy:
altmyil.nolblog.hu/archives/2010/04/22/Anyaznak_az_indexesek/

gusztí 2010.04.22. 20:39:39

@Csizmazia István [Rambo]:

Igen, én is kezdtem konteókat gyártani, miért jó ez a picipuhának, de továbbra sem értem hol sérülne a felhasználói élmény, ha az usb drive-ok autorunját letiltanák egy soron következő biztonsági frissítésben. Merthogy külön le lehet tiltani ezt, és külön az optikákat, és lemezt egyrészt jóval kevesebbet használunk, azok is főleg installok, vagy gyári programok, ott akár maradhat is az autorun a felhasználói élmény érdekében. Viszont pendrive-ról soha semminek nem kell elindulni automatikusan, az nem arra való. (Ilyenolyan lejátszókhöz meg van driver, ami felismeri hogy rádugtad, és elindítja amit kell.)



enpera 2010.04.22. 20:42:27

Én tuti nem vagyok zombi, linuxom van :D
Amúgy hasznos kis írás :)



Gépember • <http://gepembernaploja.blog.hu/> 2010.04.22.
21:05:13

@gusztí:

Az 1.0-ás felhasználók 90%-a kétségbeesetten reklamál, ha letiltom náluk az USB-s autorun funkciót.

Magyarázhatom, hogy ez mennyire káros, rossz, vagy veszélyes, ő ezt megszokta...

Talán ezért.

Nick@Day 2010.04.22. 21:13:21

Ubuntu, Linux, RedHat, Fedora, SuSe, stb. mint nyílt forráskódú cuccok, ha igazán hű botokat akarsz, ezeket keresed, mert a sok hozzáértő észre sem veszi, hogy DoS-okban vesz részt egész nap...

Tordapeti (törölt) 2010.04.22. 22:10:56

@szamojéd szomszéd: A drótmalac javasolta megoldás helyes. Csakhogy. Egy rendes BIOS-ban a Wake up on line default

értéke disable, kérdés tehát, miért lehet egyáltalán aktív nálad?

A BIOS-beállítás egyetlen lehetséges helyes útja: Vissza az egészet a gyári default-ra, (Load BIOS Setup Default) és CSAK AZON (!) az értéken változtatni, amin feltétlenül szükséges. (Sokszorosan ellenőrizve és meggondolva!)

Tartani lehet tőle, hogy ez nálad nem egészen így történt....



twollah / bRoKE n hOPe, sUppLeX •

**<http://freewaresoftwarenews.blogspot.com/> 2010.04.22.
22:18:06**

Nem bizok a virusirtokban.

Van egy Spybot Search and Destroyom es kész.



Mitya Ivanov 2010.04.22. 22:19:38

ha az egérmutatóm jobbra balra, fel-le mozog, miközben hozzá sem nyúlok, akkor zombie vagyok?

Enahma • <http://csodaidok.hu> 2010.04.22. 22:30:57

@Nick@Day: "Ubuntu, Linux, RedHat, Fedora, SuSe" - he? Az Ubuntu, a RedHat, a Fedora és a SuSE nem kerülhetnek a Linuxszal egy felsorolásba, mivel maguk mind Linux-disztribúciók.

Martian (törölt) 2010.04.22. 23:54:40

@Gépember: Meséld el nekik, hogy az is macerás, ha állandóan nyitni-csukni kell a lakásuk bejárati ajtaját... pedig mekkora "felhasználói élmény", ha tárva-nyitva tartják.
:)))



Dr. A Jó Meglepően Izmos Hercege 2010.04.23. 09:25:07

@eloszto:

Az akár a kevés ram mutatója is lehet, mert a pagefilet kergeti folyton.



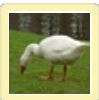
**Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.23. 11:32:50**

@Gépember: Szerintem az, aki már le tudja tiltani az autorunt, az többnyire azt is észreveszi, ha a gépével van valami guzmi. A nagy veszélyben a többi 90% 1.0 juzer van, akikről te is beszélsz. Érdek a világ ura. Megéri olyanra gyártani, ami kényelmes és sok pénzt hoz; és nem éri meg biztonságosabbra állítani.



**Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.23. 11:34:26**

@Mitya Ivanov: Hát lehet, hogy munkahelyi rendszergazda éppen VLC-vel távirányítja a gépedet. Ha nem ez a pálya, akkor valóban nem jó ömen.



Mitya Ivanov 2010.04.23. 15:50:24

@Csizmazia István [Rambo]: itthoni gépről van szó.
avastom van, mit ajánlasz mellé vagy helyette?
kösz

Nyuszika7H 2010.04.24. 10:36:27

[@Csizmazia István \[Rambo\]](#): A VLC egy médialejátszó. Nem VNC-t akartál írni véletlenül? :)

Nyuszika7H 2010.04.24. 10:54:48

[@Mitya Ivanov](#): Nem feltétlenül vírus, lehet más is. Milyen egered van?

Ha golyós, akkor ne várj csodát, állítólag ha ránézel, már attól megmozdul. :)

Ha optikai, akkor Vezérlőpult -> Egér -> Hardver fül – innen válaszd ki az egeredet, majd kattints a Tulajdonságok-ra. Itt valamelyik fülön találsz egy olyan négyzetet, hogy Gyors inicializálás. Ha ki van pipálva, akkor vedd ki a pipát. Ilyenkor lehet, hogy kicsit lassabban fog bootolni a Windows, de nem vészes.

Ha lézeres, akkor esetleg megpróbálhatod, amit az optikaira írtam, de nálam nincs ilyen opció. Lehet, hogy csak azért, mert a Microsoft úgy gondolta, hogy kiveszi ezt a Windows 7-ből. Még az is lehet, hogy lézeresnél ilyen probléma nincs, és ezért nincs ilyen opció.

Ha ez nem segít, vagy nincs kipipálva, akkor sajnos valószínűleg vírus lehet.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.24. 13:08:35

[@Nyuszika7H](#): Mea Maxima Culpa, de igen, VNC és társai.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.04.24. 13:19:49

[@Mitya Ivanov](#): Én mindenkinek jó szívvel ajánlom bármilyen vírusirtó vagy internet security csomag mellé a Spyware Terminatort és az a-squared-et. Ha már volt ilyen lakásajtó hasonlat, plusz egy zár sosem árt vagy egy trükkös gyújtás kapcsoló a verdába.

Google bot átkampózás

2010.04.26. 16:30 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [google linkek bot kártékony ellenőrzése](#)

A kártékony kódokat terjesztő weboldalak **igyekeznek furmányosan elrejtőzni a Google kártékony linkeket feltérképező szolgáltatása elől.**



Két buddhista szerzetes az aranyhalak életét figyelte.

- Nézd milyen vidámak a halak - mondta az első.

- Honnan tudod, te aki nem vagy hal, hogy mit gondolnak a halak? - kérdezte a második.

- Honnan tudod te, aki nem vagy én, hogy tudhatom-e, mit gondolnak a halak - válaszolta az első.



Azért ennél lényegesen egyszerűbb dolga van a bűnözőknek, hogy tudják, mit gondol egy bot, vagy honnan jön, hiszen egy adott, beazonosítható IP tartományból érkezik. [Megoldják okosba, és gondoskodnak arról](#), hogy ne sikerüljön neki a kártévös weboldal beazonosítása, és ilyenkor mást mutassanak kifele. **Nem új a módszer, de [a jelzések szerint egyre szélesebb körben használatossá](#) válik.**



Mikor is tört ki a vulkán? Március 21-én. **És mikor foglalta le valaki Amerikából a domaint?** Igen, másnap. **Meghalhat valaki úgy, hogy aztán végül életben marad?** [Semmi akadály, de előtte még szerepel néhány átpofozott linkben.](#) A Google [keresőtálatatok trend alapján kártévőkkel való mérgezése](#) már annyira bevett szokás, hogy [lassan nem is érdemes külön posztot írni róla.](#)



[Bejelentett támadó webhely adatbázis.](#) Amit ember az egyik oldalon megalkotott és kitalált az ellenőrzésre, azt **egy másik ember a sötét oldalon szépen ki tudja játszani, majd mikor újra pontosítanak ellenőrzésen**, akkor a támadók, ... és ez így megy. **Tisztára mint a rakéta elhárító rendszereket elhárító rakéta elhárító rendszerek.**



Szóval nem lehet minden link mellé egy közlekedési rendőrt állítani, míg a bejelentett **támadó webhelyek feketelistája sosem lehet elég friss és naprakész**, és ezenközben pedig folyik a szüntelen küzdés az internet sötét bugyaiban. Marad hát az egyetlen bombabiztos, de pofon egyszerű autentikus módszer (a ne fűrgyé le mintájára): "Ne kattinsá!"

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/1952691>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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](#) 2010.04.26. 21:19:04

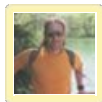
Hát ez az!

És ha letiltod a scriptet ad-block és stb biztonság, akkor pont azt látod amit a weboldal szerkesztője a txt fájlban. :-)

Néha azon veszem észre magam, hogy nem tudom mit nézek, mert már nem is úgy néz ki, mint valaki mesélte és egyébként a hivatkozásokat csak másolom és ez annyira kényelmes!

Valami nagyon elromlott.

Múltkor észrevételeztem, hogy alap Joomla! oldalaknál, már a regisztrációt követő megerősítő e-mail is csak a felhasználónak kihívás a botok simán abszolválják ezt az akadályt.



[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu> 2010.04.27. 12:44:38

Szerintem hosszú távon a Google kártékony oldalak felismerése nem fogja bírni ezt a versenyt, és így megmarad a feladat a vírusirtónak, aki aztán vagy lekezeli, felismeri vagy nem.

[nyos](#) 2010.04.27. 18:12:16

Esetleg új, toluken független IP címeket is fog használni erre a célra. (mondjuk más user agenttel)

Amúgy a cloaking régi technika, jopar eve a BMW oldal is tiltotta emiatt a gugli. Most ugyanezt a black hat technikát alkalmazzák black hat emberek, hasonló célra.

Nem tartom valószínűtlennek, hogy a Google, a Mozilla és a víruskereső cégek csinálnak majd egy nagy, közös listát. Aztán akit lebuktatnak, az felkerül rá.

Céges spam, mert megérdemled!

2010.04.28. 12:35 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [spam törvény](#) [céges eladó](#) [kéretlen címjegyzék](#) [emailcím](#)

[Vajon jó-e a magyar spamtörvény?](#) Teheti fel a költői vagy valódi kérdést az, aki elér az olvasásban a "törvényes cégneves spam" fejezethez. De persze lamentálhatunk azon is, hogy akár jó, akár rossz, [betartják-e azt a szereplők egyáltalán](#), és ha igen, akkor miért nem.



Persze az is kérdés lehet, hogy [ez a bizonyos törvény](#), amely a Spamwikiből idézve: "2009. március 1-én hatályba lépett 2008. évi XLVIII. törvény (a továbbiakban: Grt.) módosítása alapján egyértelműen céges levélcímekre (például a [info@cegnev.hu](#) címre) előzetes engedély nélkül is küldhető reklám, de azt kérésre többé nem szabad megismételni. Ez a vállalati opt-out rendszer, mely **gyakorlatilag megteremtette** Magyarországon a törvényes spam típusát. " jól szolgálja-e az érdekeinket.



Nyilván a törvényalkotók sem úgy képzelték a szebb jövőt, hogy [a korábbi Nagy Sándorok \(Alexander the Great\) helyett és után](#) ilyen újabb fajta kéretlen címjegyzék árusok irkálnak majd az embereknek, és kéretlen levélben házalva árusítják céges címjegyzéküket, kicsit a ["Diplomáciai védettség" jellegű somolygással orcájukon](#).



Mel Gibson azért **akkor és ott megoldotta azt a helyzetet**, amelynek felidézése most is bizsergetően jó érzéssel többek agyában ismét előbukkanhat ;-)



Elmélyült fejbakarás közben emellett az is felmerülhet, vajon a "rambosoft@" előtag az **mennyire felel meg az "egyértelműen céges levélcímekre előzetes engedély nélkül is küldhető reklám" kitételnek**.



Ezekután **immáron egyetlen cégnek sem javasoljuk, hogy spamelkerülés céljából mostantól furmányosan ramboisoft@-ra változtassák** a korábbi info@ vagy office@ címüket, hiszen jól láthatóan ez sem segít ;-)



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

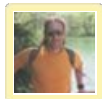
<http://antivirus.blog.hu/api/trackback/id/1958408>

Kommentek:

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

Giraffe 2010.04.28. 14:30:14

Meg Gibson akkor és ott éppen nagyon agonizált. A problémát Danny Glover oldotta meg (Pillanatnyilag felfüggesztve!).



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.04.28. 18:47:49**

Szia Giraffe!

Igazad van, most hogy mondod. Nagyon rég láttam már, de valami hajófenékben történt lövöldözés rémlik. De az útlevél lobogtatás szerintem mindenkinek egy emlékezetes momentum volt, gondolom a parlamenti mentelmi jog kapcsán is felidéződik néhanap :-)

Giraffe 2010.04.29. 10:05:21

:D És hányszor reagálnánk a legszívesebben Martaugh őrmesterhez hasonlóan ;)

Lehet más a hackelés

2010.04.30. 13:25 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [konferencia](#) [hacking 2010](#) [netacademia](#) [ethical](#)

Harmadik alkalommal gyűltek össze az Aréna Plazában az Ethical Hacking konferencia keretében az informatikai biztonsággal foglalkozó szakemberek. Mindenféle bevezető hosszú méltatás, sallangos felvezetés nélkül rögtön a lecsóba, illetve bitekbe csaptak az előadók, és talán a legsikerültebb szakmai napot sikerült így tegnap összehozniuk.



Hogy a [hackerekre, etikus hackerekre igenis szükség van](#), azt aki ezt a témát, közeget, a problémákat, szereplőket ismeri, nem is vitathatja. A program házigazdája most is [Fóti Marcell \(NetAcademia\)](#) volt, aki [gyorsan megmutatta a napirendet](#), és már indult is a konferencia.



Elsőként [Illés Márton és Gyöngyösi Péter \(Balabit\)](#) léptek a dobogóra, és az XSS témán csavartak egyet: előadásukból kiderült, milyen egyszerűen lehet jelszavakat kijuttatni egy sebezhető webalkalmazás segítségével.



[Zsíros Péter \(NetAcademia\)](#) tavalyi előadásának folytatásaként annak előzményét mutatta be. Lényegében azt járta körül, hogyan is találhatjuk meg fűzerek segítségével azt a bizonyos biztonsági sebezhetőséget, amelyre aztán tetszőleges kódot futtató exploit készíthető.





Barta Csaba (Deloitte) egy olyan rootkit változatot futtatott, amely a memória területen tudta észrevétlenül megváltoztatni, kitörölni bármely felhasználó, akár az admin jelszavát is.



Kovács László (ZMNE) a tavalyi Hacktivits előadásához (az infrastruktúra védelme) kapcsolódóan azt mutatta be, milyen óriási változáson ment keresztül a katonák felszerelése az elektronikai forradalom következtében, és mennyiben realitás az egyes országokban a hackerek szerepe a hadviselésben.



Kocsis Tamás (Biztributor) és **Dnet (Silent Signal)** a WiFi gyengeségéről beszéltek. Nyilvánvaló, hogy létezhet erős wifi is, amelynek feltétele az erős titkosítás mellett a megfelelő hitelesítés szükségessége. Váratlan buktatókat is bemutatnak, például egy access point eltulajdonítása egy célhelyszínről, és annak soroskábelén keresztüli villatása is meglepő eredményeket hozhat.





[Ezután következett Balássy György \(BME\)](#), aki ugyan a tízéves ASP.NET rendszer erősségeiről-gyengeségeiről beszélt, de mondanivalója bármely nyelven dolgozó webfejlesztőnek hasznos lehetett, hiszen az alapértelmezett beállítások, a nem megfelelő input ellenőrzés, a formokban csak rejtetten szereplő checkboxok ontják a gyenge pontokat.



[Kabai András \(PTA CERT-Hungary\)](#) egy olyan Egg Hunternek nevezett technikát mutatott be, amelynek segítségével a sebezhetőséget kihasználó támadókód memóriában való könnyű megtalálását, illetve annak finomhangolását lehet elvégezni.



[A szakmai előadások közül utolsónak Buherátor \(Silent Signal, Buhera.blog\)](#) lépett a színpadra, és a patch-alapú sebezhetőség-analízis, hibakeresés újszerű módját vázolta fel. Felhívta a figyelmet arra, hogy ezzel a technikával minden valószínűség szerint a bűnözők is igyekeznek majd a frissítések által érintett sebezhetőségekre nyomon követni, tehát nem szabad sokáig halasztgatni a már kibocsátott javítófoltok futtatását.





Zárásképpen a nyeremények sorsolása zajlott, és arról is [kaptunk jó híreket, milyen neves vendégeket - például Bruce Schneiert - üdvözölhetünk majd az őszi Hacktivity konferencián.](#)

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

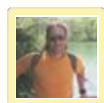
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Safe mód a Mechagodzilla ellen](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1964020>

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>
2010.04.30. 13:35:52**

Ezúton is elnézést a gyenge minőségű fotók miatt, majd valamikor fontolóra veszem egy jobb gép beszerzését ;-)

[spggg](#) • <http://www.zughekker.info> 2010.05.02. 17:56:48

Biztos érdekes volt! Jövőre már én is mehetek. :D

Ja, és a weboldal is új lett

2010.05.03. 09:47 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [remote program új weblap administrator 4.2 verziók](#)

Új funkciókkal felruházott, nagyobb teljesítményű verziókat adott ki a NOD32 Antivirus rendszerből és az ESET Smart Security biztonsági programcsomagból az ESET. A cég emellett megújította a vállalati felhasználók számára kidolgozott ESET Remote Administrator távadminisztrációs alkalmazást is.



A vállalatok számára központosított karantén kezelést, míg az otthoni felhasználóknak még gyorsabb víruskeresést és még hatékonyabb böngészés közbeni védelmet kínál az ESET NOD32 Antivirus új, 4.2-es verziója.



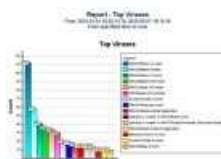
A vírusirtó nagy testvéreként számon tartott, a vírusvédelem mellett tűzfalat és levélszemétszűrőt is tartalmazó ESET Smart Security 4.2-es verziója mindezen kívül továbbfejlesztett tűzfalas védelmet nyújt a vezeték nélküli hálózatokban, vállalati környezetben pedig képes a megbízható hálózatok azonosítására, valamint az ezekhez tartozó tűzfalprofilok kezelésére.



A vállalatok számára a két új programverzió mellett fontos, hogy megújult az ESET Remote Administrator alkalmazás is. Az új, 4-es verzió a már eddig megismert távmenedzsment és monitorozási funkciók mellett támogatja a központosított karantén menedzsmentet, valamint megkönnyíti a kliensek csoportosított kezelését és Active Directory szinkronizációját.



A szoftver emellett lehetővé teszi a platform független távadminisztrációt, így az ESET Remote Administrator új verziójával menedzselhetőek az ESET hamarosan megjelenő OS X és Linux alapú szerver- és kliensvédelmi megoldásai.



A most bejelentett új termékverziókra az érvényes licenccel rendelkező felhasználók díjmentesen térhetnek át. A termékek mellett ugyanakkor [megújult az ESET magyarországi honlapja is](#).



Az új weboldalon mind az otthoni, mind a vállalati felhasználók több információhoz juthatnak hozzá. Így például [nemzetközi víruslaboratóriumok független teszteredményei alapján összehasonlíthatják a vírusirtó rendszerek teljesítményét](#), illetve esettanulmányokon keresztül is megismerhetik az ESET szoftvereinek működését.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- ["Szösölmédia" és nyaralás](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1967990>

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 2010.05.03. 12:52:47](#)

Gratula! Nagyon tetszik a nyomozás!

Víruslaborban jártunk

2010.05.06. 16:00 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [kirándulás](#) [iroda](#) [pozsony](#) [eset](#) [víruslabor](#)

A hét elején kis kiránduláson vettünk részt, meghívást kaptunk **Pozsonyba, az ESET otthonába**. Az új székházban ma már többszázan dolgoznak a cég kötelékében. A különféle médiáktól érkezett újságírók még a víruslaborba is bekukucsálhattak.



[A magyarországi képviselet](#) szervezésében tettünk látogatást a NOD32 és a Smart Security [programokat fejlesztő vállalatnál](#). Sok érdekes mozzanata volt az útnak, [a várható új Macintosh és Linux termékek fejlesztéséről éppúgy szó esett az előadásokon](#), mint a kártevők napi hatalmas számáról, a folyamatosan változó új kihívásokról.



Juraj Malcho víruslaborvezető előadásában átfogó képet kaptunk a legújabb kártevő trendekről. Ebből a legérdekesebb momentum a McAfee hibás frissítésével volt kapcsolatos. Mint ismeretes, április 21-én egy olyan vírusadatbázis került kiadásra, amely [a Windows egyik rendszerállományt tévesen kártevőnek](#) ítélte. Eddig nincs is ebben semmi rendkívüli, sajnos ritkán ugyan, de [minden antivírus céggel megesett már ilyen](#) malőr. Viszont **ami az esetet különlegessé tette az az volt, hogy másnap ha valaki begépelte a mcafee hibás frissítés és hasonló szavakat, körülbelül a Google találatok 50-60 százaléka** már a bűnözők által fertőzött linkekre mutatott a találatok célirányos mérgezése miatt. És aki a frissítés miatt bajban volt, kikapcsolt víruskeresővel könnyen beleszaladhatott egy új fertőzésbe.



A másik érdekes momentum az volt, hogy eddig ritka és nagyon Buzgó Mócsing, Fülíg Jimmy szerű bikkfanyelvű magyar adathalász próbálkozások voltak csak, amik valószínűleg azért voltak magyartalanok, és hemzsegték a helyesírási hibáktól, **mert eddig mindig valamilyen nyersfordító programmal készültek**. Ami viszont meglepő volt, és ezen mi is csodálkoztunk, a hamis antivírusok nyomában megjelent [hamis szerzői jogi programból](#) már jelent meg tökéletes szlovák nyelvű változat.



Kaptunk egy kis ízelítőt a mobil antivírusok fejlesztési terveikből is, ebből kiderült, **hamarosan lesz Symbian és Windows Mobile okostelefonra tűzfalas security csomag is**. Szó esett arról is, hogy titkon mindenki az iPhone valamint Android platformok további térnyerésére számít, ami további fejlesztéseket indíthat el.



Végül **bejártuk az egész irodát Miroslav Trnka kalauzolásával, beleértve a víruslabort is**, ahol James Bondos monitorokon látszott, amint a nemzetközi helyzet éppen fokozódik ;-)



Körülbelül **napi kétszáz ezer új minta érkezik elemzésre**, ami bőszegesen ad munkát mind az automata feldolgozó programoknak, mind pedig a képzett kódélemzőknek.





Külön falat foglalnak el a program által elnyert díjak, köztük az olyan értékes trófeák, mint a Virus Bulletin 100% Award, vagy az AV-Comparatives oklevelek. A kirándulás végén pedig az újságíróknak lehetőségük volt az ebéd során **kérdéseket feltenni, illetve a fejlesztőktől - például Richard Marko vezető szoftverfejlesztőtől - közvetlenül lehetett kérdezni**, kötetlenül beszélgetni.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [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/1977420>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Blame Canada! - Frissítve

2010.05.10. 18:11 | [Csizmazia István \[Rambol\]](#) | [10 komment](#)

Címkék: [spam per kanada péter zsolt vargay](#)

Esetleg adjunk erre a nemes célra kétszáz forintot, de legalább küldjük tovább ismerőseinknek. **Első ránézésre tucat spam és hoax terhes történetek jutottak eszünkbe.** Ám aztán később, jobban megvizsgálva másodikra is ;-)



Harmadikra talán lehet [egy kétségbe esett ember segély kiáltása \(a spam levél PDF formátumban ITT](#) olvasható). De a helyzet azért ennél lényegesen bonyolultabb. Nyilván van egy olyan vetülete is a dolgoknak, hogy [kéretlen levelet nem szeretünk kapni](#), semmilyen **ügyben sem**, akár volt méltánytalanság, akár nem. A levél magyarságával viszont ezúttal nincs baj, **régi bankos adathalász levelekhez viszonyítva nem lelhetőek fel a nyersfordító programok ordító hibái.**



A vicc szerint lopni csak annyit érdemes, hogy ügyvédre is jusson belőle. Vagyis alapból ha valaki a húsos fazék közelében, vagy a politika boszorkány konyháiban vagy a zsiros állami megrendelések közelében szaglássza a zaftos illatokat, átlagfeletti anyagi jólétben leledzik, négy lakása van, **gyűjtsön, tegyen félre szűkös időkre, és ne sikoltozzon itt nekünk, ha aztán egyszer kihúzzák alóla az ezüst tálcát, és megszűnik a kivételezés.** Villamossal kell járnia: a többi hétköznapi emberhez hasonlóan a megszokott Bentley helyett, a kaviáros, pezsgős fényűző terítékek helyett mostantól **a világ egyik leggazdagabb emberéhez kell járnia ebédelni**, igen a McDonaldsba ;-)



*"10 éven keresztül a teljes vírusvédelmi rendszerét én fejlesztettem, de több éven keresztül az általam fejlesztett védelmi rendszerek védték az összes vámhivatalt, vegyi és gyógyszergyárakat, az ország mára egyetlen és óriási acélgyárát, nyomdákat, kórházakat, polgármesteri hivatalokat". Ez különösen érdekes, **jelentkezhetnének ezek a műintézmények, de a azok a vírusvédelmi cégek is, akik őt alkalmazták,** így le lehetne ellenőrizni, ha egyáltalán van mit.*



[Mások is kaptak](#) a levélből, **még szlovák változat is létezik, amelyre a szakértők annyit mondtak**, hogy olyan passzív szerkezetet használnak benne, ami állítólag ritka a mai élőnyelvben. Mindenesetre a magyar, angol és szlovák változaton túl sikerült még [egy finn verzióra is ráakadni](#), sőt [van lengyel átirat](#) is. Még egy országokat átívelő Bikicsunáj szintű rajongói klub is létrejöhet ebből ;-)



A mérlegelés közben folyamatosan [az állítólagosan fejbőlött állítólagos orosz spammer, Alexey Tolstokozhev](#) járt a fejünkben. Mi is volt az? Semmi adat a Googleban, semmi adat a Spamhauson. Ott volt a csupasz blog, amely **szemre ugyan már hónapok óta vezetve volt, bár valójában az arhcívum linkjei nem mutattak sehova**, és a domain foglalás már egyértelműen le is leplezte: az csak pár nappal korábbi volt. Mégis ellenőrzés nélkül rámozdultak az újságok, újabb nigériai magyar törzset, **igazi Maot megszégyenítve.** A terv valószínűleg az volt, hogy **ha már elegenden linkelnek erre az oldalra, akkor hirtelen kitesznek valamilyen kártevőt.** Ez szerencsére a **leplezés miatt elmaradt.**



Most meg itt vannak ugyan ezek a **Google által fellelhető bírósági dokumentumok**, amiknek eredetiségét, valóságtartalmát, hitelességét nem lehet egyértelműen eldönteni. De **legalább a hivatkozott PDF dátuma nem tegnapi**, és [a Virus Total sem mutat ki benne friss PDF exploitot](#), persze lehet, hogy még most reszelik azt a Metasploitban ;-) Mindenesetre szorgalmas embernek kell lennie annak, aki 111 változatot is készít egy dokumentumból.



Ezenfelül az sem világos, **mit lehet kezdeni tegyük fel ötezer jószándékú naív ember felajánlott kétszáz forintjával**. Bár az épp kerek egymillió forint, de attól még ugyanaz a magánszemély áll szemben Kanadával, mint eddig aki nem élt a fellebezési jogával. Talán ennyiért a Bárándy ügyvédi irodában [már fel lehet tenni három kérdést :-\)](#) Ha elővesszük [Pólya György: A gondolkodás iskolája című könyvben szereplő hozzáállást](#), igaz-e, hamis-e, hihető-e, életszerű-e az egyszerre elküldött öt különböző nyelvű hosszú segélykérő levél, kinek a céljait szolgálhatja - nem egyszerű eldönteni, kivéve ha valóban csalásról van szó. Ekkor a sűrű fillér jó fillér szellemében értelmet nyerhet a dolog.



Kicsit zavaros, szerteágazó X aktás lett ez a poszt, és a "Nincsenek válaszok" lett a fő tanulság, persze emellett gyanús jelek vannak bőségesen. **A történet túlságosan körmönfontan hosszadalmas, bonyolult, körülményes**, talán a Bűn az élet Moldova könyvben szerepel, hogy ha valaki sikeresen kéregetni akar a Keletinél, **frappánsan ki kell találni már jó előre a történetet, ami nem is lehet hosszabb két mondatnál**: például ellopták a táskáját, és pénz kell a hazajutáshoz az állítólagos vonatjegyre. **Ennél bonyolultabb sztorit a járókelők különben már végig sem hallgatnak**. Elég hihetőnek kell hangzania, szánalmat keltőnek kell lennie, és ne legyen ijesztő sem.



Ehhez képest ebben a rákos hozzátartozóról, válásról, munkanélküliségről, hajléktalanságról, méltánytalan ítéletről olvashattunk és minden erős érzelmi hatás kiváltására alkalmas eseménysor állatorvosi lóként egyszerre szerepelt, talán egy Cernus doktor jobban kielemmezhetné magát a levelet. A hihetlen és **hiteltelen motívumot erősíti a több különböző pénzintézetnél: CIB, MKB, Volksbank párhuzamosan vezetett számla is**, ha valaki "nagyon szűkölködöm", akkor mi a frászért nyit meg ennyi számlát?



Szóval eléggé büzlik a történet így, de ha van is valóságalapja, akkor **sem sok sanszot adnánk rá, hogy talál olyan országot, aki egy ilyen gyerektartási ügy miatt egyáltalán komolyan elgondolkodna Kanada beperlésén**. Igaz, történhetnek meglepő és nem várt események, gondoljunk csak [most a MÁV ellen indított keresetre](#), vagy hogy [Magyarország hadüzenetet küldött 1941-ben az USA-nak](#). Vagyis nincs olyan abszurd, ami esetleg a nagybetűs ÉLET-ben mégse történne meg csak amiatt, hogy kevésbé valószínű. Ennek ellenére semekkora összeggel nem fogadnánk az ügy sikerére, és a **magunk részéről nem teszünk bele kétszáz forintot sem, bár egyébként néha szoktunk adakozni**, és jó ügyeket támogatni. Valahogy annyira abszurdnak tűnt a szituáció, hogy a [South Park Bigger, longer, uncut mozifilm változata](#) azon nyomban felidéződött [a Blame Canada! dallal :-\)](#) Mindenesetre aki szeret olvasgatni trükkökről, spamekről, [bátran ajánljuk a Legendavadászat](#) vagy a [Hogyan lopjunk kontinenst című könyveket](#). Nincs lehetetlenség, csak tehetetlenség - ismételte nekünk oly gyakran az őrmesterünk is ;-)

Zárás előtt még egy lehetséges forgatókönyv változat. Az internet tanúsága szerint **valóban folyt egy Vargay kontra Kanada per, erről itt lehet dokumentumokat találni**. Ebben az esetben **felmerülhet az a verzió is, hogy esetleg nem maga a főszereplő, hanem egy létező ügyet és személyt felhasználó nemzetközi csaló próbál meg így pénzt gyűjteni**. Ha pedig valóban volt jogsérelem, és mégis a főhős írja a leveleket, akkor viszont szerintünk nem jó utat és módszert választott a harcához.



Ha esetleg valaki erről [a konkrét ügyről](#), [perről](#), [Kanadáról](#) vagy magáról Vargay Péter Zsoltról többet tud, vagy csak ő is kapott a levélből egy példányt, **kommenteljen bátran**. Ha pedig nekünk lesz esetleg további infóink, **mi is frissítjük majd a posztot**.

***** FRISSÍTÉS *****

Az lenne a kérésünk az olvasók felé, hogy aki kap **BÁRMILYEN** nyelven **ILYEN VARGAY** levelet, küldje el nekünk azt **KOMPLETTEN**. Vagyis nem csak sima szöveges forwarddal, hanem a **TELJES** levelet fejléceستül (levél továbbítása mellékletként opció), hogy alaposan meg tudjuk vizsgálni ezeket.

Ide lehetne küldeni: [rambosoft GILISZTA commodore64 PUNKTE hu](#)

Előre is köszönjük.



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



Tweet

Ajánlott bejegyzések:

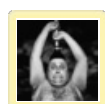
- [Gyerek-barát netezés](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/1988232>

Kommentek:

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



Mikorka Kálmán okleveles duguláselhárító kisiparos **2010.05.10. 20:37:00**

Idézetek a hup.hu/node/86385 fórumból:

Egyik:

"Nem a mekkáfonyát írta a csóka, hanem a viroverseer nevű víruskergetőt, és tényleg sokáig az ő cuccai védtek egyes bíróságok rendszereit. Tényleg matematikus, és volt olyan matematikai bizonyítása, amitől leesett pár egyetemi dolgozó álla."

Másik:

"Nekem pont osztálytársam volt ez a Vargay péter és tényleg ő fejlesztette a Viroverseer nevű víruskeresőt. Amolyan bolond zseni. Vagy zseni bolond?"

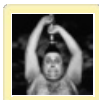
Abban az időben fejlesztőmérnök voltam és felügyeltem a cég IT rendszerét is (egy szerver meg vagy 20 kliens) és megvettem a főnökkel ezt a vírusvédelmi rendszert. Teljesen jól működött, havonta kaptunk frissítést, emlékszem Péter a DOTE-ra meg a KLTE-re járt vírusokat gyűjteni az ottani nyitott hálózatokból. Még 5.1/4-es floppy lemezekre jöttek a frissítések (1995 környéke). Ami lényeg, teljesen korrekt üzlet volt, minden jól működött."

Harmadik:

"A volt cégem is használta anno a vírusirtóját, volt olyan eset, hogy bejött hozzánk mert nálunk volt

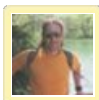


meg az a vírusminta amit felhasznált, és nálunk tesztelt egyszer.
Egyszer csak eltűntek a frissítések és nem tudtuk, hogy most mi van, be kellett szerezni másik vírusírtót."



Mikorka Kálmán okleveles duguláselhárító kisiparos **2010.05.10. 20:38:12**

Ez lehet a srác gimnazista korában: www.komal.hu/tablok/?fenykep=3582



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.05.10. 22:21:09**

Szia Géza!

Köszí a kommentet. Hát azt gindoltam én már olyan régen vagyok ebben az antivírus dologban, hogy mindenkit ismerek, de ezek szerint mégse. Pedig olyan nagy öregek mellett voltam, mint Kis János, a katona Famosi István, a Safe kft.s Szegedi Imre, jártam be a V2 épületbe floppys Chkvir frissítésért a Onehalfot visszaféjtő Leitold Ferihez, stb.

A Viroverseer-rő persze hallottam már. Most nezem ezt a linket:
itcafe.hu/tema/melyik_a_legjobb_virusirto_progi/hsz_29546-29546.html

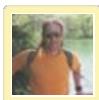
Ha valakinek, akkor neki aztán tényleg tudnia kellene, hogy ez a spamelős módózatú a captatio benevolentiae (jóindulat elnyerése) eléggé kontraproduktív, Így szerintem még nyitott kérdés valóban ő írta-e ezeket a leveleket, vagy a nevével él vissza valaki.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.05.11. 09:02:17**

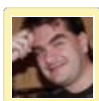
Most látom, hogy volt külön szlovák (eurós) és külön cseh (koronás) verzió is. Akkor ezzel együtt "véletlenül" hat különböző nyelven jelent ez meg kvázi egyidőben, három különböző bankszámlaszámmal :-O

www.hoax.cz/retezove-emaily/madarsky-spam---pomoc-peter-vargay/



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.05.11. 09:08:45**

Az angol verzióban szerepelnek a szomáliai kalózok is. Ez sajnos a magyar változatból kimaradt. Kár érte. :-)
hup.hu/node/86385#comment-1009770



Tigris 2010.05.11. 12:18:28

Tisztelt Barbalics Úr!

Az interneten több nyelven, többek közt magyarul is kering egy levél, melyet Vargay Péter írt és amelyben leírja, hogy hogyan perelte Kanadát. A hollandi Emberi Jogok Intézete szerint Ön képviselte az urat. A levelet annál is inkább furcsálltam, mivel kéri, hogy ügyészek, ügyvédnek továbbítsuk a levelét, miközben azt hiszem, 2007-ben már képviselte ?t egy jogi szakember, Ön.

Tehát a kérdésem az lenne, hogy a levél tartalma valós-e, mennyiben, illetve hogy az Ön tudomása szerint hogyan áll az ügy. Ugyanis egyik részr?l a levél nagyon hasonlít a Nigériából és hasonló helyekr?l érkező pénz átutalását kér? átverés-levelekhez, ugyanakkor ha ez igaz, a történet valós, akkor ennek nem körlevelekben lenne a helye. Az utóbbi esetben az úrnak nem pénzre, hanem nemzetközi jogi képviseletre lenne szüksége.

Az ok, amiért megkerestem, az az, hogy bár magam is munkanélküli vagyok, segíteni nem tudok, de ennek a levélnek mindenképpen szeretnék nyilvánosságot adni, akár úgy, hogy mindenki figyelmét felhívom rá, hogy ez kamu, akár úgy, hogy van egy ügy, aminek nyilvánosságra és támogatásra van szüksége.

Várom választ.

Üdvözzel

MM

S a válasz:

Tisztelt MM Úr!

Megtisztelő érdeklődésére válaszolva közlöm, hogy az ENSZ Humán Rights Committee által nyilvánosan közzétett No. 1639/2007 ügyszámú döntés 2009.07.31-én a hivatkozott valós ügyet lezárta, az eljárás a fenti döntéssel végérvényesen befejeződött.

Tisztelettel:

Dr B. I. ügyvéd,
társasági szakjogász, biztosítási szakjogász

Egyébként az ügyet per nélkül zárták le, elutasították, ugyanis: „inadmissible under article 5(2)(b) OP, failure to exhaust domestic remedies”, tehát VP nem élt az itthoni jogorvoslat lehetőségével.

forrás:

sim.law.uu.nl/SIM/CaseLaw/CCPRcase.nsf/a3cdc980fe0bd523c12567b70044cc02/2bbceb44eaae65b6c1257648002ab4d0?OpenDocument

részletesen:

sim.law.uu.nl/SIM/CaseLaw/CCPRcase.nsf/3167fd85523cbf75c12567c8004d4280/216059fla305aaaac12576490034c8cc?OpenDocument

Rengeteg változata van a levélnek, én franciával és göröggel találkoztam.

Boorisz 2010.05.11. 12:49:22

Annyira irigylem azokat az embereket akik nem csak pornót kapnak mint én.



Tigris 2010.05.12. 13:10:33

Részemről el tudom küldeni, de a levelet a tudomásom szerint sosem Vargay úr küldi, lévén hogy szegény annyira csóró, hogy e-mailje sincs (mobilja van). Mellesleg ha elolvasod a levelet, nem említi, hogy ő írta a levelet, hanem másokat kér hogy másokhoz juttassák el, tehát meg is indokolja, miért nem érdekes a feladó.

Amúgy tessék, az én fejlécem:

+OK 1973140 octets follow.

Return-path: <orosz.imre.dobozolo@upcmail.hu>

Envelope-to: tigrincs@tigrincs.hu

Delivery-date: Mon, 10 May 2010 07:12:47 +0200

Received: from s23.mediacentre.hu ([195.70.48.77])

by mail.mediacentre.hu with esmtp (Exim 4.69)

(envelope-from <orosz.imre.dobozolo@upcmail.hu>)

id 1OBLIN-0007hf-Oy

for tigrincs@tigrincs.hu; Mon, 10 May 2010 07:12:47 +0200

Received: from viefep12-int.chello.at ([62.179.121.32])

by s23.mediacentre.hu with esmtp (Exim 3.36 #1)

id 1OBLI3-0008Vi-00

for tigrincs@tigrincs.hu; Mon, 10 May 2010 07:12:28 +0200

Received: from edge02.upcmail.net ([192.168.13.237])

by viefep12-int.chello.at

(InterMail vM.8.01.02.02 201-2260-120-106-20100312) with ESMTP

id <20100510050600.CFHE8481.viefep12-int.chello.at@edge02.upcmail.net>;

Mon, 10 May 2010 07:06:00 +0200

Received: from vte ([89.134.179.233])

by edge02.upcmail.net with edge

id Fh3Q1e04g52Y6r502h3RGT; Mon, 10 May 2010 07:05:55 +0200

X-SourceIP: 89.134.179.233

Message-ID: <0047AB1E955DA2ADA3AD2BDD25D4EE27@vte>

From: =?iso-8859-2?Q?Vargay_P=E9ter?= <orosz.imre.dobozolo@upcmail.hu>

To: <muk@mail.tvnet.hu>

Subject: =?iso-8859-2?B?U2Vn7XRz6Wch?=>

Date: Mon, 10 May 2010 07:03:25 +0200

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="-----_NextPart_000_12B3_08A87A57.A8AD8427"

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 6.00.2900.5843

Disposition-Notification-To: =?iso-8859-2?Q?Vargay_P=E9ter?= <orosz.imre.dobozolo@upcmail.hu>
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5579
X-Cloudmark-Analysis: v=1.1 cv=SLkC287PFWo6d7eSEiSBB9255DBOWQ3bwOwHXJiyZoo= c=1 sm=0
a=jPJDawAOAc8A:10 a=o7kzLXVHS1sA:10 a=9w_aQDbYx_azopMJhGAA:9 a=qiNcleUY8d91bqr7G2yXDLO7kAA:4
a=jiObf9B0YAUA:10 a=AcJNXtNo7VnebSPVt0oA:9 a=u2XwHFXnuPsxe5MVYOE:7
a=MNT_O8cZFIK0ZN1KpiMJjzoo40A:4 a=HXfae_bayExQdyQVBkAA:9 a=Hr6FnReGvZbHMjAJGwgA:7
a=_v5ihUi3QmylWCvkkGQd7YIFAPgA:4 a=diV1Cm6KfS4A:10 a=HpAAvcLHHh0Zw7uRqdWCyQ==:117
X-MediaCenter-MailScanner-Information:
X-MailScanner-ID: 1OBLI3-0008Vi-00
X-MediaCenter-MailScanner: Found to be clean
X-MediaCenter-MailScanner-SpamCheck: not spam (too large)
X-MediaCenter-MailScanner-From: orosz.imre.dobozolo@upcmail.hu
X-EsetId: 28BF1728D51F7C6937B9177CDE4530

debian 2010.05.13. 21:32:24

A cég neve ez volt:
TENZOR Szoftver Fejlesztő és Földmérő Betéti Társaság (4026 Debrecen, Hatvan u. l/c. I/2.)
A doksiban Fenzor néven találtam.

Sheriff az égből 2010.06.02. 11:58:31

Hali,

Bar spamnek spam, a sztori igaz. Sot, ha konyvet ima belole
nemtudnatok lejenni rola.

En dologoztam vele a Tenzorban anno, sokat tanultam tole
es barataitol kollegaitol, jol ismerem Petert. Ottvoltam vele a
Legfelsobb birosagon, a TVK-ban, az Alkaloidaban es rengeteg
egyeb helyen ahol hasznaltak a programot. Sajnos a mai napig
nincs szemleleteben sem hasonlo virusvedelmi rendszer.

Annyit eltudok rola mondani, hogy egyetemista koraban peldaul
bebizonyította egy az iskolan tanított tetelrol amit 20 eve tanitanak,
hogy hamis. Programozasbol alig engedtek at, hogy nemtud
programozni, par ev mulva az egyetem megvette a rendszert.

A sztori reszleteirol nemerzem magam jogosultnak, hogy sokat irjak,
tegye meg azt o. Sajnalom, hogy igy megszivattak, megerdemelne
ez a sztori kicsit tobb figyelmet.

Aki Kis Janost ismeri annak a Vargay Petert is illene ismerni. Kis Janos
anno konyveben emlitést is tesz ra.

Emlekszem, volt egy polimorf virus ami elkodolta a winyot
szektoronkent es utana hasznalhatatlan volt minden hacsak nem
fizettel. Csak o tudta megirni a visszakodolot, senki masnak nemvolt
ra megoldasa a vilagon.

A Viroverseernek igazabol az internet rohamos fejlodese es az uj
operacios rendszerek elterjedese tett be. Amig csak adathordozon
terjedtek a virusok, addig kordaban lehetett tartani oket, mert
lehetett tudni mi terjeng az orszag hatarain belül. Az internet
es a fergek es a sok olcso semmit nemero virusvedok megjelenesevel
a piac leszukult, ezutan ment ki kanadaba.

Ott gyakorlatilag ehberert elment dolgozni egy komplett
tuzfal/virusvedo gyartohoz, ahol ket het utan olyan tiszteletet
vivott ki maganak, hogy nagyon nehezukre esett mikor a tortentek
miatt ugymond menekulnie kellett onnan.

Nyilvanvalo azis, hogy mineki a maga szerencsejenek a kovacsa es
valahol elrontott o is valamit. Nem tortenik mindenkivel ilyen, de
nemfeltetlenul a saját hibajabol tortent es szerintem ez bakivel
megtortenhet.

Ugyanakkor nemtudom mit tudna barki is tenni. Szarugy. Kuravara
sajnalom az egeszet.

Itt az ajándék iTunes Voucher

2010.05.12. 12:10 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [apple itunes csalás hamis trójai voucher](#)

Beszélgetnek két sör mellett a hamis antivírusok fejlesztői. Janikám, a [hamis AV](#) megvolt, [kitalált új programverzió](#) kipipálva, a [hamis adathelyreállítót](#) én magam javasoltam, a múltkori nagyágyú [hamis RIAA üzenet](#) is megvolt, [Macintoshra videokodek](#) már szinte uncsi, [adathalásztunk](#) is már, [Google linkeket](#) naponta mérgezzük, milyen érdekességet nem találtunk még fel eddig? Hát Ferikém, **most talán egy iTunes Voucherre lenne szükség**, akárki meglássa!



És íme megszületett igen, csak most, csak nekünk. [50 dolláros ajándékutalvány az iTuneshoz](#), **ajándokot kapni pedig jó**, még ha nincs is épp Karácsony. **A feladó (szemre legalább is) az iTunes Online Store <software@itunes.com>**. Persze lehetne ez akár csibakka@darthvader.hu is, technikai akadály a nincsen. Aki pedig még hisz a mesékben, és az ingyen ajándékokban, egy jól fejlett ZIP-nek látszó trójait vehet át. A megfertőzött gépén nyitott hátsó ajtón keresztül **valóban elközeledik jóval több, mint 50 dollár értékű ajándék, csak éppen kifelé** csúrnak majd rajta a jelszavak, ellopott adatok.



A világban, de különös tekintettel igaz ez az internetre, **egyszer s mindenkorra megszűnt az a régivágású hozzáállás, amikor automatikusan jó szándékot feltételezve mindig bizalommal lehettünk - vagy talán soha nem is létezett.** It's over. [Eladó az egész világ](#), és mindig azt kell nézni Pizskos Freddelel szólva: [Kavarják ezek vagy nem kavarják?](#) És általában zömmel mindig kavarják. Csak a javunkat akarják ;-)



Elvi síkon nem kizárt persze, hogy jó szándékú emberekkel hébe-hóba így is találkozunk, de **a számítógépes oktatásnak csak az egyik fele az, hol a power gomb, mi az az Internet Explorer és eszik vagy isszák a vírusirtót.** A másik fele kötelezően annak kell(ene) lennie, hogy **milyen valódi napi kockázatok vannak**, mik lehetnek az intő jelek, mik a tipikus átverések, mik a követendő viselkedésmódok.



Ezt kell(ene) jelentenie a "valamit konyítok" a számítógéphez kijelentésnek, amitől sajnos még messze vagyunk.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Dropbox csálival terjedtek a kémprogramok](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1994510>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.05.12. 13:04:11](#)

Sajnos az emberekben rögzült az, hogy az írott tartalom más mint az élő szó. Elfelejtik, hogy az interneten írott tartalmat olvasni idegenektől még a saját postaládánkban is olyan mintha az utca túloldalán álló idegen kiabálna át nekünk, hogy adjuk meg neki a személyes adatainkat.

Ahogy az életben úgy a neten sem kéne.

És itt most ideírhatnám régi kedvenc mondásom:

Aki hülye haljon meg!

De már úgy vagyok vele, hogy aki hülyévé teszi az embereket haljon meg :-)

Kiegészítve azzal, hogy az életben is elég nehéz lenne bárkiben megbízni, ha mindenki alakváltó lenne és nem rendelkezne egyéni azonosításra alkalmas jelöléssel. És a gyártók olyan házakat gyártanának, amiknek átlátszó a fala, és csak mindenféle mérnöki képzettség után tudnád függönnyel eltakarni a személyes dolgaidat, de a függönyöd a rendszeres mosás nélkül átlátszóvá válna amit csak kívülről veszel észre. És még folytathatnám.

[Boorisz 2010.05.12. 18:55:00](#)

Az egészében az a jó, hogy ha jól tudom Mo.n még nem működik az iTunes. Persze ez nem jelenti, hogy egyikét ember ne szívná meg.

Támadható vírusirtók világvége nélkül

2010.05.13. 18:50 | [Csizmazia István \[Rambol\]](#) | [8 komment](#)

Címkék: [földrengés világvége kernel árvíz tűzvész hook armaggedon](#)

Kétségtelenül kellene a blikkfangos címek, ez teszi eladhatóvá a cikket. Viszont a "[Leégték a népszerű vírusirtók](#)", meg a "[Minden vírusirtó kijátszására alkalmas támadást fedeztek fel](#)" - itt a földrengés - kissé túlzásnak tűnik.



Ha most mi vagyunk az Elzett Művek, vagy a Mul-T-Lock, és valaki cikket ír: "Leégték a népszerű zárgyártók, mert fejszével és csákánnyal lám mégis bejutottunk", **akkor ezt az információt azért érdemes értékén kezelni. Nyilván nem az lesz a hatása, hogy ezentúl egyáltalán nem használunk zárat, vagy nyitva hagyjuk a lakásajtót.**



Mindjárt **az elején rögtön megadhatjuk a pontot a versenyzőknek, az elismerést a szakértőknek**, ez viszi előre a világot, hajrá örökös kísérletezés. Erről szól a szakma, a támadás és védekezés örökös macska-egér harca.



[A kipécézett Kernel Hook Bypassing Engine mód](#) egyébként - amely a többszálú végrehajtással kapcsolatosan azon alapul, hogy a vírusvédelmi program már leellenőrizte, de még éppen nem adta át a Windowsnak, és ekkor ki lehet cserélni egy kártékony kódra - elv [egyáltalán nem újkeletű](#), már [többször felvetődött](#) hasonló dolog. Sőt egész pontosan **ez a mostani "vadonatúj" megközelítés is konkrétan napvilágot látott már 2003-ban.**



Az ilyen **ITW (In the Wild)** kódtól azonban **nem igen kell tartani**, mert [egyrészt elég speciális](#) (lám ennek a csapatnak is három évbe tellett a dolog). David Harley szerint a támadás kizárólag a NOD32 és ESS **önvédelmi mechanizmusát veszélyeztetheti elvileg, nem pedig magának vírusvédelemnek a működését.** [Másrészt ahhoz hogy egyáltalán egy ilyen támadás megvalósulhasson, sok dolog kell, például már eleve fertőzöttnek kell lennie előzetesen a rendszernek.](#) Víruslaborunk tájékoztatására támaszkodva kijelenthetjük: bár a módszer 1996, illetve 2003 óta ismert, de eddig ilyen típusú kártékony kóddal egyáltalán nem találkoztak.



Persze nem szabad az esetet bagatellizálni sem, hiszen valós veszélyt és kockázatot jelent, csak nem akkorát, mint a hírverés. Az F-Secure weblogja is "[KHOBE Not So High On The Richter Scale](#)" címmel jelent meg (However, this attack **does not** "break" all antivirus systems forever. Far from it.).



Nyilván amit az **antivírus gyártóknak (és nem csak a népszerűeknek, hanem mindnek ;-)** tenni kell, hogy ezt a megkerülést **mihamarabb befoltozzák** - ahogy tették ezt eddig is a fejlesztés folyamán minden hasonló esetben.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/1999935>

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 2010.05.13. 21:52:09](#)

A pc fórum-os Sting mindig érdekesítő cikkeket tud írni.
Az rss olvasómból régen töröltem az egész pc fórumos csatornámat. Győzött az it café.



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.05.14. 13:07:15](#)

A való életben nehezen használható ki a bonyolult időzítési sebezhetőség:
www.virushirado.hu/hirek_tart.php?id=1636



[gothmog 2010.05.14. 21:51:59](#)

A pcfórumra stingen kívül ki ír még?



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.05.15. 20:07:56](#)

Ruining a Myth - KHOBE The AntiVirus Earthquake - Pure Hysteria:
evilcodecave.blogspot.com/2010/05/ruining-myth-khobe-antivirus-earthquake.html



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.05.17. 10:11:27**

A Matousec tesztek "objektivitásáról" meg annyit, hogy már nem ez az első húzásuk, 2008 év végén is volt egy tűzfal leak tesztjük, amit nem az AMTSO elvek szerint végeztek, egy kiragadott tulajdonsága a tűzfalnak még nem minősíti komplexen annak egészét, sőt a pártatlanság is hibádzott, mert a győztes programot a weblapjukon közben ők maguk reklámozták és árulták.

Egy kis adalék a témáról:

antivirus.blog.hu/media/image/pdf/pcw200901.pdf



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.05.17. 13:31:39**

Ezt már tényleg csak az utókornak csinálom, mindenki aki számít *.* vélemények összegyűjtve az AMTSO lapon. Remélem, majd a 2111-ben dolgozó internet könyvtáros, aki ezt a posztot épp begyűjti, megdicsér majd, hogy alapos voltam ;-)

amtso.wordpress.com/2010/05/15/khobe-not-a-test-issue-but/



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.05.17. 13:49:02**

Na nem ígérem meg, hogy az utolsó kommentem, mert lehet, hogy nem tudom mégse betartani :-D (Rockmonitor Final Version)

Cimbora hívta fel a figyelmet az alábbi igen érdekes linkre az előbbieik közül:

blog.gdatasoftware.com/overview/article/1654-khobe-no-problem.html

Ez a Gdata blogja, még csak nem is a miénk. :) Ebből a lényeg:

1. A Matousec szenzációra vadászik.
2. A Matousec ezután a felfűjt botrányból megpróbál profitálni. A média segítségével éri el a Matousec azt, hogy az antivirus gyártók ne engedhessék meg maguknak, hogy nem veszik meg a "kutatását". Ha médiabotrány nélkül próbálna ugyanezt, az antivirus gyártók simán elküldenék a fenébe.
3. Mindeközben a Matousec segítséget nyújt a vírusok készítői számára az információk nyilvánosságra hozatalával, de megnehezíti az antivirus gyártók munkáját az információk elzárásával.
4. Végül a Matousec felajánlja az antivirus gyártók számára, hogy analizálja a forráskódjaikat, ha szeretnék. :)

Nem véletlen, hogy a Matousec nem tagja az AMTSO-nak... :-)



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.05.18. 21:44:52**

@gothmog:

Passzolok, hébe-hóba olvasom őket.

De talán ennyire nem is mehet mindenki a hírek után, ezért nem haragudhatunk. Inkább az lenne a lényeg, ha valami egy újságírónak már egyből nagyon gyanús, bűdös, hihetetlen, akkor ne kezdjen reflexből kopipasztaálni az 5 perc hírnévért, a szenzációszagra gyűlik az éji vad, elsőzőn itt cikkíróként :-).

Aztán ha meg valami kiderül így szanzsén menet közben, akkor haladéktalanul frissítsen és helyesbítsen utólag is, hiszen nem mindenki real time olvas cikket a neten. Meg tanuljon is az esetből. Lásd fejbe lőtték a nem létező orosz spammert, még hónapok múlva is láttam pár helyen a cikket.

Frissíteni kellene a Windowst

2010.05.17. 11:00 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

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

A Conficker férgek már hetedik hónapja őrzi vezető helyét a magyarországi vírusostoplistán. A felhasználók többsége nem törődik túlságosan a vírusirtó és a Windows frissítéseivel.



Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melynek elemzése tanulsággal szolgálhat a felhasználók számára. A magyar lista első helyét 2009. október óta a Conficker férgek tartja, amely az operációs rendszer frissítéseinek hiányát, a gyenge admin jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed.



Más országokban hasonló a helyzet: a Conficker Angliában, Finnországban és Németországban is hónapok óta az első helyen áll a vírusostoplistákon. Ha figyelembe vesszük, hogy a vírusirtó cégek és a Microsoft hány figyelmeztetést, technikai útmutatót és frissítést adtak ki az elmúlt fél évben, csak az a kép rajzolódhat ki ebből, hogy a felhasználók jelentős hányadát egyáltalán nem érdekli a számítógépe biztonsága.



Az áprilisi toplistán új szereplőként két trójai és egy féreg jelent meg. Egyikük ismerős lehet: a Win32/Mebrook trójai 2009 júliusában már bekerült a 10 legfertőzőbb vírus közé. Akkor sem szerettük túlságosan: mivel törölheti a merevlemez partíciós tábláját, adatvesztést okozhat.



A toplistára most felkerülő Win32/Pacex féreg érdekessége, hogy néhány változata rootkit komponenssel is rendelkezik. A Pacex így működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek az állományok nincsenek ellátva rejtett attribútummal. Ezen kívül hátsó ajtót is nyit a megtámadott gépen, majd távoli weboldalhoz kísérel meg csatlakozni, ahonnan további kártékony kódokat tölt le, illetve frissíti magát.



A Win32/Packed.Autoit trójai fájlokat hoz létre a C:\Windows\System32 mappában, és a kártékony .exe fájlok automatikus lefuttatásához külön rendszerbejegyzéseket is készít. Működése során szintén hátsó ajtót nyit a megtámadott gépen, majd több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



Az ESET több százezer magyarországi felhasználó visszajelzése alapján statisztikai rendszere szerint 2010 áprilisában az alábbi 10

károkozó terjedt a legnagyobb számban. Ezek együttesen az összes fertőzés 24.74%-ért voltak felelősek.



1. Win32/Conficker féreg

Elterjedtsége az áprilisi fertőzések között: 5.85%

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 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 válnak a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható a külső meghajtó fertőzött Autorun állománya miatt.

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



2. Win32/Agent trójai

Elterjedtsége az áprilisi fertőzések között: 4.54%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (például Temp mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett kulcsokkal gondoskodik arról, hogy minden indításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.



A számítógépre kerülés módja: a felhasználó maga telepíti.

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



3. INF/Autorun vírus

Elterjedtsége az áprilisi fertőzések között: 3.92%

Működés: Az INF/Autorun egyfajta 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/autorun>



4. Win32/PSW.OnLineGames trójai

Elterjedtsége az áprilisi fertőzések között: 2.34%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozóknak rootkit komponense is van, amelynek segítségével igyekeznek állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. 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/psw-onlinegames-nnu>



5. INF/Conficker vírus

Elterjedtsége az áprilisi fertőzések között: 2.07%

Működés: Amennyiben böngészés során az autorun.inf fájl valamely egység főkönyvtárába kerül, akkor a betöltő eléri, hogy a kártevő kódja induljon el. Vagyis az INF/Confickernek az a szerepe, hogy betöltse magát a Win32/Conficker kártevőt.



A számítógépre kerülés módja: fertőzött weblapról, vagy külső eszközön keresztül.

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



6. Win32/TrojanDownloader.Bredolab trójai

Elterjedtsége az áprilisi fertőzések között: 1.75%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, mely távoli oldalakról további kártékony kódokat tölt le és hajt végre. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is kulcsokat készít, illetve módosít a biztonságítamogatás-szolgáltató (SSPI - Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.



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

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



7. Win32/VB féreg

Elterjedtsége az áprilisi fertőzések között: 1.66%

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/vb-el>



8. Win32/Packed.Autoit trójai

Elterjedtsége az áprilisi fertőzések között: 0.99%

Működés: A Win32/Packed.Autoit fájlokat hoz létre a C:\Windows\System32 mappában különböző neveken, például autorun.inf, winlog0n.exe, svch0st.exe. A kártékony EXE fájlok automatikus lefuttatásához külön Registry bejegyzéseket is készít. Működése során

hátsó ajtót nyit a megtámadott gépen, 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/packed-autoit-gen>



9. Win32/Mebrook.K trójai

Elterjedtsége az áprilisi fertőzések között: 0.86%

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 hoz létre, illetve módosítja azokat, ha már léteznek. Ezenkívül megkísérel a google.com webcíme 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/mebrook-k>



10. Win32/Pacex féreg

Elterjedtsége az áprilisi fertőzések között: 0.76%

Működés: A Win32/Pacex féreg fertőzése során különböző DLL, EXE és BAT fájlokat hoz létre a C:\Windows\System32 mappában, majd a rendszerleíró-adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. Működése során hátsó ajtót is nyit a megtámadott gépen, távoli weboldalhoz is megkísérli a csatlakozást, és arról további kártékony kódokat, illetve saját újabb verzióját tölt le. Egyes változatai a jelszavakra is veszélyt jelentenek, mivel ezeket is összegyűjtik a megtámadott gépen. Az .AE verzió pedig Rootkit komponenssel is rendelkezik, működése során fájlokat rejt el a fájlkezelő alkalmazások elől, még akkor is, ha ezek nincsenek ellátva rejtett attribútummal.



A számítógépre kerülés módja: internetről vagy fertőzött levélmellékletben

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



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2005500>

Kommentek:

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

spggg • <http://www.zughekker.info> 2010.05.18. 20:34:47

A felhasználók nagy része nem érti, hogy miért kellene változtatnia. Úgy gondolják, hogy tökéletesen működik, lehet rajta levelezést kezelni, zenét hallgatni, stb. Így hát maradnak az XP mellett. Én, mint 15 éves tapasztalom, hogy az oktatásban semmit nem tanulunk a biztonságról. A környezetemben lévők nagy része nem is tudja, hogy milyen különféle módszerek léteznek a bizalmas információk megszerzésére.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.05.18. 21:57:17

Sajna nem várható el mindenkitől, hogy így gondolkodjon :-)
sorhab.freeblog.hu/archives/2010/05/18/Amikor_tenyleg_visszanyal_a_fagyit/

Egyébként tényleg az oktatás lenne a kulcs, valahogy keresztetni kéne a régi TV Basicet a mai NetAcademiával ;-)

ScapeDeer 2010.05.28. 19:04:35

Bezzeg Win98-cal manapság már tök nyugodtan lehet nyomulni, mert minden káros cucc NT alapú rendszereket támad...

Connie21 2010.05.28. 21:51:46

Egy kis segítséget szeretnék kérni. Egy olyan vírus került a gépemre, ami blokkolja a Nod32 frissítését. Az utolsó frissítés majdnem két hónappal ezelőtt volt, de a program mégis azt írja ki, hogy a vírusdefiníciós adatbázis naprakész. Mit lehet ilyenkor tenni?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.05.31. 10:01:27

Szia Connie21!

Ha nem tudod elérni a frissítést, ez okozhatja ugyan vírus is, de emellett még sokféle más oka is lehet. Azt javaslom, hívd fel telefonon a supportosainkat, és pár perc alatt kiderül, mi a gond:
www.eset.hu/tamogatas/kapcsolat

Privátlet ellenőrzés

2010.05.19. 18:00 | [Csizmazia István \[Rambo\]](#) | [3 komment](#)

Címkék: [adatvédelem](#) [privacy](#) [facebook](#) [ellenőrzés](#) [privátlet](#)

Kazinczy legyen a talpán, aki a kesztyű, lábtű, facebooktű után a **privacy szóra is találó, elfogadott magyar kifejezést talál vagy alkot**. Mindenesetre **akárhogy hívják is, védeni azt kell, és a rendszeres ellenőrzés is segíthet** abban, hogy nehogy nagyon eltoljuk a kalapács nyelet a beállításoknál és véletlenül túl sokat fedjünk fel.



A [Facebook érdekességeiről](#) már [itt a blogban is beszéltünk](#) sokszor, sőt [még annál is többször](#). Ezeken felül még kitérünk majd rá a júniusi PC World cikkben is, most azonban **az adatvédelmi beállításainkról lesz szó**. Sokan vannak, akik még arra sem veszik a fáradságot, hogy a Facebookon beállítsanak olyan alapvető biztonsági opciókat, mint pl. az "Események az alkalmazásokban és a játékok kezelőfelületein" rész. **Emiatt aztán a Farmwilleben a napi ötszöri aratásról folyamatosan küldik az értesítést összes barátjuk, ismerősük, de főnökeik felé is.**



A dolog persze ennél bonyolultabb, hiszen filozófiailag ugye nem létezik olyan vírusirtó sem, ami a vírusok 100%-át képes lenne kiszűrni. Így olyan beállítás sincs, ami **garantáltan minden adatszivárgást, személyiséglopást meg tudna akadályozni**, de azért ettől még törekedni kell rá, és javítani mindig lehet. **Két féle teszt módszert is találtunk**, az egyiket [az F-Secure blogjában](#) mutatták be, a [másikat a Websztánon láttuk](#).



Lényeg a lényeg, **a dolog haszna egyértelműen az lenne**, hogy aki esetleg már állítgatott ezt-azt, **az lemérje, jól csinálta-e**. De a többség valószínűleg most először csodálkozik rá ezekre az adatvédelmi beállításokra, **nekik pedig mindenképpen jól jöhet, ha rendezik a dolgaikat**. Amiről mi tehetünk, azt lehetőleg csináljuk jól, **aztán a többi már úgysem rajtunk múlik**, például a naponta változó apróbetűs rész, amivel személyes és kapcsolati adatainkat aztán majd jól kimérik egyszer kilóra.



A végére **egy bombabiztos adatvédelmi recept következik**, melyet - mintha csak egy Dr. Bubó epizódot zárnánk - akár aranyba is foglalhatunk: "Ursula, kérem jegyezze fel, **az adatok a legnagyobb biztonságban akkor vannak, ha egyáltalán fel sem töltjük őket...**"

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

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Kártya böngésző kiegészítők jönnek](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2014899>

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](#).



[neomatsek 2010.05.19. 23:52:54](#)

Hali!Az ismerősök kéretlen hülyeségei ellen a legegyszerűbb,ha te magad letiltod és kész,mivel a legtöbb ember baromira nem veszi a fáradságot,h foglalkozzon a beállításokkal.Nekem elegendő lett abból,h a főoldalam tele volt napi paraszt,napi idézet és egyéb alkalmazások üzeneteivel,ezért egyszerűen az adott üzenet jobb felső sarkában rákattintottam a megjelenő hide szóra,majd még egyszer a felkínált hide xy gombra,ennyi:D



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu> 2010.05.20. 08:44:17](#)

Szia Neomatsek!

Félreértetted a dolog célját. Nem tudom mások hogy vannak vele, de én szeretem az üzenőfalat, egyáltalán nem tekintem hülyeségnek a kapott üzeneteket, idézeteket, sőt olvasom. Persze ebben biztos benne van már a jungi szinkronicitás, a Menneyei prófécia könyv (hogy semmi sem véletlen, jönnek az útjelzők, ami nem útelágazósódás ;-)

Az írás célja az, hogy senki ne osszon váéletlenül olyat, amivel tudtán kívül maga alatt vágja a fát.

Egy jó kis posztot ütött össze Caracalla itt, szerintem érdemes megnézni:

[caracallablog.blog.hu/2010/05/03/eletek_a_facebook?](http://caracallablog.blog.hu/2010/05/03/eletek_a_facebook?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+caracallablog+%28Caracalla+blogja%29)

[utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+caracallablog+%28Caracalla+blogja%29](http://caracallablog.blog.hu/2010/05/03/eletek_a_facebook?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+caracallablog+%28Caracalla+blogja%29)



[neomatsek 2010.05.20. 14:43:38](#)

@Csizmazia István [Rambo]:

Bocs,azért reagáltam arra a kis részletre,mert én is farmvillezek és nem egy ismerősöm szolt már,h kezd elege lenni a sok tojásból,állatkából és egyébbből főoldalon,és mindegyik meglepődött,amikor megkérdeztem,h miért,szerintük én annyira örülök a sok idézetnek,szívnek,virágnak és baromságnak?Sokan nem is tudják,h ezeket a dolgokat el lehet rejteni,az átlag emberke osztja az észt a farmvillesnek,és fordítva,holott pár kattintással meg lehetne oldani a dolog,és mindenkinek meglepnie a lelki békéje.Csupán ezt szerettem volna jelezni:D:D:D

Hogyan lehetne mégis segíteni nekik?

2010.05.21. 11:35 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [oktatás](#) [biztonság](#) [kockázat](#) [átlagjuzer](#)

Az átlag ember az, akire évi 4.5 kilogramm hús és 110 liter palackozott víz fogyasztása esik. Nem számítógépprogramozó, nem hacker, **csupán használni kívánja a számítógépét**, szeretne vírusmentes maradni - ha egyáltalán hallott már ilyesmiről - **valamint nem olvas olyan blogokat sem, mint amilyen ez itt**. És ezzel követi el a legnagyobb hibát... ;-)



Mi pedig itt a másik oldalon **írhatjuk szorgosan az egyik tanulságosabb tantörténetet a másik után**, a törzsközönség csendben értékeli, elolvassa, de a várt áttörést a másik oldalon mindig csak remélhetjük. Aggódhatunk azok miatt, **akik ab ovo nem olvasnak szakmai cikkeket**, számítástechnikai folyóiratokat, magazinokat, **közben meg könnyen áldozatul eshetnek csalásoknak, adathalászatnak, kémprogramoknak**. Ahogy persze mi sem olvassuk a bejgli sütés rejtelméről, vagy a feng shui bútor elrendezés varázslatos világáról szóló írásokat - igaz, ezzel nem is sodorjuk magunkat veszélybe. Mik és hol hiányoznak, **hol lehetne valami picit mégis tenni az átlagfelhasználók** számítógépes biztonságaért, kinek és hogyan lehetne üzenetet eljuttatni hozzájuk? Ha barátunk, családtagunk, ismerősünk az illető, akkor közvetlenül máris segíthetünk, de jó lenne azért egy ennél lényegesebben nagyobb merítés.



Ha elolvassuk egy olyan cikket, **amiben egy ilyen átlagfelhasználó számítógépes megpróbáltatásairól értekeznek**, jellegzetes tünetekről olvashatunk: **pár hónap alatt drasztikusan lelassul a gép, elborítják a reklámok, kártevők**. Ilyenkor egy férj, unoka, barát, rendszergazda, rendőr, postás, vasutas, halbiológus, vadakat terelő juhász ismerős segítségére szorulnak, és az illetőnek rendbe kell tennie a gépet. **Kitakarítja Augiász istállóját**, vírusot irt, kémprogramokat szed le, program megoldásokat javasol a jövőre nézvést.



Miben kellene minden számítógépet vásárlónak tisztában lennie? **Legalább alapfokon a kockázatokkal**: adatait ellophatják, tipikus csalásokkal csálhatják ki tőle ezeket, milyen jelszavakat használjon, milyen fizetős vagy ingyenes védelmi programokkal ajánlatos körbepásztázni magát, és ezek kezelését el tudja-e sajátítani. És persze a ráadás kérdés, kihez fordulhat segítségért, ha mégis problémája támad. Megtehető persze ez a "kis lépés nektek, egy hosszú lépés nekem" bátorságával is, de azért ezek nélkül az ismeretek nélkül ez csak vakrepülés, a gépvásárlással egyúttal fejest ugrik láthatatlanul a dolgokba.



Az érem másik oldala lehet a szakmáé. Vajon **a vírusirtók, internet biztonsági csomagok** automatikus módja elég könnyű és érthető-e számukra? A vásárláskor a kereskedő tisztázta-e velük, hogy **a géphez esetleg "járó" víruskereső nem ingyenes**, és sok esetben csak egy 2-3 hónapra szóló próbaverzió, amit utána pénzért majd meg kell vásárolni? Sok esetben **hallgatnak erről, vagy gyorsan túl esnek a "van hozzá ajándék program is" fordulattal**. Amiről egy újonc honnan is tudhatná, neki kell majd foglalkoznia ezzel a későbbiekben.



Ez az összemosás sokszor nem teljesen korrekt még a számítástechnikai magazinok lemezmellékletein, weblapok letöltéseinek szóhasználatában sem. **Amikor teljes verziós Internet Explorert, ajándék Firefoxot hirdetnek, az legalább csak vicces**. De amikor a demo, kipróbálható idő- vagy funkció korlátos próbaverzió, teljes értékű freeware, shareware és kereskedelmi programok közötti különbséget szépítgetik a gép eladásnál, vagy kódösitenek, az hosszú távon senkinek sem jó.

A védelmi programoknál mindenkinek más az igénye, de **ha valaki nem tudja az övé micsoda, legalább az elérhető ingyenes**

programokkal kellene védenie magát. Ha pedig valaki szoftvert vásárolni is hajlandó, a vírusvédelmi megoldásoknál pont az ilyen **kezdő felhasználók** profitálhatnak sokat például **a segítőkész support segítségéből.**



A végső kulcs persze valamilyen rendszeres oktatás lenne, ami a gyerekeknek, fiataloknak már jön az iskolából, **a gondot ez inkább a felnőtt fejjel a géphez ülőknél jelent.** Egyre jobban elfogadottá válik az állás keresésnél, hogy legalább alapfokú számítástechnikai ismereteket mindenkinek fel kell tudni mutatnia. Jó ötlet lehet **egy zombitudatosági hét** is, de **a wifi kötelező alapfokú védelme** (ami még mindig jobb mint a semmilyen) is egy **hasznos kezmenyezésnek tűnik.** Talán az internet szolgáltatóknak kellene egy füzetet adnia minden egyes új előfizetőnek? **Nehéz kérdés.** Ha valaki tud erre jó receptet, más országban látott követendő példát, kommenteljen bátran!

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

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

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2018464>

Kommentek:

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

spggg • <http://www.zughekker.info> 2010.05.21. 14:00:49

Szerintem az oktatás a hiba gyökere. Angol előkészítő informatikára nyertem felvételt és ha jól tudom, valahol az év közepén már le is lehet tenni az ECDL -t. Ez késő! Nem veszik figyelembe az informatika fontosságát. Ha hetente legalább 2 óra lenne, akkor az egyikben már el lehetne kezdeni 8. osztályban az ECDL -re való felkészülést. Talán így kevesebb lenne az, aki bedől a "Gratulálok, 10.000FT -t nyertél!" típusú támadásoknak. Nem azt mondom, hogy ez megoldás lenne, de egy szinten javulna a helyzet!

[amodent](#) 2010.05.25. 20:06:10

Azért örülök, hogy nem csak engem zavar a magyar IT lapok szóhasználata. Kiskutyafüle 4.0, teljes verzió! ingyen! Aztán telepítéskor kiderül, hogy tényleg teljes verzió, tényleg ingyen, de csak 30 napig...

Az ECDL pedig... nekem is van, láttam a kolleginákon, ahogyan bemagolták a válaszokat a pár tucat kérdésre, hogy hová kell kattintani és mit beírni, a papírt aztán betették a fiókba és azóta is vígan küldik ezerszáma a ki tudja honnan lebányászott vicces ppt fájlokat.

Bocsánat, elnézést, sajnáljuk

2010.05.25. 12:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [usb kulcs](#) [ibm](#) [fertőzött autorun](#) [auscert](#)

Fertőzött USB kulcsokat osztogattak [az ausztrál AUSCERT konferencián](#) az IBM standján. Ez duplán is fájó, hiszen ez a konferencia éppen a kiemelt biztonságról, a kockázatokról, azok kezeléséről szólna, így ez egy abszolút nem várt esemény volt, a suszter cipője nem lehetne lukas.



Természetesen [elnézést kértek a kellemetlenségeikért](#). Ami érdekes, [hogyan az IBM-mel sem első esetben fordul ez elő](#), 2002-ben szintén egy USB eszközön volt egy ritka boot vírus fajta, és az AUSCERT is hibázott már, legutóbb [2008-ban](#). Akkor a Telstra által osztogatott USB kulcsok voltak szintén fertőzöttek.



A havonta megjelenő számítástechnikai újságok CD/DVD lemezmellékleteinek tisztasága hasonlóan kényes és fontos kérdés. Itt általában több, különböző gyártótól származó biztonsági termékkel is rendszeresen átfésülik az anyagokat a lemez gyártásba adása előtt. Még így is előfordult Magyarországon, hogy például a [Chip Magazin 1997 júliusi száma fertőzött volt a magyar HDD Cleaner-rel](#), emlékszem, [ezt akkor még](#) a Déli Krónikában is bemondták.



És volt egy másik régi PC Guru eset is, ahol pedig a BIOS-t felülíró hírhedt [CIH vírus példányai szerepeltek egyes fájlokban](#). Szerencsére ezek az esetek ritkák, de hasonlóan a hibás vírusadatbázis frissítésekhez, [még egy is túl sok](#) belőlük.



Az ilyen fertőzött eszközök osztogatása rámutat arra, hogy [biztosan elmulasztották az ilyenkor szükséges vírusvizsgálatot, az elvárható legnagyobb gondosságot](#). Mert ha lett volna egyáltalán előzetes ellenőrzés (még ha nincs is 100% védelem, és valamilyen speciális, vadonatúj kártevő esetleg átment volna a védelmen), akkor sem úgy kommunikálják, hogy "bármelyik antivírus felismeri".



Szemléltetést itt nem valamilyen zseniális vadonatúj kórokozóról van szó, hiszen akkor nekik is ugyanilyen könnyen észre kellett volna venni bármelyik antivírussal, ha valóban megnézték volna. És tulajdonképpen ez az igazán sajnálatos momentum ebben a történetben.



Az USB eszközökre, és [az Autorunos kártevők rendszeres "jó" havilistás szereplésére](#) visszatérve pedig hozzáállhatunk úgy is, hogy **ahogy töltetlen fegyver a lőtérén sosem létezik**, úgy Windows alatt ártalmatlanul indítható USB kutyü sincs. Ellenőrizni mindig kell, bárkitől is kapjuk, és [a full autorun letiltása a választható legjobb túlélési stratégia](#).



Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2029540>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Kattintare necesse est

2010.05.27. 13:50 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [google trends tanulmány est noscript mérgezés találat kattintare necesse](#)

Azt már eddig is láttuk, hogy a Google keresések búzája között sok lehet az ocsú, meg hogy ez korántsem a véletlen műve. Korábban csak alkalmilag, kiemelkedő katasztrófák, [hírességek vélt vagy valós halálhíre](#), Valentin nap, sportesemények megrendezése esetén került sor tömeges link mérgezésre, de [mára ez a foglalatosság állandó jelleggel](#) ipari méretekben veszélyezteti a netezőket.



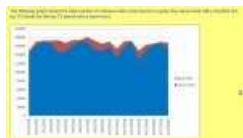
A [Symantec végzett egy felmérést](#), amiből az derült ki, hogy **szervezettebb és automatizáltabb ez a jelenség, mint azt korábban gondoltuk volna**. A háttérben gyaníthatóan a [hamis antivírus programok fejlesztői](#) állhatnak, erről tanúskodik az az adat, miszerint az első 70 találat körülbelül 68 százaléka vezet kártékony oldalakra, és [ezek szinte mindig az emlegetett pánik programokat tartalmazzák](#). Nem kell vulkán, nem kell Storm Worm, Eurovíziós dalfesztivál, NHL kupa, ezektől teljesen függetlenül **állandó jelleggel folyik a Google trends monitorozása, automatizált kihasználása**.



A vizsgálatok eredményei, melyet a Google márciusi és áprilisi találatai alapján végeztek azt mutatták, hogy a napi aktuális top 10 keresőszó alapján indított keresések eredményei közül mindig volt legalább 3 olyan, ahol kártékony linkekre mutattak az oldalak.



[Átlagosan az első 70 találat közül 15 tartalmazott kártékony oldalra irányító URL-t](#), ami nem kevés, de **bármely napon is vizsgálták, legalább 7% mérgezett találatot mindig észleltek**. Nyilván amikor **kiemelkedő érdeklődésre számotartó esemény** - pl. az Ikeás dohányzóasztal nevű Eyjafjöll vulkánkitörés van, akkor magasabbak a számok.



És az idő faktor is igen lényeges, **valószínűleg a kártévő terjesztők sokkal gyorsabbak, és amíg a Google gépezet szűkebb keresztmetszet**, a lassú víz partot mos effektussal [le is tiltja a linkek egy részét](#), addigra már régen más újak vannak a nyitó oldalakon. Tehát ez egy Neverending Story állapot, ami idővel lehet még rosszabb is.



Keresni azonban mégis kell, mit lehet hát akkor tenni? Ebből a nagy tanulság csak az lehet, hogy **a kereső találat nem Szentírás**, a józan paraszti eszünket, alaposágunkat, figyelmünket ekkor se kapcsolhatjuk takarékra, legyünk résen.



Segíthet **a találat linkjének szemrevételezése is** (mint a piacon az almáé, lehet gyakorlatot szerezni ebben is ;-), például nyilván nem egy kínai oldal tájékoztat majd a legautentikusabban Johnny Depp haláláról, ez is elég egyértelmű. De emellett utunkon hasznosnak bizonyulhat

egy megbízható antivírus fegyverhordozó, valamint NoScript nevű hűséges ebünk.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2034924>

Kommentek:

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

[mikka 2010.05.27. 17:35:22](#)

Nos...ez egy nagy baromság mar megbocsass :)
Nem kell faszságokat keresgelni..

[tippan 2010.05.27. 17:37:40](#)

Hát, nem tudom.
Sokat keresek, sokfelé megfordulok, de sem a céges, sem a magán gépemen nincs ilyen problémám.
Persze, aki azért vesz új tv-t, mert foci vb lesz, annak bármit el lehet adni :-)



[kilobike 2010.05.27. 17:40:06](#)

Van pár ellenszer:
Részemről AVG linkscanner, egész elfogadhatóan szűr.
Aztán nem vagyok zombi, (igen, a piacon is megnézem az almát),nem kattintgatok összevissza.
Aztán még van pár összetevője. Meg lehet ezt tanulni.
(Olyan ez, mint átmenni egy forgalmas úton. Vagy megtanulsz körbenézni, és átkelni, vagy szarrá gyúrnak.)

[koljano1 2010.05.27. 18:06:16](#)

mikka! Nem csak faszságok keresése közben lehet ilyenbe belefutni!

És ha valaki arra a kérdésre, hogy milyen böngészőt használ, azt mondja, hogy Google-t (és nem a Chrome-ot érti ezalatt), az vajon ideális célpontja-e az ilyen támadásoknak? Vagy tudna-e internetezni NoScript-tel?



IPG 2010.05.30. 01:00:22

Firefox WOT-kiegészítő is hasznos segítség, AVG linkscanner szintén, valamint a noscript alap :)

URL ellenőrzési weboldal indult

2010.05.31. 21:00 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [google filter link url szűrés kártékony](#)

Többször volt szó már [a bejelentett támadó webhelyek kapcsán](#), hogyan is [próbálja szűrni a temérdek kártékony linket](#) a Google. Most ehhez a harchoz csatlakozott egy külön weboldal elindításával egy antivírus cég is.



Az F-Secure [elindította a Browsing Protection](#)-nak nevezett oldalát, ahol [bármilyen URL vizsgálatát](#) elvégezhetjük. Megnézegettük néhány linket, és **talán gyorsabban reagáltak a Googlenél**, az orosz kártékony oldalra mindenesetre máris riasztott.



Több antivírus termékben működik már kártékony linkeket nyilvántartó adatállomány, többek közt a **NOD32** is tartalmaz ilyen.



A jövő [várhatóan a kereső cégek és az antivírus gyártók közös adatbázisán](#) alapuló szűrés lehet, **így biztosítható lenne a védekezéshez szükséges egyre rövidebb** reakció idő.



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2044653>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Kártékony antivirus linkek - villám őrjárat

2010.06.01. 13:20 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

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

Nemrég olvashattunk egy újabb súlyos adatot, hogy egy ukrán-svéd-amerikai **hamis antivírust terítő nemzetközi bűnbanda 22 millárd forintnak megfelelő összeget keresett**. Egyfajta röpke "Link Patrol" keretében teszünk majd időnként kisebb őrjáratot hamis vírusok, a hamis antivírust terítő linkek nyomában, különösebb sallangok, terjedelmesebb tiszteletkörik nélkül.



Mai áldozatunk az **RTS Antivirus 2010**. A domain [idén márciusi ukrán bejegyzésű](#). A hamis vírus telepítő csomagja ezúttal egy .MSI kiterjesztésű állomány, [amelynek Virustotalos](#) vizsgálata is egyértelműen mutatja, [kártékony programmal van dolgunk](#).



Az elnevezésbeli rövidítősdi mostanában jött divatba, [ez a hamis program az "AKM Antivirus 2010 Pro" utódjának tekinthető](#). A weblapon **minden jellemző árulkodó jegy megtalálható**: hamis ajánló emblémák, hamis köszönő levelek nem létező felhasználóktól, VISA és MasterCard bankkártya elfogadás, üvegszerű látványos ikonok.



Zárni minden villám őrjáratunkat egységesen ezzel az okossággal fogjuk: **"Soha ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google szinte összes találata „How to remove...” szófordulattal kezdődik."**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

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

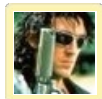
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2047406>

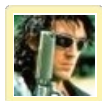
Kommentek:

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



[Yann Le Pentrec](#) • <http://lnk.bz/t7c> 2010.06.02. 14:50:09

OMG, 22 milliárd forint! De ha bebizonyosodik a csalássorozat, annyit fognak ülni, mint varjú az ágon. Az amerikai jog tényleg nem lacafacázik, ha esetenként 20 évet dobnak fel valóban... A szoftverrel kapcsolatban: most mondjam, hogy meg is érdemli, aki ilyen noname szemetet telepít fel? Nem mondom, mert nem mindenki ért pro módra a számítógéphez, sőt: rengeteg olyan ember használ gépet, aki nem is akar hozzá érteni, csak munkaeszköz vagy ilyesmi.



[Yann Le Pentrec](#) • <http://lnk.bz/t7c> 2010.06.02. 15:09:44

Ja, ahogy így utólag látom, írtál is ezekről a userekről a Hogyan lehetne mégis segíteni nekik? bejegyzésben. Tehát jogos a probléma, ha én is ugyanarra a következtetésre jutottam egy másik megközelítésből. :)

[nyos](#) 2010.06.05. 17:19:41

"Soha ne használjunk és ne telepítsünk olyan programot, amelyre rákérsva a Google összes találata „How to remove...” szófordulattal kezdődik."

Jo gondolat.

Kiváncsiságból rákerestem fordítva: mik azok a programok, amikre a "how to remove" kereses talalatot ad.

3. talalat a WGA. Kartekony, nem vitas. (XP SP2 is az elso oldalon van)

Feltört postafiók - instant remedy

2010.06.03. 15:10 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [feltörés](#) [okok](#) [postafiók](#) [teendők](#)

Már a Sarah Palin esetről is látszott, [nem szükséges a Yahoo-t vagy a Gmailt feltörni ahhoz](#), hogy valakinek a postafiókjába mégis be lehessen jutni. De legyen bármi is a módszer, [mit tegyen az, aki gyanítja, vagy éppen biztos benne, hogy a levelezését feltörték?](#)



A biztonsághoz való megfelelő hozzáállás az, hogy biztos információ nélkül, már pusztán gyanú esetén is úgy járjunk el, mintha biztosak lennénk a kompromittálódásban. Az okok keresésében és a teendők megválasztásában az alábbiak talán segíthetnek.

- az érintett szolgáltató azonnali értesítése (pl. Gmailnél Google) az incidensről. Később az ő rendszer naplói segíthetnek majd a tisztázásban, felderítésben is. Ilyen esetekben a szolgáltatók igyekeznek mindent megtenni, és segítőkészek.



- használtam-e másik postafióknál, webes szolgáltatásban ugyanazt a jelszót? Mert ha igen, gyakori forgatókönyv, hogy egy jelszó megszerzésekor végigpróbálgatják az illető egyéb levelező, csevegő, webes, ftp eléréseit - és gyakran nem eredmény nélkül. Ha igen a válasz, akkor a feltört helyszínen mindenképpen, és az esetleges megegyező jelszavú helyeken úgyszintén azonnali jelszó csere szükséges.



- használtam-e túlságosan beszédes, könnyen kitalálható jelszó emlékeztető kérdést? Ha igen akkor azonnal meg kell változtatni. Ha esetleg ezzel egyező jelszó emlékeztető kérdés van másik helyszínen, akkor azonnal azt is változtatni. Már a Sarah Palin email fiók feltörési esetről látszott, nem célszerű ész nélkül minden személyes adatot túlzottan kiplakátolni a közösségi oldalakra. Mi is volt ott a probléma? [A módszer nem feltörés, nem jelszó találgatás volt, hanem új jelszó igénylése.](#) A születési hely és idő megszerzése nem okozott gondot, a titkos ellenőrző kérdés pedig az volt, hol ismerkedtek meg a férjével. Az ismert és kevésbé ismert embereknek komolyan el kellene gondolkodniuk, érdemes-e olyan adattal védeni bármit is, amit a bulvárlapok lapok hetente megírnak, vagy valaki önként kiplakátolja az IWTW-es lapjára.



- Használtam-e a jelszavamat nyilvános helyen: kávézóban, hotspoton, [kileszette-e valaki a vállam felett?](#) Találtam-e a kocsim mellett (direkt-véletlenül nekem csalinak odahelyezett) USB kulcsot, vagy egyéb eszközt, amit a gépembe később bedugtam? Ha bármelyik igen, érdemes a jövőben ezekre kiemelten figyelni.

- Adatvagyon leltár felmérése. Milyen bizalmas adatok voltak a levelezésben, amik ha illetéktelen kezekbe kerültek, bajt okozhatnak? További szolgáltatásokhoz, munkahelyi elérések belépő jelszavai, partnereinkkel folytatott levelezések, magánéleti dolgok, amiket nem szívesen látnánk a szanalmas.hu vagy a kreten.hu oldalakon. Teendő lehet a levelekben szereplő összes account haladéktalan megváltoztatása, fontosabb üzleti partnerek figyelmeztetése, ismerőseink, rokonaink, barátaink értesítése, hogy postafiókunk áldozatul esett, és ha x-től - y időtartamig a nevünkben levelet kaptak, ellenőrizték le annak tartalmát velünk külön egyeztetve. [Itt az elkövetők például a tulajdonos Propeller.hu nevében beadtak egy törlési kérelmet is a Google-hoz.](#)





- Ha **bankkártya** számok, **elektronikus fizetés** adatok is szerepeltek, akkor a banki egyenleg, tranzakciók azonnali vizsgálata a kétes időszakra. Ugyanez vonatkozik a [fizetés online játékokra](#) is, [például World of Warcraft, és hasonlók](#).

- **Feljelentést tenni a rendőrségen az ügyben.** Indokolt esetben mind a Google központjától, mint az érintett IP cím aktuális felhasználójának internetszolgáltatótól való kikérése megtörténhet a nyomozás folyamán.



- Beléptünk-e bármilyen webes levelezésbe, szolgáltatásba, és **kipipáltuk-e az "Emlékezz rám" vagy a "Maradjak belépve" idiótikus opciókat?** Ha igen, üssünk a kezünkre ;-)

- És érdemes lehet **egy alapos vírus és kémprogram ellenőrzést is tartani** a biztonság kedvéért.



Végül imádkozni, hogy ne legyenek további kellemetlenségek, és [megfogadni szent esküvéssel az erős jelszó használatát](#), **mindenhol másikat alkalmazni, és ezeket rendszeres időközönként cserélni**, valamint [Facebook, Iwiw, Myspace profilunk átgondolását](#) a jelszó emlékeztető kérdésekkel kapcsolatban, [fokozott óvatossággal viselkedni a jövőben](#). Legvégül pedig inni egy White Russian az izgalmakra...



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



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2051832>

Kommentek:

Nincsenek hozzászólások.

A jó név felsiker

2010.06.07. 12:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam](#) [jelszó](#) [twitter](#) [trójai](#) [center](#) [reset](#) [protection](#) [safebrowser](#)

Nem véletlenül hívják az akció hősokeket John Rambonak, John Matrixnak, Joe Armstrongnak, Max Headroomnak, Rocky Balboanak vagy Tony Starknak. A sok pörgő, kemény mássalhangzót tartalmazó, "beszélő" nevek már előre sok keménységet sejtetnek, és egyértelműen pozitív töltetük van.



És semmiképpen nem nevezik őket Fülölaj Emmánuelnek vagy Mukinyúl Balambérnak. A jól csengő névválasztás felsiker nem csak egy mozinál, de az élet minden területén, és így van ez a megtévesztő alkalmazások világában is.



Sorjáltak itt már korábban [XP Antivirus 2008, 2009, 2010](#) és hasonló nevek, [ekéztük is őket már sokszor](#), de úgy tűnik nem elégszer. [Most a Protection Center Safebrowser hívó szavak mentén indult](#) egy újabb spam hullám a Twitter tagok felé, és tegyük a kezünket a szívünkre, ki ne akarna a gépére egy igazi Protectiont, ami ráadásul Center is, sőt állítólag még a Safebrowserekkel is valamiféle távoli homályfedett rokonságban van, pláne ha mindezt a Twitter Team kínálgatja túlsorduló szívéllyességgel? Valószínűleg csak az, aki már tudja, mi is ez pontosan.



A hamis jelszó emlékeztető, pontosabban [jelszó kinullázásra buzdító kértelen levél](#) érkezett nagy számban (55 ezer) az utóbbi napokban. Aki figyelmetlen, és rákattint a gálánsan felajánlott linkre, letölt magához egy password.exe trójai állományt, amely megfelelő vírusvédelem hiányában le is fut, és mint hamis internet biztonsági csomag tengeti szánalmas életét gépünkön. Az idők szavára hallgatva már nem holmi ósdi, őskövület "xxx trójait találtam, yyy vírust fertőzés a számítógépen" avitt szlogeneket sütögeti csak el, hanem "modern világ, italunk Pepsi" jegyében a jelentősen korszerűbb, tudományosan hangzó "Network intrusion detected", meg "Attack from XXXX IP cím" is megjelenik a képernyőn.



Ami jelentősen megkülönbözteti az eddigi pánik programoktól, hogy az ottani légből kapott, kamu riasztásokkal szemben itt valódi kártevőket is megjelenít az áldozat Asztalán, amire aztán "hitelesebb" álriasztásokat tud produkálni. Ez valljuk be, már egy újabb lépcsőfok az evolúciós harc történetében.



Jó látni, hogy a hamis antivírus programok fejlesztői [mennyre kreatívan](#) és [hangyaszorgalommal tüsténtkednek](#). Végülis [a Facebookon már megvolt ez a mutatóvány](#), és semmi nem indokolta, hogy a Twitter felhasználók bármilyen versenyhátrányba kerüljenek ;-) és eléggé el nem ítéhető módon kimaradjanak az ilyen esetekből - így végül nem kell majd tiltakozó nagygyűlést szervezniük az Egyenlő Bánásmód Hatóság székháza elé.



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2062281>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Deaktiválták a Facebook hozzáférésünket

2010.06.09. 17:30 | [Csizmazia István \[Rambo\]](#) | [14 komment](#)

Címkék: [spam facebook login kínai account adathalászat gyógyszerész](#)

Ám áldott szerencsére kaptunk erről egy tájékoztató emailt, melyből kiderül, hogy nem is akkora nagy a baj. Hurrá!



Ha a megadott linken bejelentkezzünk a régi név-jelszó párossal, akkor reaktíválják számunkra, és továbbra is használhatjuk a régit. Minderre a Facebook Csapata által írott levél a garancia. Vagy mégsem?



Először is nézzük meg a levél fejlécét, és vegyük észre, hogy jó, nem is a Facebook küldte. **Claudia von Huberspritz** küldi valamilyen **német végződésű címről**, és a levél továbbítását egy amerikai levéltovábbító szerver végezte.



Szándékosan hagytuk a második pontnak a gondolkozzunk opciót, **vajon létezik-e akkora marha szolgáltató, hogy nem vadonatúj jelszót választat velünk, hanem a régit erősített meg?** És vajon miért kell neki a régi is, mikor az úgyis ott van nála rossz esetben clear textben, jobb esetben hash lenyomatban, mégjobb esetben salted hashben.



Thunderbird a gyengék fegyvere, már **a levél kinyitásakor jelez, ez az üzenet becsapós lehet**. Nyilván érzékeli a megjelölt és valódi feladó közti ellentmondást, emellett a href linkek körüli katyvaszt is gyanúsak látja, és talán arra is pontoz.



A készítők nem bíztak semmit a véletlenre - kattintja ez vagy nem kattintja - adnak bőségesen választási lehetőséget, hármat is. Az első mindjárt a fentemlített **reaktíváljuk Facebook tábornokot, de van egy külön "Sign in" és egy "leiratkozás az ilyen idiótikus levelekről" is**. Ezek sorrendben a `hxxp://auto-insurance-company.org / africans.html`, a `hxxp://1perhousehold.com / certifiable.html`

valamint a hxxp://a3030.com/unselfish.html.



Lassúak voltunk, ezek közül **mi már egyiken sem találtuk meg az eredeti phishing oldalt**, helyette ezúttal a már jól ismert - egyáltalán nem afriakai - fehérköpenyes gyógyszerész bácsi mosolyog szélesen és derűs tekintettel a szemünkbe kínai webes patikája ajtajából ;-)



Sajnos szinte **biztos, hogy voltak azért jópáran, akiknek a mutatóujjuk gyorsabb volt az eszüknél.**

 Tetszik  17 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/2068351>

Kommentek:

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



[morrisal_](#) • www.plafoncsapszeg-gyalu.com 2010.06.09. 22:21:18

a gmail volt olyan kedves és kiírta egy vörös sávba, hogy vigyázzak, mert elképzelhető, hogy nem az a valódi küldő, aki annak van feltüntetve. ja, és eleve a spam mappába tette be, aminek a tartalmát én gyakorlatilag gondolkodás nélkül törölöm. eleve naponta kismillió értesítést kapok a FB-ról, ugyan mibánatért rakná a spam-mappába? szóval gyanús volt eleve, na.

[wan2bee](#) 2010.06.10. 03:06:49

kurvara senki nem kíváncsi a facebookodra.. tolem uj jelszot es a 13. macskam nevet kerte..



[romesz](#) • <http://romesz.blogspot.com/> 2010.06.10. 05:37:38

mikor leiratkoztam a Facebookrol akkor elve kiírta, hogy barmikor visszamehetek a regi felhasznalo nevemmel es jelszavammal.

Kulonben en ilyen leveleket ki sem nyitok. Neha benezek a junk levelek koze de csak azert, hogy nehogy elveszitssek valami fontos levelet.

A facebook meg a nigeriai ozvegylet levele nem tartozik a fontosak koze.

[mbazs](#) 2010.06.10. 07:50:36

A cleartext-es eset egyébként létezik.



A "hotdog.hu" nevű csodálatos (azaz kurva gagyi) tiniknek szóló oldalra regelttem egyszer már a franc tudja miért. Néhány hónap múlva volt valami (már nem emlékszem), és a jelszót elküldték egy az egyben a mailmre. El is küldtem őket a kurva anyjukba a "jól fejlett" biztonsági rendjükkel. Jelszót clearben tárolni? Rohadjanak meg mind az ilyenek.



Szpájk 2010.06.10. 09:00:08

Gyanítom, hogy off, de mi a fasznak egyáltalán bárkinek fbook?
Meg az összes ilyen szar?
De tényleg, minek?
Az /normális/ ember társas lény, offkorz tehát magányra vágyik.
Sztem.

nál 2010.06.10. 09:03:53

@Szpájk:

Mi a fasznak ilyen baromságot kommentelni?

Értem én, hogy nincsenek barátaid, és valami interakcióra vágysz legalább az online környezeteddel, de totálisan felesleges feltenni ilyen kérdést, főleg úgy, hogy magadban már meg is van a válasz.



TROLL 2010.06.10. 09:30:19

Hehehe, az oldalt lájkolni se lehet :)



Szpájk 2010.06.11. 08:16:17

@nál: Vicces, de ennek ellenére vannak barátaim, pont amennyi elég, viszont inkább élő interakcióban szoktuk tartani a kapcsolatot.

Valahogy szórakoztatóbb.

A net csak szarakodásra jó, mint pl. a kommentelés, igaz arra nagyon.

Abban viszont igazad van, hogy a saját válaszom már megvan, csak érdekelt a másé is.

nál 2010.06.11. 11:35:50

@Szpájk:

Nem, téged nem érdekel más válasza. A fenti kommented inkább provokáció, trollkodás. Ha érdekelne, akkor azt kérdeznéd, "ti mire használjátok a Facebookot?" és nem azt, hogy "mi a fasznak egyáltalán"...

Ha pedig te tényleg csak szarakodásra használod a netet, akkor nem érdemes előfizetned.



Szpájk 2010.06.12. 12:36:13

@nál: Azt gondold nyilván, hogy jobban tudod nálam, engem mi érdekel, és mi nem, de ez epic fail a részedről.

Aztán; a hozzászólásom azért nem trollkodás, mert végül is a témába vágott.

Troll úr hozzászólt a kommentem alatt, és csak egyet érteni tudok vele.

Valamint szerintem a stílisztikától eltekintve mindegy, hogyan teszek fel egy kérdést, a lényeg a válasz lenne.

Ami nem volt.

Szóval, "Ti mire használjátok a fbook-ot"?

Mert a spanjaim meg a haverbigék állandóan meghívót akarnak nekem küldeni, hogy menjek velük farmolni és lehetünk ott szomszédok, meg ilyesmik.

Erre meg mondtam nekik, hogy elképzelhető, hogy az életben egy nagy paraszt vagyok, de ennek ellenére sem kívánok virtuálisan répát vetni és hasonlók.

Az arcukat meg naponta látom, nem akarom a képernyőn is.

Szarakodás alatt meg értem azt, hogy itt szájkaratéunk sok témában, de a világot ez nem fogja semmilyen fronton megváltani, vagyis végül is értelmetlen szarakodás, bár jól esik.

És megint szavakon lovagolsz.

A netre meg nem én fizetek úgymond "elő", mert ilyet nem tennék sosem.

Túl lusta vagyok.

Elnézésetek kérem, amiért ilyen hosszúra nyúlt ez a betűfolyam.

Tisztelettel maradok.

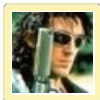


Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.06.12. 14:00:44**

Szia Szpájk!

Nekem tetszett a kommented, ez a legutolsó pedig 10/10 :-D

Én is maradok tisztelettel :-)



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.06.13. 22:04:34

Azért ez se rossz, épp most lőttem: lnk.bz/tNc

A Thunderbird itt is megmutatja az igazságot, még mielőtt nagy igyekezetemben megadnám a (nem létező) WoW accountomat a tolvajoknak. :)

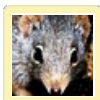


Szpájk 2010.06.19. 12:54:51

[@Csizmazia István \[Rambo\]](#): Nagy vonalakban ez az őszinte véleményem a témáról, jobban belemenni felesleges. Örülök, ha tetszett.

Ha úgy adódik, később is visszatérhetnél a témára, mert ez akkora szar, hogy többször kell ellapátolni...:))

Üdvözlettel maradok.:)



dibbler 2011.11.18. 16:06:12

A FB, IWIW vagy akár a blog, kommentelés forradalmian új dolog. Minek facebookozni? ugyanolyan kérdés mint minek autózni (mondjuk 120-al) vagy minek repülni ...

Csalók és hiszékenyek pedig mindenütt vannak, ami kellene már az a közérthető, nemzetközileg elfogadható jogi szabályozás. De legalább ajánlás.

Nem tudom, hogy pl. az Unesco foglalkozik-e az emberiség internetes kultúrájával?

A labda kerek, de a bitek szögletesek

2010.06.11. 12:55 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [foci vb online fogadás figyelem csalás 2010 adathalászat](#)

Indul a [2010-es foci világbajnokság](#), és a sportok szerelmesei, a rendszeres vagy alkalmi fogadók is lázban égnek. Következzen néhány jó tanács, mire érdemes vigyázni az online fogadásoknál, hátha jól jön.



[Minden jelentős esemény jó alkalom a kártevőterjesztőknek, bűnözőknek](#), ezért ezer százalékgig [biztos, hogy labdarugó VB-t is megpróbálják majd kihasználni](#). Sőt, nem jövő idő ez egyáltalán, hiszen korábban már [olvashattunk a jegyek hamisításáról](#), és biztos, hogy a csalók sokféle módon igyekeznek majd pénzhez jutni. [Megpróbálunk pár tippet adni az online fogadásokhoz](#), persze [nem az eredményekhez](#), hanem az adatvédelem szempontjából.



- mindig [ellenőrizzük le az online fogási oldalt, hol és kik üzemeltetik](#), legális-e, [rendelkezik-e érvényes üzemeltési engedéllyel](#), megbízható-e - például a Googleban keressünk rá. Ha nem az átvért áldozatok panaszáradatát látjuk hatvan oldalon keresztül, az már esetleg lehet egy biztató jel.



- ha már a belépéshez sem biztosítottak HTTPS elérést, felejtjük is el. SSL nélkül az adataink clear textben utaznak, [mukinyulas szolgáltatókkal nem érdemes pénzügyekbe kezdeni](#).

- [gondoljuk át előre, mire mennyit teszünk, illetve az mivel jár a legjobb és a legrosszabb esetben](#), tehát pontosan mennyi lehet az esetleges nyereség, illetve mennyit veszünk.



- válasszunk olyan [fogadó irodát, amelyik erős hitelesítést nyújt](#), ezt egyfajta pozitív biztonsági garanciának is tekinthetjük.



- nézzük meg, [van-e adatvédelmi nyilatkozat](#). [Ha egyáltalán nincs, akkor nem is érdemes több szót vesztegetni az oldalra](#). Ha van, olvassuk át, pontosan mit írnak, [mit vállalnak, személyes adatainkat kiadják-e harmadik félnek](#), stb.



A felhasználói szerződést egyébként [mindig el kell olvasni, ha csak az ember nem akarja eladni a lelkét :-\)](#)



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Akiknek a Captcha kínszenvedés](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2073559>

Kommentek:

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



[TROLL 2010.06.11. 14:13:44](#)

A poszt jó mint mindig, de az istenért, hogy lehet egy jel-nem jel, frekvencia vagy amplitúdó eltérés, stb. szögletes :D ?



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu>](#) [2010.06.12. 14:05:14](#)

Szia TROLL!

Kellett valami ellentét pár, me aztán a labda nem is kerek, hanem gömbölyű, kivéve a fogadási maffia mást rendel meg, szóval ennyiből lehet az egyes szögletes, a nulla meg ... ne firtassuk.

Kedvenc bites sztorim az volt, mikor valami berhelt soroskábeli norton commanderes másolgatásnál két gép között, szedett vedett sodorgatott drótokra gondolj, egy kolléga arra jött, hajtogatott fehér papírból egy hamutálcaszerűséget, alá tette, és rajzolt bele tollal egy csomó egyest meg nullát, amik ugye kihullottak :-)

Foci VB és a kártevők

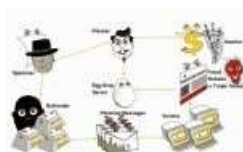
2010.06.14. 11:25 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam vb adobe pdf 2010 kártevő exploit](#)

A [múltkori posztban](#) inkább csak az online fogadással kapcsolatosan kérdésre fókuszáltunk, de természetesen - és sajnos - nem maradt el az eseményt felhasználó egyéb kártevői tevékenység sem.



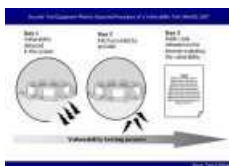
Dancho Danchev számolt be róla, hogy [az Adobe egy nulladik napi sérülékenységet kihasználó exploitot tartalmazó weblapra](#) irányítják az áldozatokat. A fertőzési módszerről a [Websense is kiadott már egy videót, melyet a YouTube-on](#) is megnézhetünk. A kártékony HTML oldal aztán dolga végeztével továbbít minket egy hamis gyógyszerész oldalra, valószínűleg azért, mert mind a két kampányt ugyanaz a bűnözői kör menedzseli.



Ugyancsak érdemes átgondolni, ha arról [kapunk kéretlen levelet, hogy olcsó vb jegy áll rendelkezésünkre vagy éppenséggel nyertünk](#) a foci vb lottón, vagy látszólag maga Beckham lesz a követőnk váratlanul a Twitteren.



De [ilyenkor gombamódra szaporodnak a hamis weblapok is](#), melyek [a megtévesztést szolgálják](#), végcéljuk pedig a megfertőzött gépekről megszerezni a személyes, jelszó, banki, stb. adatokat.



Az pedig már csak pusztá mellékhatás, hogy [a Twitter rendszere vajon bírni fogja-e az eddigi napi 55 millió poszthoz képesti megemelkedett üzenetszámot](#), vagy esetleg összeomlik.



Mindenesetre mi igyekezzünk megóvni magunkat a hasonló spamektől, csalásoktól, kéretlen PDF-ektől, fertőzésektől, illetve ezek helyett kattintsunk inkább a TV távirányítón ;-). És ha nemzeti csapatunk nem is került be a résztvevők közé, örüljünk ezúttal annak, hogy [nem olyan országba születünk, ahol pusztán a VB meccsnézés miatt halál jár](#).

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás



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 adathalászattal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2080173>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Én csak okosan netezek. Nyerghhhh!

2010.06.16. 14:40 | [Csizmazia István \[Rambol\]](#) | [8 komment](#)

Címkék: [spam](#) [javascript](#) [twitter](#) [kártevő](#) [exploit](#) [obfuscated](#)

Az "én nem látogatok x, y, z oldalakra, tehát biztonságban vagyok" mítosznak **már réges-régen vége**. Persze mondhatja valaki, aki valóban okos, az közösségi oldalakra sem regisztrál. Viszont Twittert sokan használunk, sokan olvasunk és az alábbi **trükk teljességgel demokratikus**, miszerint a sors által kiporciózott észmennyiségtől függetlenül igyekszik megfertőzni a számítógépeket.



A régi "ha kevés az eszed, legyen noteszed" mondás helyett inkább **a legyen NoScripted lenne a helyes megközelítés**. Lássuk, miért is. A Trend Micro blogjában figyelmeztet - és nem is először - [olyan kártékony Twitter üzenetre, melynek Javascript kódja lefutva kártékony weboldalakra továbbít](#). Az emberek általában sokkal jobban megbíznak egy közösségen belüli üzenetben, mint egy "szedett-vedett" emailben, de [erre még akkor sincs okunk](#), ha az látszólag ismerőstől jött.



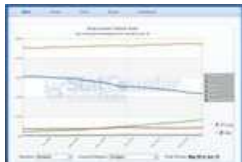
Persze az ilyen üzenetek [folyamatosan érkeznek](#), és a [korábbi Gazai incidens](#) na meg [a futball VB is megadta-megadja az apropót](#) és az alkalmat hozzá.



Maga a javascript szándékos összezavarása szinte ellentétes a jó újságíróra vonatkozó elvárásokkal: "Aki 10 mondatban mondja el azt, amit ötben is lehet, egyéb gazemberségre is képes!". Kevésbé frappánsan, de vonulatilag ezzel analóg módon "Aki 100 zavaros Javascript sorban programozza le azt, amit olvashatóan ötben is lehet, az egy sutyerák."



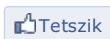
Aki okos, az inkább EXE vagy PDF mellékletre nem kattint, ha már mindenféleképpen muszáj valamilyen alaptételt felállítani és idecitálni. [Nagyjából már hetvenötezerszer javasoltuk a Noscriptet](#), így hát ehelyett vessünk most egy pillantást a magyar böngészőhasználati szokásokra.



Az Internet Explorer szelete bár látványosan csökkent, de **láthatóan még mindig masszív negyede a felhasználóknak** esküszik rá, és a vezető Firefox esetében is élhetünk a gyanúperrel: **valószínűleg csak egy kicsi hányad** lehet az, aki **pluszban válogatott biztonsági pluginokkal jól felszerelve**, bemosakodva lép ki az internet országútjára.



Védelmünk érdekében a **biztonságos böngésző környezet mellett** érdemes lehet azt is ellenőrizni, beállítani, tesztelni, hogy a vírusvédelmi programunk valóban blokkolja-e az ilyen kártékony linkeket. Ha igen, akkor van akváriumunk ;-)



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



Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2085488>

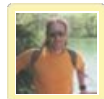
Kommentek:

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



wmiki • <http://apostolimagyarkiralysag.hu/> 2010.06.17. 09:46:17

melyik a legjobb vírusirtó?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.06.17. 16:12:48

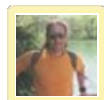
Szia wmiki!

Ez kb. olyasmi, mint hogy milyen nő az ideális feleség? Szőke, barna, fekete, jól főz, jól mos, jól takarít, alacsony, magas, ésatöbbi részlet ;-)

Eredeti kérdésedre a jó válasz szerintem májusi Chip újság 54. oldalán szerepel, és pont ez a cikk címe is. Érdekes elolvasni, nem hosszú, de ha esetleg nem férsz hozzá, itt a válogatott lényeg: legyen komplett internetbiztonsági megoldás (ne csupán szimpla vírusirtó), a szakmailag (AMTSO által elismert) teszteken szerezzon rendszeresen jó eredményeket, legyen könnyen kezelhető, ne okozzon sok vakriasztást, legyen hatékony, legyen hozzá jó support és a legfontosabb: neked tetszen.

Ha magánembernek kell, érdemes néhány cég próbaverzióját letölteni, és az adott 30 napig ingyen tesztelni: kényelmes-e, jól kezelhető-e, megfelelően működik-e, stb.

Ha ugyanezt egy cég kérdezi, akkor már további szempontok is beléphetnek: lehet-e központilag frissíteni, távmenedzselni, távtelepíteni, több platformra is van-e megoldás, etc.

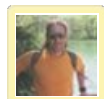


Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.06.17. 16:15:03

Látod milyen diplomatikus voltam, nem írtam rögtön csuklóból, hogy a NOD32 az :-D

pobeda 2010.06.17. 17:36:54

@Csizmazia István [Rambo]: ESET Smart Security :))



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.06.17. 18:21:55



@Pobeda:
Hát ja :-)

További kérdés lehetett volna még: melyik a legjobb sörálátét méretű adóbevallás?

A Kretén Magazin egyszerűsített adóbevallása, mely 2 pontból állt:

1. Mennyi zsét kerestél tavaly?
2. Na akkor tedd be a borítékba, és küldd el nekünk.

Valakinyolc 2010.06.17. 19:13:25

A Security Essentials-ről vélemény esetleg? :)

Egyébként ezek a Twitteres spamok hasonlóak az Msn-es okosságokhoz, amikor az offline emberke rádír, hogy nézd meg a képeit és küldi a nem túl bizalomgerjesztő linket.

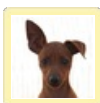


Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.06.18. 10:41:35**

@Valakinyolc:

Security Essentials-ről csak egy gondolat a minőségtől teljesen függetlenül.

Ha a gázai incidens jogosságát Izrael vizsgálja ki, ha egy rendőrkapitány maga jár el saját gyorsajtási ügyében, ha egy igazgató maga bírálja el etikusan járt-e el, vagy ha ugyanaz a cég fejleszt védelmi programot, aki a biztonsági réseket is "gyártja", az szerintem mind már eleve hendikeppel indul. A több szem többet lát, a külső kritikus kontroll jobban működik, és az AV cégek évtizedesnél is több tapasztalata szerintem sokat nyom a latba.



Jaffar 2010.06.25. 13:07:09

@Csizmazia István [Rambo]:

Ez mind igaz, viszont aki tényleg ért egy kicsit is jártas a dologban annak már nem is biztos, hogy kell vírusirtó. Nekem Security Essentials van most fenn, előtt 3 évig volt Kaspersky-m (eredeti ofc). A vírusirtó létszükséglete nagyban függ attól is, hogy mire használja a júzer a gépet.

Mennyi? 420 ezer. Mi 420 ezer? Miért mi mennyi?

2010.06.18. 11:40 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [internet brit bank felmérés csalás üzenet](#)

Egy friss brit tanulmány szerint elképesztő mennyiségű a kéréstlen levéláradat, az ezzel járó csalások, megtévesztések pedig egyre több kárt okoznak az óvatlan felhasználóknak.



Széles csövön ömlik a csaló üzenetek sokasága, az elmúlt egy évet vizsgálva óránként 420 ezer ilyen érkezik a szigetországi postafiókokba. A banki csalásoknál pedig mintegy 55 százaléka az üzeneteknek hivatkozott valamilyen közismert neves bankra, próbálkozott annak nevében.



A csalók emellett egyre emelkedő mértékben adják ki magukat valamilyen jótékony, adománygyűjtő szervezetnek is. Ugyancsak gyarapodó számú DNS eltérítéssel és keresőtalálat mérgezéssel találkoztak a szakemberek, de nőtt az olyan hamis ügyfélszolgálatok száma is, akik a bank vagy hivatalos szerv nevében telefonálva próbálnak érzékeny adatokat szóban kikérdezni.



Ami viszont igazán ijesztő, hogy a korábban kalkulált "csak" 5-10 százalékos viktimológiai ráta helyett a valóságban tapasztalt számok ennél jelentősen magasabbak voltak. A felmérés szerint már minden negyedik brit (25%) áldozatul esett adathalászati támadásnak, és egy átlagos pénzübeli veszteség 285 GBP, vagyis nagyjából százezer forint volt. Ebből pedig egyenesen következik, ha a támadási potenciál emelkedik, úgy a védekezés hatékonyságát is különféle megoldásokkal, eszközökkel és persze felhasználói programokkal, oktatással sürgősen emelni kellene.

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](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Ez történik a weben egy perc alatt](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2091044

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Álmában szendereg a robogás

2010.06.21. 13:10 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

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

Nincs érdemi változás a listán, a Conficker féreg már nyolcadik hónapja őrzi vezető helyét a magyarországi vírustoplistán, és **mellette az élmézőny első öt tagja változatlanul tartja pozícióját**. Mindössze egyetlen újonc trójai bírt felkapaszkodni, és az is csak nyolcadiknak. Ám ha menet közben váratlanul egyszer csak lekapcsolja a gépünket, akkor őt azért sokáig emlegetni fogjuk.



Az ESET minden hónapban összeállítja a **Magyarországon terjedő számítógépes vírusok toplistáját**, melynek elemzése tanulsággal szolgálhat a felhasználók számára. **Mintha megállt volna az idő, az első öt helyezett nem akar moccanni a helyéről**, talán odaragasztották magukat Palmatex-szel. Mindenesetre **a megtévesztésre utazó trójai programok megint jelentős többségben vannak**, hatan is képviseltetik magukat az első tízben.



A magyar lista első helyét **2009. október óta a Conficker féreg tartja**, amely az operációs rendszer frissítéseinek hiányát, a gyenge admin jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed.



Az előző hónaphoz képest előrébb rukkolt egy hellyel az első ízben 2009 júliusában listára kerülő Win32/Mebrook trójai. Ez egy igen **kellemetlen kártevő, mivel törölheti a merevlemez partíciós tábláját**, és így könnyen adatvesztést okozhat.

Maradt kilencedik a Win32/Packed.Autoit trójai, amely működése során hátsó ajtót nyit a megtámadott gépen, majd több különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.



És végül a **bevezetőben már emlegetett újonc a nyolcadik helyet elfoglaló Win32/Shutdowner trójai**. 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. Aki figyelemmel kíséri a számítógépes kártevők történetét, az talán még emlékszik a hasonlóan **zavaró 2003-ban megjelent Blaster (Lovsan)** féregre, amely egy üzenet ablakban visszszámolt, és szintén lekapcsolta a gépünket.



Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2010 májusában az alábbi 10 károkozó terjedt a legnagyobb számban**. Ezek együttesen az összes fertőzés 27.43%-ért voltak felelősek.



1. Win32/Conficker féreg

Elterjedtsége a májusi fertőzések között: 6.31%

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 válnak a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható a külső meghajtó fertőzött Autorun állománya miatt.

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



2. Win32/Agent trójai

Elterjedtsége a májusi fertőzések között: 5.04%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (például Temp mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett kulcsokkal gondoskodik arról, hogy minden indításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.



A számítógépre kerülés módja: a felhasználó maga telepíti.

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



3. INF/Autorun vírus

Elterjedtsége a májusi fertőzések között: 4.90%

Működés: Az INF/Autorun egyfajta 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/autorun>



4. Win32/PSW.OnLineGames trójai

Elterjedtsége a májusi fertőzések között: 3.51%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. 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. INF/Conficker vírus

Elterjedtsége a májusi fertőzések között: 2.19%

Működés: Amennyiben böngészés során az autorun.inf fájl valamely egység főkönyvtárába kerül, akkor a betöltő eléri, hogy a kártevő kódja induljon el. Vagyis az INF/Confickernek az a szerepe, hogy betöltse magát a Win32/Conficker kártevőt.



A számítógépre kerülés módja: fertőzött weblapról, vagy külső eszközön keresztül.

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



6. Win32/VB féreg

Elterjedtsége a májusi fertőzések között: 1.72%

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.

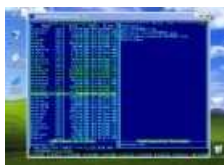
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21vb>



7. Win32/Packed.Autoit trójai

Elterjedtsége a májusi fertőzések között: 1.05%

Működés: A Win32/Packed.Autoit fájlokat hoz létre a C:\Windows\System32 mappában különböző neveken, például autorun.inf, winlog0n.exe, svch0st.exe. A kártékony EXE fájlok automatikus lefuttatásához külön Registry bejegyzéseket is készít. Működése során hátsó ajtót nyit a megtámadott gépen, 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/%21packed-autoit>



8. Win32/Shutdowner trójai

Elterjedtsége a májusi fertőzések között: 1.00%

Működés: A Win32/Shutdowner trójai 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, 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/Mebrook trójai

Elterjedtsége a májusi fertőzések között: 0.87%

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 hoz létre, 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/Tifaut trójai

Elterjedtsége a májusi fertőzések között: 0.84%

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 Registry bejegyzést is készít. 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>



Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.



Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kinszenvedés](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2097521>

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói 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.

Hiába bújsz

2010.06.23. 16:25 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [spam](#) [reklám](#) [védekezés](#) [kéretlen](#)

Jön a szép új világ, egyen szómát, hüvelygomba elleni krém, bifidus essensis - **mindenhol kéretlen reklám hegyek**. Kevesen kérik, de sokan kapják a PH értékeket, és **elugrani előlük egyre nehezebb**.



Ha valaki nem genetikailag reklámzabáló, akkor kevésbé örül annak, hogy egyre jobban és több helyről áradnak a kéretlen reklámok, reklámprogramok. Nem egyszerű **áttekinteni a szövevényes összefüggéseket**, melynek mindenképpen első fele az cikk, amely azt boncolgatja, hogy [lassan egy főállású ügyvéd is a víruslaborok tartozéka lesz](#). Hogy miért is?



Hát mert az olyan ódivatú hozzáállás, ha valaki hibázik, és azt beismerné, sajnos nem létezik. Hogy tényleg **nem volt szép amit tettem, elnézést, bocsánat, vagy ha nagy bajt okoztam, főbe lövöm magam itt a múlt századelőn - ezek már rég kimentek a divatból**. Inkább megjelennek másnap a reggeli műsorokban, a kérdésre, hogy szabályos vagy etikus-e amit tettek, arra a sztenderd hangsúlyozott válasz: "mi az hogy". Ja igen, **és pert is indítanak az antivírus cégek ellen**, hogy azok a kéretlen reklámjukat, becsületes üzleti trójai programjaikat szűrni merészelik. Azért [szerencsére néha pert is vesztenek, még ha évek is kellenek ehhez](#).



Ez a "kérjük x napon belül szüntessék meg termékünk kártevőként való szűrését, különben kénytelenek leszünk jogi lépéseket tenni" formula annyira gyakori lett, hogy **exponenciálisan nőtt az ilyen adminisztrációs munkák száma a víruslaborokban**. Ennek lett aztán az is a következménye, hogy **az antivírus telepítésnél nincs perelhető alapértelmezett állapot, hanem a felhasználóknak kötelezően dönteniük kell** a "Kéretlen alkalmazások keresése", a "Veszélyes alkalmazások keresése" és a "Reklámprogramok, kémprogramok és biztonsági kockázatot jelentő programok keresése" opciók ki- vagy bekapcsolt sorsáról.



Ha a tvben sugárzott és a műsort agyonvágó reklámokat nézzük, egy mozi filmet, vagy akár csak egy rövid NCIS epizódot sem lehet kettő-három-négy 8-10 perces reklámblokk nélkül megúszni, és mire harmadszor jön a levehető ajtós turmixgép, meg tizedszer promozzák be a Hazudj ha tudsz következő évadát, **az ember szinte el is felejtí, ki volt a gyilkos, mi történt eddig és ki is tette a nyomravezető lószórt a bárszekrénybe**.



De cserében elküldhetjük a **kecsege** szót SMS-ben az **06-90-1234 számra**, és ezzel jó eséllyel nyerünk egy erdei fazsetont, amiből már csak ötven darabot kell összegyűjteni ahhoz, hogy indulhassunk az automata kávéfőzőért folyó sorsoláson. Aztán meg [nagy a csodálkozás, hogy emberek tv helyett miért torrenteznek](#).



Van emellett egy olyan szegmens, ami teljesen kívül esik a hatáskörünkön: [profitorientált üzleteknek kapnak egy kedvező ajánlatot, és nagy ívben tesznek az olyan ódivatú dolgokra, mint becsület, etika, szerződés, törvényesség](#). Eladják a felhasználók személyes adatait közvetlenül a reklámcégeknek, bár korábban erről nem volt szó, engedélyezésről szintén nem. Az örökmozgó és mindig változó felhasználói szerződés korunkban egy valódi súlyos dilemma, és [korántsem csak a Facebookot érinti](#).



Legutóbb például az Apple új IOS-a kapcsán jött elő, nevezetesen az új szoftververzióhoz új szerződés tartozik, amit el kell fogadni annak telepítéséhez, frissítéséhez. [Ez pedig azt tartalmazza, hogy beleegyezzünk, hogy gyűjtsék a felhasználók pontos tartózkodási helyét](#). Állítólag anonim módon, és még állítólagabb [a hirdetési rendszerük fejlesztésével függ össze mindez](#).



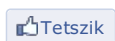
Mit lehet hát tenni? [Vonuljunk el remetének?](#) Fülünkbe forró ólmot öntsenek? Vegyük elő a padlásról a porosodó Nokia 1610-et, ami igazi áldásként semmi mást nem csinál, kizárólag telefonálni képes? **A netes böngészés közben mindenesetre lehet a Noscript és AdBlock plus áldásos hatásait élvezni**, a tv filmeket fel lehet venni, be lehet digizni, és reklámkivágni - ami persze izzadságszagú, munkás - enélkül marad a netes műsorforrások nézése, DVD vásárlás vagy a letöltöttség.



Az e-maileknél pedig vagy az internet biztonsági csomagunk spamszűrője, vagy a szolgáltónk - esetleg a kettő együtt kezeli a szemétlevelek kérdését. [Enélkül a levelezésünk normális menete](#) gyakorlatilag megbénulna.



Ám hogy mindez ne legyen elég, a jövőben át kell értékelnünk a multifunkciós nyomtatókról és azt ezt forgalmazó cégekről is a **korábbi elképzeléseinket**. Ez pedig annak a hírnek a kapcsán merül fel, miszerint [a HP teszteli, hogy miként tudnának célzott hirdetéseket elhelyezni a webeléréssel rendelkező nyomtatóikkal](#). Szép, nem? Hogy pink frappáns kommentjét idézzük: "fizeted a tintát, hogy kéretlen reklámot kapj, csodás elme".



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



Ajánlott bejegyzések:

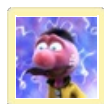
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrző 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Akiknek a Captcha kinszenvedés](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2103127>

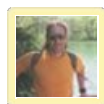
Kommentek:

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



Zizidor 2010.06.25. 00:21:53

Majd amikor bejön az a trükk, hogy a tévé nem vált csatornát a reklám ideje alatt... Vagy minden telefonhívás előtt meg kell hallgatnod egy rövid reklámot...



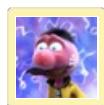
Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.06.25. 11:12:19

Szia Zizider!

Kivételesen beajánlottam a címlapra is ezt a posztot. de úgy tűnik, sajnos nem érte el az ingerküszöböt. Pedig iphone ügyben júli 12-re beidéztek Jobs bácsit egy kis beszélgetésre:

voices.washingtonpost.com/posttech/2010/06/lawmakers_grill_apple_ceo_jobs.html

A tévéknél már sokszor van, hogy majdnem mindhol egyszerre tolják a reklámot. Például 7:50 és 8:00 között kapcsolgathatsz, de mindenhol csak a péháérték csörgeti láncát. Szerintem majd az a trükk lesz érdekes, amikor a reklám követi a szemmozgásodat, és mindig oda ugrik, ahová nézel. De ne adjunk itt ingyé jó ötleteket ;-)



Zizidor 2010.07.02. 13:16:29

"a hirdetési rendszerük fejlesztésével függ össze mindez" - Ez nagyszerű! Ha például Jack elsétál a mozi előtt, már tolják is neki a legújabb filmajánlókat?

Lesz személyre szabott reklám is, mint a Különvélemény c. filmben? (Ha jól emlékszem). Sétálsz az utcán, beazonosítanak, egy pillanat alatt lekérik a rólad összegyűjtött információkat, és máris kapod a képedbe: "Á, kedves Rózsika! Repülőjegyet foglalt Görögországba? Jöjjön be hozzánk, akciós napszemüvegek, fürdőruhák és hűtőtáskák érkeztek! Az emeleten időpontot is foglalhat a nyaralás utánra saját bőrgyógyászunkhoz!" :-S

Amikor mások baltázzák el - part II.

2010.06.25. 14:35 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [admin](#) [biztonság](#) [jelszó](#) [twitter](#)

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.



Volt már itt biztonsági [konferencia résztvevők összes személyes adatának véletlen elküldése minden egyes résztvevőnek](#) típusú hibázás pont biztonsági cég által, de ha össze akarnánk foglalni a különféle szolgáltatók, hivatalok, üzemeltetők mit is tudnak elrontani, **két fő csoportot** különböztethetünk meg.



Az **elsőnél a biztonsági kérdésekre (lehet ez adatbázis, weblap, személyes adatok védelme, fizikai gép őrzése, stb.) nem fordítanak elég figyelmet különféle okok miatt**: erőforrás spórolásból, lustaságból, figyelmetlenségből. A második típusú találkozásnál a megbízhatatlanság nyer teret: **például jó pénzért alattomosan eladják a személyes adatainkat közvetlenül a hirdetőknak**.



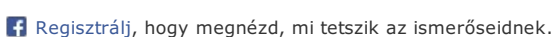
Felhasználói részről ugyan mindkettő kivédhetetlen, és a végeredményt tekintve - kikerül közprédának, aminek nem kellene kikerülni - nincs különbség, de a nagynevű, profi szolgáltatóktól az ember automatikusan azt várná el, hogy elegendő kvalifikált szakembert alkalmazzanak ezek megbízható kezelésére. Most viszont [éppen az ellenkezője derült ki a Twitter kapcsán](#).



Az FTC (amely ezúttal nem a Ferencvárosi Torna Club, hanem a Federal Trade Commission, azaz amerikai fogyasztóvédelmi hatóság) szerint a Twitter üzemeltetők számos helyen hibáztak: személyes magán fiókjukat használták admin célra, valamint adminisztrációs jelszavaik is primitív, szótáralapon könnyen kitalálhatóak voltak. Nem fordítottak gondot a jelszavak időszakos rendszeres cseréjére sem, és előfordult eset, hogy jelszavakat sima clear text állományban tároltak. Ezzel a felelőtlen hozzáállással súlyosan kockáztatták a felhasználók biztonságát, amelyet több ízben - például 2009 áprilisában - ki is használtak külső támadók.



Nyilván nehéz vagy lehetetlen minden támadást kivédeni, de azért **egy óriás cégről az ember akaratlanul is feltételezi, ilyen primitív hibákat már nem követnek el**. Hát de, és ez nagyon-nagyon szomorú. "A francia és az olasz csapat tagjai kedden közösen meglátogattak egy fokvárosi árvaházat. 'Szívszorító volt látni a szomorú kis arcukat és a reménytelenséget' - nyilatkozta később a 6 éves Dzsamal." Reméliük, a Twitternél gyorsan javítanak, és nem születik róluk valami hasonló vice.



Ajánlott bejegyzések:

- Kárty könyv böngésző kiegészítők jönnek

- [Akiknek a Captcha kínszenvedés](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2109026>

Kommentek:

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

Nincsenek hozzászólások.

Facebook csoportot csak őstermelőtől

2010.06.28. 13:10 | [Csizmazia István \[Rambo\]](#) | [25 komment](#)

Címkék: [személyes privacy facebook adatok csoportok](#)

Ez a jó kis komment adja a mai címet, ezúton is köszönet érte bpo478-nak. A mai példa alapján **érdemes lehet alaposan átgondolni**, mit is adunk ki magunkról, amikor egy Facebook csoporthoz, vagy rajongói klubhoz csatlakozunk nem agysebészi pontosságú adatvédelmi beállításokkal.



A jó üzletember mentalitás már gyermekkorban kiütözik. Móricketől kérdezi a tanítónéni: Mennyi kettő meg kettő? **Az attól függ - érkezik a válasz - hogy venni akar a tanárnő vagy eladni.** Ennek fényében Móricket elömenetele miatt már nem kell aggódnunk, és **korábban talán a Zuckerberg szülők is beszélgethettek otthon:** "Nem tudom, mit csináljak a fiunkkal, olyan megbízhatatlan? Arra gondoltam, talán adjuk meteorológusnak!" De aztán végül láthatjuk, [mégiscsak számítógépes üzletember lett belőle.](#)



Nyilván vannak hozzám hasonló pesszimista hozzáállású emberek, akik úgy gondolják, [a DM biztonsági örök centiméterben mért vevőkövetési távolsága](#), az [összes plebejus állampolgárra és külön Stohl Andrásra vonatkozó](#) büntési tételek szigorúsága, vagy [Hajdú Péter empátikus parkolási szokásai](#) **nem egy Facebook csoport létén vagy nem létén múlnak vagy változnak meg varázsütésre.** Szerintem ilyen csoportokat létrehozni nagyjából annyi értelme van, mint atombunkert építeni Kocsordon, de biztos én látom rosszul, hogy ilyenekben nem hiszek.



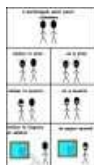
Ám ha már állampolgári kezdeményezésből, alulról szervezeten mégis megalakul egy ilyen, természetesen nem úgy képzelem az ember, hogy az érintett HMCS/multicég/whatever [izomból simán megkaphatja az admin jogot felette, és vele az összes csoporttag személyes adatához](#) való hozzáférést. Ez **vastagon minősíti** nem csak például az így eljáró cégeket, hanem **magát a Facebookot is, sőt őket leginkább.**



[Adatvédelmi szempontból](#) pedig **több is, mint aggályos.** Mindenki emlékszik arra az esetre, mikor a [Yahoo kiadta a kínai hatóságoknak egy ottani újságíró adatait, akit ezért tíz év börtönre](#) ítélték. De az is megtörtént, hogy [Pakisztán blokkolta az egész országban a Facebookot és a Youtube-ot.](#) Nem kell még csak szélsőségesnek sem lenni, egy hétköznapi Facebook [csoporttal technikai hiba miatt is történhetnek](#) különféle érdekes dolgok, egy konkrét nyomozás során egy internetszolgáltató vagy közösségi oldal üzemeltető természetesen köteles átadni ilyen adatokat a hatóságoknak, de csak úgy puszira, [egy szimpla céges kérésre ilyet kiadni](#) elég érdekes.



Gerincességben fajsúlyra körülbelül a [személyes adatok hirdetőknél való közvetlen, titokban és engedély nélküli eladásával egyenértékű](#). Még ha [ez a link itt inkább elvont szélsőséges ideológiai agymosás](#), azért a fentiekből mégis látszik valamennyire, [a különféle Facebook vagy egyéb csoportokban való részvételnek vannak, lehetnek nem várt következményei is](#).



Ma úgy tűnik, mindenben a TH kommentelők mondják meg a tutit, a végszót is Énbagolynak köszönhetjük: "Ja, azon szoktam röhögni, hogy ugyebár a blogolásnál az emberek nicknevek mögé bújnak, aztán meg csatlakoznak a blog fészbukos rajongói oldalához névvel, címmel, fényképpel, mindennel együtt. :)" [De a hajó azért megy](#).



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



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászzal](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2115348>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.06.28. 13:52:16](#)

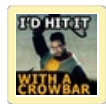
Sajnos ezt a cikket nem a regisztrációt megelőző kikerülhetetlen ablakban olvashatja a leendő nagyon közösségi ember. Ettől az egész wiw-fb-twitter stb f*szságoktól fálnak tudnék menni, ha nem azt gondolnám, hogy "aki hülye haljon meg". :-)

[daylienn \(törölt\) 2010.06.28. 16:36:55](#)

Még mindig nem értem, hogy mit tudhatnak meg egy emberről, ami személyes adat.

Számomra értelemszerű, hogy csak olyan adatokat adok meg, képeket rakok ki, amiket amúgy is nyilvánosnak tartok. A FB profil arra szolgál, hogy az ember egyfajta imázst alakítson ki magáról. Semmi többre.

Aki ennyire fél, hogy megtudnak róla valamit, az inkább mondja fel a net és telefon előfizetését.



[hydra 2010.06.29. 01:35:54](#)

közösségi oldalt csak nyílt forráskódból.

[Kulminaator 2010.06.29. 07:34:11](#)

"a Yahoo kiadta a kínai hatóságoknak egy ottani újságíró adatait, akit ezért tíz év börtönre ítélték."

Ez így ebben a formában fasssság :D

[Kulminaator 2010.06.29. 07:35:00](#)

Most nézem a tetejét, nod32 ? loál!

Zka 2010.06.29. 09:00:47

@daylienn: pontosan.

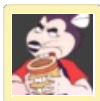


dr. phil. Sün!! ツ • <http://sunews.blog.com> 2010.06.29. 09:08:50

Internetet csak őstermelőtől!

LegjobbVagyok • <http://legjobbvagyok.hu> 2010.06.29. 09:35:27

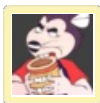
Egy antivirus blog írójától elvártam volna, hogy azon túl, hogy fikázza a világ legnagyobb közösségi oldalát, talán valamilyen javaslatot tesz az átlagos regisztráltak, hogyan védje meg magát meg az adatait az ilyen helyeken. De mint a legtöbb bérblogger, ő is csak a szenzációhajász és egyoldalúan negatív véleménnyilvánításig jut el, a hogyan tegyük jobbá már eszébe sem jut... Na persze, abból neki mi haszna...?



iii • <http://nemzetimarhulat.blog.hu> 2010.06.29. 09:37:27

A csoport gazdája semmiféle személyes adatot nem tud meg, egyedül üzenetet tud küldeni a tagoknak. Ezt mint több FB csoport alapítója állítom.

A csoport einstandolását persze elítélem, de nem kellene tájékozatlanul a sz*rt kavarni.



iii • <http://nemzetimarhulat.blog.hu> 2010.06.29. 09:38:25

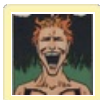
Plusz: rendkívül zavaró olyan cikket olvasni, ahol minden második szó ki van linkelve valahova.



Pong 2010.06.29. 09:44:27

Látom a cikkíró teljes mértékben figyelmen kívül hagyta a társadalomtudomány azon oldalát, ami a nagy tömegek viselkedésének befolyásolásáról szól. A FB csoportokon keresztül egy "awareness" épül fel, amit később felkapnak tradicionális médiák, mivel közvetlen visszajelzést kap a néptől, amit a tűzijáték esetében a a médián is igazolt.

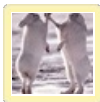
Másik butaság az, hogy összemosza a céges s a szociális oldalakat, ugyanis teljesen más tézisa, ha "Dögöljön meg a Stárbaksz" oldalt csinállok, ugyanis az akkor a whistleblowing/customer protection alatt menni, miközben ha olyasmit csinállok mint "Starbucks Magyarország", akkor persze jogosan érezheti a cég azt, hogy elvették szócsövét/vuvuzeláját.



Pong 2010.06.29. 09:45:21

@iii:

+1, hogy csoporttulaj nem tud nézni személyes adatot, én developperkedek egy kicsit, s nekem sem szabad, avagy nem teszem.



Circus 2010.06.29. 09:50:52

@Sün!!:

Hamár őstermelő és net, a Pók dolgozik már?

@daylienn:

A gond szerintem itt lehet:

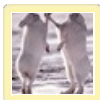
1, nem Rólad van szó, hanem azokról, akik agyatlanul töltik fel jobbra-balra az adataikat, képeiket, stb. Lásd balhé a parlamentbe frissen bekerült nembaloldali párt prominens képviselőiről. De akár a klasszikus, -18 HP buliképei, telefonszáma, mellmérete, stb, merugye a wiw az kéri meg buli... Meg ugyanezért van középkorú, angolul nem tudó férfinemű ismerősömnek

vagy húsz angolnevű cicababa ismerőse fb-n - bejelölték, visszajelölte. Aztán meg majd pislog.

2, ámdebar, hiába vagy nagyon fifikás, keresztivatközásokkal simán utánad lehet nyomozni (amikor először kerestem rá pl. a nevemre, utána napokig lúdbörzött a hátam). Kivéve persze, ha ezermillió különböző e-mail címet használsz, külön-külön minden életfunkcióra. Én sem titkolom annyira, mert beválok, amit mondok/teszek, de ha valami rosszindulatú barom betalál...

És hogy ON is legyenek - kell még vagy 15-20 év és rengeteg botrány, hogy az emberek megtanuljanak védekezni (gondolkodni?). A következő generáció már ebbe nő majd bele, de a mai 50 feletti korosztály kb. menthetetlen. Ugyanaz és ugyanúgy, mint a most 70 feletti a rendszerváltás után - teljesen új világ, amibe ártatlanul mennek bele, és ott cseszik át a fejüket, ahol tudják.

Mindazonáltal az elsomorít, hogy rossz dolgokra használják az amúgy egyik (szerintem A) legnagyobb találmányt az emberiség történetében...



Circus 2010.06.29. 09:55:04

@SárgaEminenciás_sargacsik.hu:

"egyoldalúan negatív véleménnyilvánítás"

kontra

"fikáz"

"bérblogger"

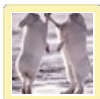
"tegyük jobbá eszébe se jut"

"na persze, neki mi haszna"

gratulálok :D

LegjobbVagyok · <http://legjobbvagyok.hu> 2010.06.29. 09:58:37

@Circus: én kritikát nyilvánítottam a cikkről, azt kértem számon, hogy ha valaki nemet mond, mondjon igent is. Te miről írsz?



Circus 2010.06.29. 10:04:10

@SárgaEminenciás_sargacsik.hu:

Nekem csak szimplán nagyon tetszett, ahogy egyoldalú, negatív véleménnyilvánítás miatt kritizálsz a cikket egyoldalú, negatív véleményekkel. Ügyes kifigurázás, nagyon tetszett. Vagy Te nem így gondoltad?

(de ne offoljuk már ezt szét szerintem)

LegjobbVagyok · <http://legjobbvagyok.hu> 2010.06.29. 10:11:39

@Circus: szerintem se...



Csizmazia István [Rambo] · <http://antivirus.blog.hu> 2010.06.29. 10:48:08

@Circus, Mindenki:

Igen, aki ide kommentelt, annak már lehet valamennyi tapasztalata, őket nem féltsem, de a sebezhető többség, ahogy Circus is mondja naivan bereggel, hallgatja a rádiót (tegnap tedd fel a legvadabb bulis képeidet, és nyerj toshiba kamerát), aztán csodálkozik.

@ SárgaEminenciás_sargacsik.hu

Nem esett jól, amiket ismeretlenül írtál, hiszen jobban volt személyeskedő, személyem ellen irányult és csak kevésbé a cikk tárgyát cáfolta. Ha zsidó vagy cigány lennék, akkor ez is ott szerepelt volna a beírásban? Megnéztem a sargacsik.hu oldalt,

onnan idézek: "Hisszük, hogy minden ember egyedi, és különleges értéket képvisel világunkban" És ez nekem miért nem jár?

Egyénként szoktam tanácsokat is adni, bár elsősorban tényleg tükröt tartok, de itt vannak a legutóbbi posztok, pcw cikkek:

antivirus.blog.hu/2010/04/22/tiz_gyanus_jel_hogy_zombi_e_vagy
antivirus.blog.hu/2010/05/19/privatlet_ellenorzes
antivirus.blog.hu/2010/06/03/feltort_postafioik_remedy
www.commodore64.hu/pdf/vvv34.pdf

"Hidd el, engem a legjobb szándék vezet, hibát csak elkövetetek vagy nem?" (Beatrice)



Pong 2010.06.29. 10:57:36

Anyám tegnap jelölt be FB-on. Most mit csináljak, tutorialt írok, ja s angol oldalak nem mennek, csak germán.

LegjobbVagyok • <http://legjobbvagyok.hu> 2010.06.29. 10:58:16

@Csizmazia István [Rambo]: Elég rége olvasom a blogodat, és hidd el, nem szokásom öncélúan fikázni, trollkodni. Ismerem a hozzáállásodat, olvastam több hasznos tanácsot adó írásodat, pl. a zombisat is. Pusztán csak annyit hiányoltam ebből a posztból is, hogy mit tehet az egyre növekvő FB tábor az ottani kiismerhetetlen privacy policy kivédésére, milyen eszközei vannak. Igen, mi is közösségi portált üzemeltetünk, és mint ilyen, egy kicsit közösségiportál ellenesnek is érzem ezt az írásodat, mert azt sugallja, hogy ha a user regisztrál egy ilyen helyre, előbb-utóbb biztos visszaélnék az adataival. Egyébként, akinek nem elég a hazai közösségi oldal kínálat, és csak olyan szolgáltatások elégítik ki, mint a FB, msn, yahoo, az ne siránkozzon, ha ellenőrizetlenül visszaélnék az adataival, és nincs az a fórum, amely megvédené. Mi a magyar törvények szerint építjük és üzemeltetjük a portált, és mint ilyen, számonkérhetők vagyunk, ellentétben az un. nagyokkal.



samcro 2010.06.29. 11:07:44

Nem vagyok paranoiás, de amikor az FB a regisztrációkor megkérdezte a mail-es jelszavam, hogy ismerősök után kutasson a címjegyzékemben, leveleimben, úgy döntöttem, hogy erre nekem nincs szükségem. Viszont nagyon sokan itt automatikusan megadják. Nem beszélve a sok összekapcsolódott közösségi oldalról, amikre egy accounttal lehet bejelentkezni. Még ha az ember nem is csinál olyat, ami esetleg mások szemében rossz, akkor sem biztos, hogy jó ötlet ennyire összekapcsolni mindent.



Circus 2010.06.29. 11:46:03

@Pong:

Ha jól akarsz magadnak, akkor igen... én folyamatos tanfolyamszervezésben vagyok, különben több energiába kerül csak a kártevőmentesítés és újjáépítés. A gond az, hogy kikerült adatok esetén olyan károkat lehet szerezni, amit nem lehet kiírtani...

@samcro:

persze, hogy nem jó összekapcsolni mindent, de egy egyszerű g****e keresés magától összerakhat adatokat, amelyeket nem biztos, hogy szeretnél...



Circus 2010.06.29. 12:04:07

@SárgaEminenciás_sargacsik.hu:

Amit észrevettem mezei felhasználóként, az az, hogy a közösségi oldalak előbb-utóbb vagy átmennek fizetősbe/fizetős szolgáltatást IS nyújtóba (mondjuk, ha ebből élsz meg, akkor érthető) és innentől kezdve akarva-akaratlanul kommercializálódik - egyenes út a kétértelmű reklámlevelekhez illetve így-úgy kikerülő adatokhoz és szuper melegágy az adathalászhoz meg egyéb netes gusztustalanságokhoz.

Utóbbi természetesen nem egyedül az üzemeltető hibája - legelső hozzászólásomban, amit írtam, az nem okvetlenül a fenntartó/üzemeltetőről szól, hanem inkább a szándékosan rosszindulatú, reklámozó, mittudomén felhasználókról, akik nem arra használják az oldalt, mint amire való.

És akkor még nem is beszéltünk az egyik csúcsról, a különböző társkereső oldalakról - itt lehet igazán kártékony, aki olyan. Ott ráadásul többé-kevésbé szándékosan adod ki magad.

Részben kapcsolódik ide - a Subba hétvégi iwiw-es akciójáról is megvan a véleményem. Hülyébbnél hülyébb képeket linkelnek be olyanokról, akik voltak akkora marhák, hogy ezeket fel is rakják. Ez is egyfajta átnevelés lehet, mondjuk... Kérdés - megérdemlik, vagy ezt azért nem kellene?

Lásd még a Szalacsi-féle világhír...

És ha Rólad (itt általános alany) kerül fel egy kép, amit valaki valamikor egy 'jókedvű' pillanatban készített? Nagyjából cseszheted, hogy be vagy-e regelve, vagy sem akárhová...

Nekem nagyon úgy tűnik, hogy az internet térhódításával a magánszféra EL FOG TŰNNI. Sajnos.



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.06.29. 22:01:24](#)

Közösségi portálokról mazsoláznak a valóperes ügyvédek:
hvg.hu/Tudomany/20100629_kozossegi_oldal



[atko 2010.07.05. 11:41:46](#)

Érdekes volt olvasni a hozzászólásokat arról milyen jó is a közösségi on-line lét. A hazai mindig jobb, mert látom mit csinálnak és hazai törvények szabályozzák... Ha ha.

Ha az iwiw törölné rendesen az adatokat igaz lenne. Ha már most törlik ellentétben a régmúlttal elnézést. De ugye a bizalom már elszállt.

Ha az internetbiztonságos lenne, akkor nem lenne para a közösségi oldalak miatt.

Ha a közösségi oldalak üzemeltetői tévedhetetlenek lennének szintén nem lenne para.

A probléma az, amit már többen megfogalmaztak, hogy nem vagyunk készek az online életre.

Annak idején a wiw-hez 2003-ban, vagy 2004-ben csatlakoztam. Tök jó volt. Kapcsolat olyanokkal akiket ismerhetek, vagy régen ismertem. Aztán jöttek azok akik 100-200-300 és még több ismerőssel bírtak, mert könnyű jelölgetni egymást. Így lett nekem is hirtelen ismerősöm a Fanta. Na ekkor töröltem magam. A közösségi oldlak hülyéinél (itt a hülyékre gondolok, nem mindenkire), már csak a továbbít gombot utálom jobban a levelezőkben.

A notórius meghaló

2010.06.30. 13:55 | [Csizmazia István \[Rambo\]](#) | [1 komment](#)

Címkék: [spam is trójai botnet eminem dead zeus](#)

A régi vicc szerint két japán beszélget. Mi van a markomban - kérdi az egyik? Hát hifi torony. Jó, jó, nyilván az, na de mennyi? A kártevőket terjesztő linkekkel felvértezett spam kampányban van olyan sztár, amely már a Guinness Rekordok Évkönyvébe is bekerülhetne a leggyakrabban költött halálhír kategóriában.



[Keltették már a halálhíredet Johnny?](#) És mennyi a mennyi? Miiii, hogy csak egyszer. Hát ez nagyon karcsú, ezzel a gízda eredménnyel biztosan nem kerültél fel a táplálkozási lánc csúcsára.



Mostanában (újra) Eminem halálhíre az újdonság, [érkezik egy "Eminem , Marshall Mather is DEAD!!!" tárgyú kéretlen üzenet](#), benne a CBS News nevében közölt álhírrrel. Az ígért videóra, ami valójában EXE kattintani nem érdemes, kivéve, ha feltett szándékunk, hogy [számítógépünk kapacitását olümpuszi görög istenekkel kívánjuk önként megosztani](#). Akit bővebben érdekel az ilyen típusú [forgató könyv](#), olvassa végig a Johnny Depp halálhíréről szóló posztunkat.



Ami viszont érdekes, hogy [Eminem lassan tényleg rekorder lesz](#) - persze nem önhibájából. A mondás szerint akinek hamisan a halálhírét költik, az hosszú életű lesz itt e Földön.



Figure 1. The 100 most important variables from the 10000 variables in the 10000 variables dataset.

[És vajon akinek hetente kering ilyenje, azzal mi helyzet?](#) Sajnos látszólag hosszú élete itt főként a hamis hírrel, ZLOB trójaival küldözgetett kéretlen leveleknek van, az biztosan örökéletű lesz, akárki meglássa.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 Tweet

Ajánlott bejegyzések:

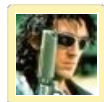
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2120461>

Kommentek:

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



[Yann Le Pentrec](http://lnk.bz/t7c) • <http://lnk.bz/t7c> 2010.07.06. 13:27:22

Aki meg bedől egy ilyen "hírforrásnak", miből feltételezi azt, hogy valódi halál esetén nem erről zengene a világsajtó? Bár valóban sok a tájékozatlan ember, még több, aki nem is vágyik a tájékozottságra.

Captcholtam

2010.07.02. 13:30 | [Csizmazia István \[Rambol\]](#) | [6 komment](#)

Címkék: [video captcha](#)

[Folyamatos a küzdelem a Captcha fronton](#). Az embert a géptől szétválasztani képes kérdés eleinte még jól működött, mára inkább bosszantó szemmeresztgetés vagy felesleges akadály [a fejlett captcha törőknek](#).



Tömegesen regisztrálnak postafiókokat, amiről aztán árad a sok spam, kártevő, szemét. Hogy ez ne így legyen, jönne a captcha kérdés, hogy ne botok, hanem hús-vér emberek tudjanak csak regisztrálni. Ám a leleményes sötét oldal **hatékonyan képes kijátszani** ezeket az akadályokat. A közkeletű problémára [még maga a Google is megpróbált](#) valamilyen ütőképes megoldást kitalálni az elfogatott ábráival. [Egy mostani újabb változat talán néhány szempontból biztonságosabb, szebb és használhatóbb megoldást kínál a kanadai Nucaptcha](#) cég jóvoltából.



Az alap OCR-ezés ellen azt találták ki, hogy **a hagyományos amorfá gyűrt betűk helyett egy video ablakban hullámzó, és jól olvasható karaktereket mutatnak**, amelyek még színre is lehetnek különbözők, így a kérdés lehet akár az is, hogy csak a piros betűket vagy a kék számokat kell begépelni.



Persze egy kiskapu megmarad: [a captcha törő rabszolgák nyilván ezt is el tudják majd végezni](#), de azért **van sok pozitívum is**. Figyelemre méltó, hogy mind az olvashatóság, mind **például a gyengénlátók részére nyújtott hangalámondás jó iránynak látszik**.



Sőt, a technológia abból a szempontból is érdekes, hogy **a flasht nem támogató platformokon (például iPhone, iPad) is működőképes**. Meglátjuk, hogy a ["video kill the radiostar"](#) módi beválik-e majd hosszútávon.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

• [1 trackback](#)

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Dropbox csálival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2125146>

Trackbackek, pingbackek:

[Trackback: CAPTCHA megoldás Joomla-hoz, Drupalhoz és WordPresshez](#) 2010.07.03. 07:11:28

A Confident Technologies néhány napja jelentette be, hogy kép alapú azonosító megoldása, a Confident CAPTCHA elérhető WordPress pluginként, Joomla kiterjesztésként és Drupal modulként is. A Confident CAPTCHA™ egyedi, kép alapú CAPTCHA megoldás, amely S...

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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>
2010.07.02. 17:34:09**

Kenczler Misi írja: "Vajon mit kezdenek távol-keleten ezzel a magyar CAPTCHA-val: 'Milyen nap van ma?'" :-)

[Giraffe](#) 2010.07.03. 20:37:39

l. az xpress.hu captcha-ját. Pl. "öt + nyolc", és számmal kell beírni az eredményt. De 1-1 jól eltalált kérdéssel nem csak a robotokat, hanem az IQ-szegény droidokat is távol lehet tartani :)



[Moszkva téri Dzsed](#) 2010.07.04. 02:31:47

[@Csizmazia István \[Rambo\]](#): majd jönnek a magyar kapcsolódó csapatok is...

ez az egész captcha dolog macska-egér játék, és mióta vannak kapcsolódó csapatok, azóta gyakorlatilag már nem éri meg pénzt, időt és energiát belelőni az újabb és ravaszabb kapcsa-rendszerek fejlesztésébe :)



**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
2010.07.05. 10:39:49**

Hello Giraffe :-)

Igen, vannak ilyen jópofaságok, például az ubuntu.hu is ilyen.

pl.

A második osztály 7 tanulójaiból 3 szemüveges fiú. 2 lány jár az osztályba. Hány fiú nem szemüveges?:

vagy

Dóra bélyegeket gyűjt. Eddig 23 bélyege van, ennek a felénél egy fél bélyeggel többet a szüleitől kapott. Hány bélyeget kapott édesanyjától, ha ez kétszer annyi, mint amennyit édesapjától kapott?:



**[Csizmazia István \[Rambo\]](#) • <http://antivirus.blog.hu>
2010.07.05. 10:45:46**

Szia Vuvuzelaaa!

Igazad van, ez egy örök harc. És az említett furmányos kérdések is hiábavok, ha például mindez angolul lenne egy nagy oldal esetében, akkor máris megéri a rabszolga toborzás.

[nyos](#) 2010.07.07. 20:49:07

Egyik oldalra par eve irtam egy szoveges captchat, de kesobb lecsereltem, mert par kollega is fennakadt rajta. :) Az otlet az Idiocracy cimü filmbol van.

Ha egy vodorben 5 liter, egy masikban 3 liter viz van, osszesen hany vodrunk van?
(a szamok randomizalt ertekek, a filmben mar nem emlekszem mi volt, de ez a lenyege)

Adathalász levelek a Wikipedia nevében

2010.07.05. 15:10 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [spam](#) [wikipedia](#) [link](#) [email](#) [kártékony](#) [adathalászat](#)

Nem maradt ki a szórásból az angol Wikipedia sem, ismeretlenek arra kéri a címzetteket, legyenek olyan kedvesek ellenőrizni egy ottani állítólagos accountot.



[Az emailben küldött linkek aztán különféle kártékony, fertőző vagy csak kéretlen reklámodalakra mutatnak](#). Nyilván az kell, hogy ilyenkor mindenkinek pavlovi reflexként eszébe jusson, **hiába nem bank vagy hatósági szerv küldte ezt most, akkor sem kattintunk ilyen kéretlen linkre**. Ott vannak szépen a saját böngészős könyvjelzőink, az oldalra való belépéshez használjuk mindig azt.



Ez amiatt is jobb megoldás, mert **előfordulhat, hogy a link preview ablakban nem mindig olyan ordítóan és nyilvánvalóan gyanús URL-ek jelennek meg**, mint például "hxxp://regisztracio-microsoft-akcio.984download.com.cn" vagy hasonló. Sokszor a csalók az o és nulla, az 1 és az l betű cseréivel, [egyéb betűcserékkel, szándékos elgépeléssel](#), meg egyéb trükkökkel - [lásd Raural furmány](#) - a linket kinézetre az eredetihez nagyon hasonlóra igyekeznek elkészíteni.



Egyre gyakoribb a hivatalosnak látszó és hihetőnek tűnő linkek használata, de [emellett sűrűn fordul elő a már jól ismert linkrövidítés](#) is. Tulajdonképpen minden egyszerű lenne, **továbbra se kattintsunk kéretlen linkekre, oszt jónapot**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2130741>

Kommentek:

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



Metal Warrior • <http://ordogvilla.blog.hu/> **2010.07.05.**
19:13:09

Én ma a yahoogroupstól kaptam egy levelet, hogy xy feltett pár linket, amire neivan rányomtam, cserébe minden ismerősöm kapott egy viagrareklámot... :((
Közben kiderült, hogy az illető tényleg feltette al inkeket, és a link is a yahoogroupsra mutat... Akkor hogy kaparinthatták meg a címjegyzékemet?

Alig várom, hogy a tárgyaláson meg

2010.07.07. 17:33 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [spam](#) [kína](#) [bank](#) [hollandia](#) [üzleti ajánlat](#) [kéretlen](#)

Kicsit furcsa hangvételű kéretlen üzleti ajánlat érkezett, amely kissé a "hazakísérhetlek? igen meg" típusú párbeszéd nyomait hordozza magán.



Már volt szerencsénk hasonlóan remek kéretlen üzleti ajánlathoz, [akkor Patrick kapitány gondoskodott a jó hangulatról](#). Ezúttal **Móka Miki** helyett maga **Mr. Peter Wong Tung Shun** libbent ki középre, hogy a vendégeket táncával szórakoztassa. Levelének zavartalan elolvasásához csak annyi kellett, hogy átbillentsük a Cyrillic 1251-ről az olvasható ISO8859-2-be a karakterkódolást, és máris tovasuhantak a jerük, egzotikus légyságjelek és egyéb orosz betűk.



"Üdvözetek és bókákat.

Én vagyok Mr. Peter Wong Tung Shun dolgozom a Bank of China Nekem van egy design üzleti értékben USD 22500000 méter át egy offshore számlára a segítséget, ha úgy kívánják.

Ha kérem a segítségét megvalósításában az ügylet, kívánom tenni 30%-a teljes pénzeszközök kártérítést a segítséget, de ha küldök neked minden tranzakciós információt átvételekor meg a választ.

Akkor vegye fel velem a magán e-mail: (peterhungsung@aol.com), és elküldi nekem a következő információkat dokumentációs célra.

- 1) név
- 2) aktuális lakcímváltozás
- 3) Privát telefonszámot,

Alig várom, hogy a tárgyaláson meg."

Pedig nem is akartuk hazakísérni ;-). Egy biztos: **nem igazán javasolt a fenti gördülékeny mondat klisék könyvformátumban való kiadása és publikálása "Angol-magyar kereskedelmi levelezés és szófordulatok gyűjteménye az üzleti életben titkárnők számára" címmel.** Továbbá jól láthatóan Hollandiában is vannak fertőzött spamterjesztő zombi gépek.



"Négy különböző nemzetiség képviselője volt az asztalnál: egy amerikai gyalogos, egy francia őrvezető, egy angol géppuskás és egy orosz hússaláta." **A párhuzam részben itt is fennáll a kínai bank, a hongkongi emailcím, a holland IP és hússaláta helyett ezúttal orosz karakterek formájában.**



Azt is tudjuk már korábbi tapasztalatainkból, hogy [Leila esetében a vendégek határozott állásfoglalása hallgatásra tudta kényszeríteni](#), ilyenkor egy távoli sarokba kuporodott, és démoni érzékenységében megsértve, szomorúan pipázott. **De mit kéne tenni egy ilyen Mr. Peter Wong Tung Shunnal, hogy mi is hallgatásra tudjuk őt kényszeríteni? Rejtély. Lehet hogy itt is csak egy ideges bennszülött zsebkése hozhatna hosszútávon üdvözítő megoldást.** Addig is tűnődhetünk, vajon mire kell neki az USD 22500000 méter. Mindenesetre üzleti ajánlatokat továbbra is csak őstermelőtől.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [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/2136372>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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](#) 2010.07.08. 18:17:52

"Patrick Chan"tól naponta kapok legalább egy üzleti ajánlatot a kuka freemailes fiókomba. Tud valamit az arc, minden ajánlatát más címről küldi, csak a név ugyanaz. :DDD

Újabb postafiók, újabb politikus

2010.07.09. 11:11 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [spam yahoo pénz csalás nigériai szenátor](#)

Aki esetleg olvasta a korábbi hírt, amikor [Sarah Palin republikánus elnökjelölt postafiókját feltörték](#), gyaníthatta, hogy a poszt címében szereplő "mit tanulhatunk az esetből?" kérdés nem mindenkinek lesz majd gyakorlati, némelyeknek megmarad költői. **Most végre a demokraták is bebizonyíthatták, semmivel sem alábbvalóbbak, ők is remekül tudnak áldozatul esni**, sőt meg ez nekik lovon és trapézon is.



[Külföldön vagyok \(Skóciában\), nem vagyok elérhető telefonon, ellopták a tárcámat, a nagykövetség még nem reagált, küldj pénzt gyorsan, tízezer font jó lenne a hazajutáshoz](#), később majd megadom - szól az email. Természetesen a levél csalás, vélhetően **Bob Dvorsky a Yahoos postafiókjának** korábbi feltörését nem észlelte, így [jött aztán a klasszikus](#) csalási forgatókönyv.



[Hazai aggyal már az is egyfajta érthetetlen extrém perverziónak számíthat, hogy egy ismert politikus ismeretlen emberektől kérjen kölcsön pénzt.](#) (A klasszikus vicc szerint a híres politikus egy egyetemre látogat, ahol az egyik hallgató az után érdeklődik, mivel készüljön erre a pályára, hogyan lehetne ő maga is politikus. Kinek a pénzét költi fiatalember? - kérdezi a politikus. Hát az apám szokott minden hónapban küldeni egy csekket. Gratulálok fiam, akkor már el is kezdte.)



[Nem csak amerikai, hanem brit politikus is kért már Nigériában állítólagosan ellopott tárcája miatt elektronikus levélben pénzt, ugyancsak egy feltört gyenge jelszóval vagy gyenge emlékeztető kérdéssel védett email fiókja miatt](#) - ezen lehetne/kellene változtatniuk, na meg a rendszeres jelszó cserén is.



Nálunk nem tudni mi lenne a végkifejlet egy hasonló esetben, de ha arra gondolunk, [már Isaura felszabadítására és Esmeralda szemmütétéjére is adakoztak](#), hát nagy valószínűséggel itt is bejönne a spamküldők számítása ;-)

Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Ez történik a weben egy perc alatt](#)
- [Safe mód a Mechagodzilla ellen](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés [trackback címe](#):

<http://antivirus.blog.hu/api/trackback/id/2140340>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 császárnak ami a császáré

2010.07.12. 17:55 | [Csizmazia István \[Rambo\]](#) | [2 komment](#)

Címkék: [uk család](#) [adathalászat](#) [adófizetés](#)

Két biztos dolog van az életben: az egyik a halál, míg a másik az adófizetés. Az Egyesült Királyságban éppen közeledik is egy július 31. bevallási határidő, és létezik egy hivatalos weboldal is, amelyen az ottani állampolgárok eleget tehetnek bevallási kötelezettségüknek. Na vajon mi történik az ezt megelőző időszakban?



A. A garnéla rákok populációjában jelentős és megmagyarázhatatlan gyarapodás áll be, a nők pedig világszerte egyenlő munkáért egyenlő bért kapnak

B. Az olaj világpiaci ára váratlanul és tartósan az 1970-es árszintre csökken, kivéve persze Magyarországot, ahol úgynevezett árfolyamnyilvántartással kapcsolatos többlet kalkulációs kezelési pótköltségek ellentételezése címén még drágul is

C. Óramű pontossággal megjelennek az adathalászok, és a hivatalos weboldalra megtévesztően hasonló oldalakra mutató spameket kezdenek el tömegesen küldözgetni az adóhivatal nevében Usain Bolt sebességű adóvisszatérítést ígérve.



A Trusteer szakértői szerint a bűnözőknek annyira megéri ez a zavarosban való halászás, hogy [a brit állampolgárok jövedelemadó és ÁFA befizetéseivel kapcsolatos csalásukhoz külön botnetet](#) hoztak létre.



Ugyancsak veszélyt jelent, hogy emellett egyre gyakrabban [jelentkeznek az adóhivatal vagy bank nevében telefonáló csalók is](#), akik állítólagos adategyeztetéssel vagy kedvező és gyors adóvisszatérítési ígéretükkel [igyekeznek majd megtalálni a balekjaikat](#). Akik aztán duplán rosszul járnak, mert minden személyes és banki adatuk csalóknak való megadása után egyszer majd az igazi adóhivatalnak is fizetniük kell, [ha addigra marad egyáltalán valami a számlájukon](#).

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Ez történik a weben egy perc alatt](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2146857>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.07.13. 19:26:12

☐ annak, akik azt hiszik, hogy az orvostudomány fejlődése és a ragadozók visszaszorulása miatt a természetes szelekció már nem működik emberek esetén.
Tevednek.



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.07.16. 19:16:21

Kemény, mibe nem nyúlnak bele a hackerek... Bár az "enrolment" szó elég gyorsan megütötte a szememet, így 1 db. l betűvel... :)

Trójai Firefox kiegészítőt tiltottak le

2010.07.15. 13:20 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [firefox plugin extension mozilla trójai sniffer jelszólopó](#)

Ismét egy kétes Firefox plugin miatt van helyzet. A trójai programok, kétes letöltések vagy ismeretlen hatású frissítések mindig alaposan feladják a leckét. A megfelelő hozzáállást talán éppen Senecától leshetjük el: **"Aki mindenkiben megbízik, az éppolyan káros, mint aki senkiben sem."** Mi valószínűleg nem tudunk kibújni a bőrünkől, és többször követjük el az utóbbi hibát az előbbi helyett.



Egyszer [volt már a vietnámi nyelvi kiegészítőben kártevő](#), majd [idén februárban a Master Filer kiegészítő tartalmazott trójait](#), ezért kellett **exkuzálniuk magukat**. Most a "ha valami egyszer történik, az véletlen; ha kétszer, az egybeesés; ha már háromszor, az összeesküvés" jegyében mind a felhasználók, mind a fejlesztők vigyázó szemüket a Mozilla Snifferre vetették, majd rövid úton ki is vonták azt a forgalomból.



[Bebizonyosodott ugyanis, hogy a kiegészítő szerzője jelszóadatokat gyűjtött a plugin használók gépéről](#). Mintegy **1800 letöltést regisztráltak a Mozillánál július 6. és 12. között**, és a gyanú felmerülése után azonnal eltávolították a letölthető kiegészítők közül, sőt figyelmeztetést is küldenek azoknak, akinek a gépére még mindig fel van telepítve.



A Mozilla valószínűleg megpróbál majd szigorítani a korábbi szimpla vírusellenőrzéshez képest, [sőt állítólag már dolgozik is ezen](#), de egyáltalán nincs könnyű dolga. [Érdemes lesz alaposabban is vizsgálnia a plugineket](#), de hasonlóan az AppStore zárt világához [az égvilágon semmi garancia nincs arra](#), hogy a bevizsgált biztonságos kezdeti állapothoz képest [később nem kap egy olyan váratlan frissítést, ami már egy trójai funkcionalitást is tartalmaz](#). [Lásd a jó kis AdblockPlus VS. NoScript csörtét](#).



Persze nyilván mindent felfedeznek és nyilvánosságra hoznak egyszer, **de tegye fel a kezét, akit vigasztalna az, hogy a webes és banki jelszavait pont a kettő közötti ultrarövid pár napos időszakban lopták el és nem pedig egy hosszabb időintervallumban?** Jelentem, az én kezem lent van, és éppen a hideg poharat tartja.



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



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Ez történik a weben egy perc alatt](#)
- ["Szösölmédia" és nyaralás](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2153085>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.07.15. 18:32:13](#)

Hát ha olyan a webes bankom, hogy elég hozzá a netes jelszót ellopni, akkor ássam el magam egy mély sírgödörbe. Jelentkezzen az, akinek nem kell sms-ben megküldött megerősítő kódot, vagy kódgenerátorral generált jelszót beírnia tranzakció előtt.

Ha meg ellopják a 123. kényszer regisztráció miatti jelszavam a mostvalamiertfontoshogyregisztraljak.com oldalról, hát éljenek vele vissza.

Persze a hiba ettől még hiba és nekem is van egy hideg pohár a kezem ügyében. :-)



[WonderCsabo 2010.07.19. 18:46:53](#)

Ez nem plugin, ez extension.



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu> 2010.07.29. 10:39:35](#)

Szia WonderCsabo!

Köszi, javítottam a címet.

[zeugma 2010.08.03. 02:14:14](#)

"ezért kellett exkluzálniuk magukat"

Szerintem exkuzálták magukat.

(Exkuzál: mentegetőzik, bocsánatot kér. Exkluzál: kizár.)



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu> 2010.08.03. 10:05:52](#)

Hello Zeugma!

Megnéztem, köszi, és teljességgel igazad van, én kérem szépen ötven évig rosszul használtam ezt a (excusez moi) kifejezést.

Gyorsan javítom is, és cserkész becsszóra a rákövetkező ötvenben már nyelvtanilag helyesen fogom írni aztat ottan máma ;-)

Új trójaiak a falak között

2010.07.19. 10:00 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

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

Bár a Confickert már kilencedik hónapja nem sikerült eltüntetni a magyarországi vírusstoplista első helyéről, az elmúlt hónapban változott a legfertőzőbb kártevők köre: két új trójai került be a 10-es csapatba.



Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik a hazai felhasználók számítógépeit. A magyar lista első helyét 2009 októbere óta a Conficker féreg tartja, amely az operációs rendszer frissítéseinek hiányát, a gyenge jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed. A csúcstartó kártevő és a lista már megszokott szereplői mellé most két új trójai csatlakozott.



Az ötödik helyen debütáló JS/TrojanDownloader.Pegel először megfertőzi a számítógépet, majd az összes webcímet átirányítja egy oroszországi weboldalra. A kártevő hamis e-mailekhez csatolva kerül a számítógépre, melyek látszólag a Microsoft Outlook terméktámogatásától érkeznek. A Pegel telepítését már a gondatlan felhasználók végzik el. A lista hatodik helyén bemutatkozó Win32/Packed.VMProtect trójai szintén elsősorban e-mailekben csatolva érkezik a felhasználókhoz, majd miután hátsó ajtót nyit a megfertőzött gépeken, rejtve távoli weboldalakhoz csatlakozik, melyekről a háttérben kártékony fájlokat tölt le.



A két új szereplővel együtt most összesen 6 trójai van a toplistán, ami mutatja, hogy a felhasználók hiszékenysége és megtévesztésére épített kártevők a leghatékonyabbak. Ezek hasznos segédprogramnak álcázzák magukat, és így érik el, hogy a gyanútlan felhasználók feltelepítsék őket. A számítógépre bejutva aztán megmutatják igazi énjük: a legtöbb közülük azonnal hátsó ajtót nyit, melyen keresztül további "kártévőcsapatokat ereszt be". A Conficker töretlen elsőségére ugyanakkor magyarázat lehet, hogy a féregből folyamatosan jelennek meg az új variánsok, melyeket készítenek gondosan tesztelnek az antivírus programok ellen.



Érdemes még kitérni az Autorun vírusra is, mely szintén hónapok óta a toplista állandó szereplője. A kártevő terjedését megkönnyíti, hogy külső adathordozókon terjed, ez lehetővé teszi, hogy a legkülönbözőbb helyeken bukkanjon fel. Így például nemrég Ausztráliában és Németországban tapasztalták, hogy több fotókidolgozó automata fertőződött meg. Így a felhasználók, akik USB kulcsaikról vagy memóriakártyájukról feltöltötték fotóikat, az előhívott papírképeken kívül rögtön egy vírussal is gazdagabbak lettek. Az Autorun terjedésének csökkenéséhez szükség lenne arra, hogy a felhasználók kikapcsolják a külső adathordozók automatikus futtatását Windows operációs rendszer alatt, de úgy tűnik, hogy nem szívesen mondanak le erről a kényelmi funkcióról.



Az ESET több százezer magyarországi felhasználó visszajelzése alapján statisztikai rendszere szerint 2010 júniusában a következő 10 károkozó terjedt a legnagyobb számban, és volt felelős együttesen az összes fertőzés 31,34%-ért.



1. Win32/Conficker féreg

Elterjedtsége a júniusi fertőzések között: 7.29%

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 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 válnak a megfertőzött számítógépen.



A számítógépre kerülés módja: Változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható a külső meghajtó fertőzött Autorun állománya miatt.

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

2. Win32/Agent trójai

Elterjedtsége a júniusi fertőzések között: 4.95%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (például Temp mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett kulcsokkal gondoskodik arról, hogy minden indításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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

3. INF/Autorun vírus

Elterjedtsége a júniusi fertőzések között: 4.36%

Működés: Az INF/Autorun egyfajta 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/autorun>

4. Win32/PSW.OnLineGames trójai

Elterjedtsége a júniusi fertőzések között: 3.33%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött

számítógépen leplezni, eltüntetni. 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. JS/TrojanDownloader.Pegél trójai

Elterjedtsége a júniusi fertőzések között: 3.02%

Működés: A JS/TrojanDownloader típusú kártevők általában veszélyes állományokat tartalmazó weboldalakra irányítja át a felhasználót, illetve onnan igyekszik letölteni/letöltetni további kártékony kódokat. A Javascript kártevővel való fertőzésnek jól látható nyomai is vannak például megjelenik egy "The NTVDM CPU has encountered an illegal instruction" hibaüzenet ablak. A JS/TrojanDownloader.Pegél működése során az összes webcímet átirányítja egy adott oroszországi weboldalra.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



6. Win32/Packed.VMProtect trójai

Elterjedtsége a júniusi fertőzések között: 2.49%

Működés: A Win32/Packed.VMProtect trójai bemásolja magát a Windows/System32, a Temp és/vagy a Windows mappába, ahol különböző DLL állományokat hoz létre. Ezek automatikus lefuttatásáról úgy gondoskodik, hogy a Rendszerleíró adatbázisba bejegyzéseket készít. Ezzel biztosítja magának a betöltődést a rendszer indításakor, illetve a legtöbb esetben külön szolgáltatást (szervízt) is létrehoz. Különböző portokon képes hátsó ajtót nyitni, melyen keresztül távoli weboldalakhoz csatlakozik, és a háttérben fájlokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



7. INF/Conficker vírus

Elterjedtsége a júniusi fertőzések között: 1.93%

Működés: Amennyiben böngészés során az autorun.inf fájl valamely egység főkönyvtárába kerül, akkor a betöltő eléri, hogy a kártevő kódja elinduljon. Vagyis az INF/Confickernek az a szerepe, hogy betöltse magát a Win32/Conficker kártevőt.



A számítógépre kerülés módja: Fertőzött weblapról, vagy külső eszközön keresztül.

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



8. Win32/VB féreg

Elterjedtsége a júniusi fertőzések között: 1.46%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) főleg 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 júniusi fertőzések között: 1.43%

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 hoz létre, illetve módosítja azokat, ha már léteznek. Ezenkívül megkísérel a google.com webcímet is csatlakozni. Működése során tönkreteszi a merevlemez partíciós tábláját.



A számítógépre kerülés módja: A felhasználó maga telepíti.

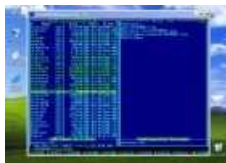
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21mebrook>



10. Win32/Packed.Autoit trójai

Elterjedtsége a júniusi fertőzések között: 1.08%

Működés: A Win32/Packed.Autoit fájlokat hoz létre a C:\Windows\System32 mappában különböző neveken, például autorun.inf, winlogon.exe, svchost.exe. A kártékony EXE fájlok automatikus lefuttatásához külön Registry bejegyzéseket is készít. Működése során hátsó ajtót nyit a megtámadott gépen, majd különféle weboldalakhoz 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/%21packed-autoit>



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



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Ez történik a weben egy perc alatt](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2155963>

Kommentek:

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

[PSPRovocative pr ügynökség \(törölt\) 2010.07.27. 10:57:56](#)

Szerinted meddig marad még a Conficker az első? :-)



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.07.29. 10:43:40](#)

Még egy darabig biztos :-) Lehet, hogy felteszem majd az oldalra egy szavazó dobozba, lássuk ki mit saccol rá, lehet tipp mixelni.



[manson karcsi • http://goo.gl/FVvVX](#) **[2010.08.10. 08:33:16](#)**

a toplista nagy többségénél a pebcak hibából lehet kiindulni.

Bővült a supercsoport

2010.08.02. 11:45 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [online vizsgálat](#) [kártévő](#) [virustotal](#)

Egy új taggal immár negyvenkettő biztonsági program ellenőrzi a VirusTotal oldalra feltöltött gyanús állományainkat.



A SUPER AntiSpy [néhány napja hivatalosan is bekerült](#) a motorok közé, és bár még a dokumentáció/névjegy részben egyelőre nincs feltüntetve, de [a vizsgálatoknál már működik](#). A SAS egy 2004-ben alapított amerikai cég terméke, amely kifejezetten kémprogramok észlelésére készült. A kémprogramirtó ingyenes változata csak kézi keresésre, míg a fizetős változata már valós idejű védelemre is alkalmas. A Panicware cégnév inkább azoknak lehet ismerős, akik használták korábban a fejlesztők egy másik programját, a Super Ad Blocker alkalmazást, mellyel blokkolhatóak a flash, popup, popunder, Messenger, stb. alatt megjelenő kénytelen reklámok.



Három éve a [Virusok Varázslatos Világa legelső része](#) is foglalkozott az akkor még 32 víruskeresőt egyesítő Virus Total oldallal annak apropóján, hogy a weboldal magyarul is elérhetővé vált. Azóta is folyamatosan fejlesztenek a spanyol Hispasec munkatársai.



A motorok bővítése mellett az EXE típus elemzéseire is hasonlóan az igen sebezhető PDF formátum vizsgálatához is integráltak egy PDFID fejlécelemző programot, de a vizsgálat sebességére is jótékonyan hatott, amióta a kereső motorok immár nem egymásután ABC-ben rontanak neki a vizsgált kódoknak, hanem csoportokban párhuzamosan, és a kijelzés menetközben rendezzi aztán őket találati listába.



Ezekon kívül nem csak a hagyományos weboldali feltöltési módszer használható már a vizsgálatához, hanem küldhető a minta e-mailen keresztül is, de lehetőség van a VirusTotal Uploader telepítésére is, amelynek segítségével a Windows Intézőbe beépülő helyimenüjéből egy jobb egérgérintéssel is elküldhetjük a vizsgálandó állományt.



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



• [1 trackback](#)

Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- [Dropbox csálival terjedtek a kémprogramok](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés [trackback](#) címe:

<http://antivirus.blog.hu/api/trackback/id/2192661>

Trackbackek, pingbackek:

[Trackback: Bővült a szupercsapat](#) 2010.08.02. 13:33:59

Egy új taggal immár negyvenkettő biztonsági program ellenőrzi a VirusTotal oldalra feltöltött gyanús állományainkat...

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.

Minden, amit a privacy-ról tudni akartál... I. rész

2010.08.04. 17:10 | [Csizmazia István \[Rambol\]](#) | [20 komment](#)

Címkék: [privacy](#) [facebook](#) [privátltét](#)

... de sosem merted megkérdezni, éppen hiányoztál vagy mást csináltál. **Háttér információk a Facebook előéletéről, gyűjtemény eddigi privacy incidensekről, temérdek példa linkkel**, meggyász, és még több meggyász. Összefoglalva: az életben csak egy szép dolog van, de az most épp nem jut eszünkbe :-)



Pár hónapja kezdtünk bele ebbe a mindent egy helyre összeszedésbe, és bár ezek részleteiben már szerepeltek itt-ott, így egyben most először jelenik meg. Az ["Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót"](#) eset adta az apropót és a végső lökést, hogy ezúttal **megdöntsük a Guinness Rekordok Évkönyvébe kívánczós leghosszabb blogposzt rekordot**. Remélhetőleg aki végig tudja olvasni, az talán nem azt fogja mondani, hogy inkább egy teletubbies maratonnal amortizálja le az agyát, mintsem ezt még egyszer végig kelljen szenvednie, hanem örülni fog ennek az írásnak. Ígérjük, nem lesz gyakori az ilyen gigászi méret.

Nehéz dolog a privacy-ról írni, mert egyrészt elég **összetett dolog, másrészt időben állandóan változó folyamatról van szó**. Személyes adataink egy részéről amúgy sem tudunk mindig rendelkezni: jól-rosszul őrzik a különféle hivatalokban, szabályozzák vagy nem szabályozzák ki is tekinthet bele, be tartják vagy nem tartják be a titkosítási előírásokat, az adatbázis kezelés során olyan támadható pontokat hagynak, amik miatt az kiszivároghat, ellophatják, stb. Ezek miatt különösebben aggódni nem érdemes, nem tehetünk semmit, vagy maximum szavazzunk négyévente olyanokra, akik ezt állításuk szerint komolyabban vigyázzák :-)



Nem egyértelmű, ki tehet jobban a jelenlegi káoszról: a felhasználók, akik nem olvassák el az adatvédelmi irányelveket, vagy az ezt vastagon kihasználó, és a szétkürtölést alapértelmezettnek beállító üzemeltetők. Az adatkezelési szabályzatának egyik pontja szerint az abban foglaltakat bármikor egyoldalúan módosíthatják - de nincs ez másként a magyar Iwiw esetében sem. Lehetne persze minden alaphelyzetben biztonságos állapotban, de akkor a "felhasználói élményre" hivatkozva nem tudnának tömeges forgalmat generálni. A forgalmi, viselkedési, kapcsolati adat pedig érték, a reklámozni kívánó cégek pénzt fizetnek érte az üzemeltetőknek.

<http://hu-hu.facebook.com/privacy/explanation.php>

A problémák gyökere nem is azokkal a személyes adatokkal van, amit közintézmények hivatalból őriznek, kezelnek, hanem **inkább azokkal, amiket mi magunk kezelünk jól-rosszul: megadjuk, és nem gondoljuk végig**, vagy a folyamat később megváltozhat ahhoz a pillanathoz és szerződési feltételekhez képest, amikor regisztráltunk. Amíg egy olyan ingatlanközvetítő, [autópálya e-matracát árusító cég is van](#), amely orvul menet közben módosítja ezeket a szerződési feltételeket, és a sűrű fillér alapon mindenkitől bevasalja azt utólag, adataink, pénztárcánk veszélyben vannak. [Az egyes álláskereső, társasági, társskereső oldalak is kérdezhetnek túlságosan is bizalmasakat](#), illetve **a jelentkező is gondolhatja azt, jót tesz az esélyeinek a részletes, önfeladós válaszai, vagy adott esetben nem tudja ezeket elkerülni, ha eredményt akar**. A drogozott-e már, sorolja fel negatív tulajdonságait, akar-e gyereket, milyen a szexuális orientációja, adja meg levelezési postafiókjainak jelszavát - **nem éppen szokványos állásinterjú kérdések**.

Ilyen szemszögből **akár úgy is vélhetjük, lehetetlen tökéletes biztonságban lenni**, például elég a csalóknak egy hamis álláskereső irodát létrehozni, és máris áramlanak a címek, részletes önéletrajzok. Persze amint hibák minden programban vannak, minden közösségi portálon is lehetnek. Például [egy programhiba miatt a felhasználók elolvashatták az összes Facebook ismerősük csevegését](#). **Ki tudja mennyi ideje, esetleg évek óta volt ez így?**

Facebook tagok leszünk, mert megérdemljük

Ha nem is ilyen szélsőséges esetekről fogunk most beszélgetni, de alapvető ökölszabályokról, és gyakorlatias megközelítéssel minden beállítási javaslat mellett hétköznapi példákkal is szemléltetjük annak veszélyét is, mi történhet a megfelelő beállítás elmulasztása esetén. **Az 1000 legnépszerűbb oldal listáját a Facebook vezeti napi 570 millió látogatóval**. A közösségnek pedig már több mint 400 millió aktív felhasználója van a regisztrált 500 millióból. [Átlagosan minden tagnak körülbelül 130 ismerőse van, a tagok pedig havonta mintegy egymilliárd képet töltenek fel](#). Emellett 70%-uk valamilyen alkalmazást, játékot is futtat az oldal kínálatából. Mindegyikük kapcsolódik 60 további oldalhoz, csoporthoz, rendezvényhez és minden hónapban körülbelül 70 új tartalom (bejegyzés, üzenet, kép, videó) hoz létre.



Hibátlan program nem létezik, csak olyan, amely eddig esetleg hibamentesen futott le. [Egy érdekes török internetező, Ozan Yılmaz vette észre](#), hogy egy egyszerű script kód segítségével bárkit a Twitter követői közé tud varázsolni. Egy másik esetben [a Facebook értesítő leveleiből kinyerhető volt az eredeti feladó IP címe](#). Ezeket a hibákat azóta állítólag már kijavították. Vajon hány lehet még?

Nagyon fontos persze az is, hogy az üzemeltetők ezt helyesen kezelik-e, de ezt csak remélhetjük. Amire viszont nekünk, felhasználóknak befolyásunk van, az hogy jól átgondoltan, és **saját érdekeink mentén csak annyi adatot, képet, információt adjunk meg, amit később biztosan nem bánunk meg.** Jöjjenek hát ehhez a részletes tanácsok.

Szervezzük barátainkat listákra

Bármivel előfordulhat, hogy főnöke, anyósa meghívót küld számára. Ha okosan szervezzük ismerőseinket, akkor külön csoportba tesszük családtagjainkat, munkatársainkat, kollégiumi osztálytársainkat. A listáinkat más nem láthatja, mi pedig könnyen tudunk így egy adott célcsoportnak üzenetet küldeni. Elrontani is nehezebb a címezett, például **elég rosszul veszi ki magát, ha a barátok helyett péntek délutáni "a munkahely nem kocsma, hogy állandóan ott legyünk, indulok is haza"** üzenetünk a munkatársaknál, főnököknél landol.

Állítsuk be a "Beállítások -> Adatvédelem Beállítások -> Profil menüpont" alatt, mit engedélyezünk

A beállításokkal elvileg meghatározhatjuk, kinek és mibe engedélyezünk bejelentést. A lehetséges választások a csak a barátok, a barátok és csoportjaim, a barátok barátai, és a mindenki között mozoghat. **Sajnos az alapértelmezés gyakran a bátor megosztás, így ha valaki lusta, figyelmetlen, vagy csak mert megjíj a huszon-egynéhány opció szerkesztgetésétől, az minden mozdulatát, mondanivalóját kisugározza a Világegyetemnek**

Mit oszthatnak meg rólunk az ismerősök

Érdemes az "Adatvédelmi beállítások -> Alkalmazások és Weboldalak" résznél korlátozni az "Információk, melyeket ismerőseid alkalmazásokon és weboldalakon keresztül tudnak megosztani rólad" opciókat. Van itt állapot frissítés, online jelenlét, vallási és politikai nézet is. **Ha valaki éppen politikusnak készül, és a megfelelő imázst akarja magáról kisugározni, akkor persze kipipálhat itt mindent**, de valószínűleg az átlag felhasználónak erre nincs szüksége.



Minden egyes alkalommal, ha például a 83 millió virtuális farmer valamelyike a FarmVille mezőgazdasági szimulációs játékkal, vagy a MafiaWars-szal játszik, megengedi, hogy letöltsék a profilját és továbbadják az adatait egy harmadik félnek. Az ismeretlen harmadik féllel pedig semmilyen szerződéses viszonyban nem vagyunk.

Rendelkezzünk körültekintően a fotóalbumaink megtekinthetőségéről

Érdemes gondolni arra, ha családi vagy nyaralási képeket töltünk fel, akkor szabályozzuk azok megtekinthetőségét. Itt személyre, vagy csoportokra bontott lehetőségek között lehet választani. **Ha ezt nem tesszük meg, olyasfajta kellemetlen élményekre ébredhetünk, mint a választási kampányban némely politikus.** Egyre több kamera egyre több felvételt készít egyre több fiatal részegeskedéséről. **Az idő múlik, és tisztes családapaként nem hiányzik egy rosszakaró, aki kettőtöri karrierünket fiatalkori botlásunk miatt.** Vessük az eszünkbe, az adatok a legnagyobb biztonságban akkor vannak, ha egyáltalán fel sem töltjük őket.

Ki láthatja a kommenteket?

Azt is be tudjuk állítani, látszódnak-e a kommentek az összes ismerősünk üzenő falán. **Külön beállítható, hogy a kommentjeink, vagy "lajkjaink" a fotóknál, üzenetknél, linkeknél, videóknál láthatóak legyenek-e mindenki számára, vagy sem.** "Ügyelj, hogy senki se lásson át rajtad teljesen, mert a találgatás és kétség, vajon mennyire vagy képes, több tiszteletet kelt, mint szellemi kincseid pontos ismerete, bármily nagyok is legyenek azok." (Gracián)

Hirdetések, broáffff

Érdemes a Fiókbeállítások - Facebook Hirdetések menüpontnál az "Engedélyezem, hogy a főoldalakon rólam szóló hirdetések jelenjenek meg az alábbi személyek számára" pontnál a "csak az ismerőseim" helyett a "Senki"-t választani. Bár a kedves fülszöveg arról tájékoztat, hogy a Facebook soha nem adja át a felhasználók nevét és fotóit harmadik reklámozó félnek ([muahahaha](#)), de Mózes tábláival ellentétben ez itt nincs kőbe vésve, és bármikor egyoldalúan megváltozhat, például "Csak akkor, ha ezért cserébe x csillió dollárt kínálnak"-ra.



Volt egy Fan Check nevű Facebook alkalmazás is, amely elméletileg profilunkon keresi meg, hogy mely ismerősünk írt/kommentelt a legtöbbet a dolgainkra. Ehelyett azonban a kezdőlap összezavarását és egyéb káros mellékhatásokat lehetett tapasztalni

Az online paraszt nem kérkedik, nem fuvalkodik fel, nem viselkedik bántóan

Szinte hihetetlen, de még a gazdasági válság alatt is sokan vannak, akik megkockáztatják, hogy játsszanak munkaidőben a munkahelyi gépükön, ráadásul a napi öt aratásról folyamatosan küldik az értesítést barátaik, ismerőseik, főnökeik felé. Emelje fel a kezét, aki már legalább végignézte a Facebookon a "Profilom - Adatvédelmi beállítások - Alkalmazások és Weboldalak" idevágó lehetőségeit. Huh, senki? Nos akkor elmondanánk, van itt egy "Események az alkalmazásokban és a játékok kezelőfelületein" opció is, érdemes lehet beállítani a "Testreszabás - Csak én" opciót. Íme egy elrettentő példa. [2010 márciusában kirúgták egy bolgár város önkormányzatának egyik tagját](#), mivel a költségvetés tárgyalása helyett inkább virtuális tehenét fejte a Facebook népszerű, FarmVille nevű játékában, és pechére ezt mások is észrevették. Vajon mit nem állított be az illető?

Állítsuk be részletesen a kereshetőségünket

Lehetőség van beállítani az Adatvédelem -> Keresés menüpontnál, mi látszódjon. Nyilván adatvédelmi szempontból az a legrosszabb, ha minden publikus a fotóktól kezdve ismerőseink listáján át azoknak az oldalaknak a listájáig, amelynek rajongói vagyunk. Tartozik ez tényleg másra?

Csoportokhoz csatlakozunk

Vegyük górcső alá a csoportok, fan klubok kérdését. A klasszikus Shakespeare idézet szerint ezt mondja Polónius: "No lend, and no borrow" (Arany János veretes fordításában "kölcson ne adj, ne végy!"). Ha Polónius ma élne, intelmei között biztosan szerepelne valami ilyesmi is: "És közösségi oldalakon vala ne csatlakozzál te semminemű ismretlen csoporthoz, mert sosem tudhatod vala, mily szándékú halandók valának annak tagjai, és idővel milyen czélokot fognak követni". Van-e értelme egyáltalán ismeretlen klub tagjának lenni? Mi is történik ilyenkor, nézzük meg. Belépünk a Dr. Schön Ubul Ferencvárosi Szurkolói Körbe, vagy az "Új Élet" Koporsókészítő Kisipari Szövetkezet Barátai közé és nem tudjuk pontosan, kié a klub. Nem tudjuk, kik a tagjai. Mi Róbert bácsiként önként odaajándékozunk nekik a bizalmas személyes adatainkat. **Nem tudjuk, milyen adatkezelési irányelveket vallanak magukénak, ha egyáltalán hallottak ilyesmiről.** Nem tudjuk, milyen körülmények között tartják nyilván az adatainkat. Nem tudjuk, eladják-e harmadik félnek, ha kapnak egy jó ajánlatot. Nem tudjuk, nem lopják-e el egyszer tőlük, mert abc123 típusú jelszót választott magának a klubelnök.



Lehet persze csak névvel és egy darab fotóval is fent lenni, és közben okosnak gondolni magunkat. Nem árt tudni azonban, hogy amikor a Facebook eladhatja az adatainkat, akkor annak csak egy kisebb része az esetleg nem kitöltött személyes adat. Ennél is érdekesebb és értékesebb lehet a kapcsolati háló, az üzeneteink, és rendszerbeli viselkedésünk, eddigi kattintásaink története.

Ugyan mit árthatnak nekem?

Ideje leszámolni az "[Én egy egyszerű hétköznapi ember vagyok, ugyan mit tudnának nekem ártani a számítógépes bűnözők](#)" című téveszmével. Meglepő módon azt is mondhatjuk, [csatlakozni egy Facebook csoporthoz kockázatosabb, mint egy direkt linken érkező kártevőre kattintani](#). De miért-e nagy maliciózus kijelentés? Íme példaként egy olyan Facebookos csoport, amelyik [eredetileg magasztos és pozitív célok érdekében alakult: a Haiti földrengés áldozatainak gyűjtöttek adományokat](#). **Csalók azonban megváltoztatták csoport nevét Svéd Nekrofilek Egyesületévé**, sőt még egy üzenetet is kiírtak a csoport weboldalára: "Ahogy mindnyájan tudjátok, a Svéd Nekrofilek Egyesülete 500 ezer koronát adományoz arra a célra, hogy a Haitiról visszahozott holttestek minél jobb állapotban legyenek, hogy közöskülhessünk velük". Egyáltalán nem vicces a dolog, és **valószínűleg senkinek nem hiányzik, hogy a nevét leendő munkaadója egy ilyen tömörülésben találja meg**. Egy érdekes felmérés szerint az amerikai [személyzetisek 70%-a utasított már el állásra jelentkezőt amiatt, hogy negatív lett a közösségi oldalakról begyűjtött információ](#) a jelöltől. Figyelemreméltó naivság, hogy ennek ellenére a leendő álláskeresőknél mindössze csak a 7%-a gondolja úgy, hogy ezek az adatok egyáltalán befolyásolhatják a pályázatukat.

Ki van a túloldalon?

[Egy 2008-as tanulmány szerint a Facebook-profilok negyven százaléka nem valódi](#). Valószínűleg bűnözők regisztrálnak már eleve csalási céllal. Ha valakinek ezernél is több barátja van, vajon ismerheti személyesen mindet? [Tom Scott elkészített egy olyan Evil nevű demonstrációs alkalmazást](#), amellyel felhasználók telefonszámait gyűjtötte ki egészen könnyedén. **Hányan lehetnek, aki ötletszerűen telepítenek ismeretlen Facebook alkalmazásokat? Vagy kattintanak egy olyan linkre, amit egy ismeretlen Facebook partner küldött.** Egy új oldalon aztán újra be kell lépni egy Facebook oldalhoz megszólalásig hasonló oldalra, egy óvatlan kattintás után azonban kikerülhet a jelszavunk. [A feltört fiókok pedig hasznosak lehetnek a bűnözőknek további látszólag ismerősök nevében küldött csaló pénzgyűjtő üzenetekhez](#). Magyarán az ember a postafiókjára nem csak saját maga miatt, hanem **ismerősei védelme miatt is** kell, hogy vigyázzon.



Egy olyan biztonsági elem is található a Facebookon, amellyel a Gmailhez hasonlóan kézben tarthatjuk, milyen IP címről jelentkeztek be legutóbb fiókunkba. Kérhetünk emailes riasztást az esetleges idegen belépésről.

A csalóknak három dolog kell: pénz, pénz és pénz

Mire lehet használni ilyen személyes adatokat? Hát először is lehet szipkázni olyan infót, amivel jól válaszolhatunk a jelszó-émlékeztető

kérdésekre. De új típusú csalások is terjedőben vannak, például a személyes lapról kinézett barátok nevében Facebook üzenetet írnak az áldozatnak, hogy [állítólag elvesztették a reptéren a mobiljukat, útlevelüket](#). A feltört fiókok így jól felhasználhatóak csalásra. Látszólag az ismerős nevében lehet üzenetet küldeni a barátoknak: „**Hello, Londonban vagyok, ellopták a pénztárcámat, tudnál nekem pénzt küldeni?**” Több alváltozat is ismeretes, de a lényeg, [gyorsan egy kevés pénzt segítséget szeretnének kérni](#), általában a Western Unionon keresztül. Ha valaki pedig segítőkész és bedől, keresztet vethet az ilyen átutalt pénzre. És mindig lesz, aki küld. Nyilván **nem lehet figyelmen kívül hagyni a magyar felhasználókat sem, körülbelül 1.3 millióan lehetnek**, és egy részük beszél angolul, vannak külföldi barátaik, ismerőseik.



"Dolgozzál te hélóta, mert jönnek a spártaiak" Vegyük észre, az internet világában nincsen undo. Ha valaki meglegfelvonuláson vett részt, pornosztárként kereste a betevőt, füvet szívott, vagy a Kék Osztriga Bár törzsvendége volt és erről képek is készültek, akkor azok szépen elő is fognak kerülni a megfelelő pillanatban: ha választások közelednek, vagy egy állás sorsa forog kockán. [Külön üzletág lett a lejárató információk megrendelése, bányászata.](#)

Facebook accountot adok-veszek

A VeriSign kutatói egy olyan weboldalra bukkantak, amelyen akár másfél millió, lopott Facebook felhasználónév és jelszó is könnyűszerrel beszerezhető. A Facebook - és a többi hasonlóan népszerű közösségi webhelyen - iparággá vált az adatlopás és az adatokkal való visszaélés. **Ezt támasztja alá a VeriSign bejelentése is**, amely szerint egy cracker különböző [internetes fórumokon nem kevesebb, mint 1,5 millió lopott Facebook felhasználónév és jelszó értékesítésbe fogott](#). A biztonsági cég szerint nem is sikertelenül, hiszen a bizalmas adatokból már közel 700 ezer el is kelt. De a 2010 júliusban kikerült [100 millió Facebook felhasználó adataira is sokan rámozdultak](#) a cégek és szervezetek közül.

Alkalmazásokat telepítünk, jujj de izgi

Volt aztán egy Fan Check nevű Facebook alkalmazás is, amely elméletileg profilunkon keresi meg, hogy mely ismerősünk írt/kommentelt a legtöbbet a dolgainkra. A gyakorlatban ehelyett azonban a kezdőlap összezavarását lehetett tapasztalni, és nem mindig jelenítette meg az új postokat sem, néha régiakat tett előre, stb. Összefoglalva: "Elméletileg nincs különbség elmélet és gyakorlat között. Gyakorlatilag van." **Nem egyedi eset a Fan Check, divat lett a dologból a Facebook kiegészítők háza táján**, és [ezekből a kártékony kisalkalmazásokból egy egész csokorra valót nevez meg Roger Thompson, az AVG szakértője](#). Néhány hónapja keletkezett egy vakriadó a Facebookon, amiben arra hívták fel a figyelmet, ha valaki egy "unnamed app", magyarul névtelen alkalmazás nevű holmit talál magánál, akkor azonnal törölje, mert az állítólag kémprogram. Persze nem az, de az már az ötletgazdák képzelőerejét dicséri, hogy **a Google találatok kártevőkkel való mérgezésével rákészültek a szituációra, ha az egyszerű Facebook jüzer rákeres az "facebook unnamed app" kulcsszóra**.



Temérdek különböző adatvédelmi beállítás. Van akit ez elriaszt attól, hogy egyáltalán állítgasson bármit is. És az alapértelmezett állapot rendre "igen, az egész Univerzummal meg akarom osztani" opció. A sűrű cikkezés hatására talán végre elindult egyfajta öntudatra ébredés.

Száz barát négy nap alatt

Nem mindenki az, akinek mondja magát - ehhez még Arsene Lupin rajongónak sem kell lenni, mindenki megtapasztalhatta már.

Emberünk gondolt egyet, hamis néven beregisztrált a Facebookra - de megtehetette volna bárhol máshol is - és összeállított egy kamu adatlapot. Kellett hozzá egy új e-mailcím, majd jött a hasraütésszerű keresztnév választás - valami jól csengő, hangzatosra volt szükség - és ezt keresztelte aztán a blogjában használt álnevével, és máris megszületett Dolus Carlsson. Aztán kell még egy vonzó fotó - esetünkben ez Marcus Vick, 183 cm magas, 93 kg-os amerikai profi footballistát ábrázolja, de se baj ;-), és máris lehet tölteni az adatlapot. Egy-két véletlenszerűen kiválasztott egyetem, középiskola, klub bejelölése csodát tehet. **Máris indulhat a "Kit ismerhetek?" című népi játék**. Az első harminc perc nehezen akart eltelni, de végül szép részeredménnyel zárult: tíz "barát" megszerzése volt a scalp, megtört a jég. Innentől már olyan ez, mint a kitüntetések száma Brezsnyev mellkasán: akinek már van, az minden piros betűs ünnepen kap egy újabbat, csak a legelsőt olyan pokoli nehéz megszerezni. [Alig négy nap leforgása alatt ennyi ismerősre lehetett szert tenni](#). Itt még csak nem is arról van szó, hogy valaki nem ismer minket és téved, amikor azt gondolja, mégis ismer, hanem ez a profil egy a valóságban nem is létező személyről szól, és mégis vannak ismerősei. Igen, vannak, és akiknek ugye Dolus Carlsson például már láthatja is a részletes adatlapját. És **a statisztikák keményen azt mutatják, hogy az ismerősöktől érkező levelek, üzenetek, linkekre aztán már sokkal könnyebben kattintanak az emberek**.



Egy social engineering-kísérlet a Facebookon. Egy hamis profil, nem létező adatokkal, egy élvonalbeli sportoló képét kölcsönözve három nap alatt több mint száz „barátot” eredményezett. Vajon mi járt a kapcsolatként megjelelő emberek fejében? Az biztos nem, hogy mostantól az új „ismerős” akár beláthat a személyes adatlapjukba is

Sarah Palin postafiókja

Már a [Sarah Palin email fiók feltörési esetnél látszott](#), nem célszerű ész nélkül minden személyes adatot túlzottan ki tacepaozni a közösségi oldalakra. Mi is volt ott a probléma? A módszer nem feltörés, nem jelszó találgatás volt, hanem új jelszó igénylése. A születési hely és idő megszerzése nem okozott gondot, a titkos ellenőrző kérdés pedig az volt, hol ismerkedtek meg a férjével. **A dolog érdekessége, hogy erről is beszélt már nyilvánosság előtt - és ez egy középiskola neve volt.** Innentől már meg is volt oldva a dolog. A Sophos érdekes párhuzamot vont - és nagy valószínűséggel igaza is van - a korábbi Paris Hilton PDA telefonjával és feltört mailboxával kapcsolatosan. Ott az ismert celeb (brrr, de szörnyű egy szó ez) kedvenc állatának neve volt a jelszó emlékeztető kérdés. Az ismert és kevésbé ismert embereknek komolyan el kellene gondolkodniuk, érdemes-e olyan adattal védeni bármit is, amit a bűvárlapok lapok hetente megírnak, vagy valaki önként kiplakátolja az IWIW-es lapjára. **Ez kb. olyan szimpla akadály, mintha Kíszel Tünde jelszava "Donatella" lenne.** Persze sok helyen van lehetőség saját ellenőrző kérdést írni - ezt érdemes is kihasználni - ezekben is alkalmazni lehet a fenti okosságot, ez pedig jócskán csökkentheti a találgatási lehetőségeket. Hogy hívják a kedvenc tanárodát? Csütörtök - hangzik a válasz, és ez egy jó válasz. Melyik kórházban született? Lekváros palacsinta fahéjjal.

Itt vagyok, most fordulok be a sarkon...

A [Pleaserobme.com honlap egészen érdekes dolgot mutat meg](#): nagyon sokan interurbán realtime közvetítésként osztják meg életünk minden apró rezdülését a nagyérdeművel. Az általuk mellékelt keresési javaslattal élve magunk is meggyőződhetünk arról, hogy éppen ebben a pillanatban is milyen sokan közlik a pillanatnyi helyzetüket. Nem kell GPS vagy okostelefon póráz a munkaadónak, de [a betörők is minden bizonnyal örülnek az ilyen nüanszokra kihegyezett részletes online közvetítésnek](#), mert frankón látszik, hogy lesz még idő kivinni a plazma Tv-t is a teherautóba. Pláne, ha még a "nyaralni mentünk Mallorcára, hurrá" kezdetű blogpostot is olvasták.



Ha vásárolunk egy új kamerát vagy telefont, az úgynevezett extrák közt szerepelhet olyan funkció, amivel "egy kattintással" megoszthatunk képeket, videókat. Szerintünk ez nem hogy nem extra, hanem inkább hátrány: egy óvatlan vagy véletlen kattintással egy soha nem törölhető tartalmat is feltölthetünk

A wifi kapcsolatom neve: Dr Kovács III. 2.

Szóval nem éppen praktikus dolog ilyen percre kész üzenetekkel részletesen beszámolni pillanatnyi helyzetünkről, ez szinte felhívás keringőre, gyere és törjél be hozzám. Aztán a wifi kapcsolatokról szóló elmélkedéseink közben is felmerült, [ha már neten gyerekjáték elérni az összes hálózati eszköz gyári jelszavát](#), akkor az "okos pilóta alagútban nem katapultál" mintájára kevésbé szerencsés **alapértelmezetten hagyni a jelszót**, vagy Dlink, Linksys, Dr. Kovacs III.2. neveket adni a WiFi kapcsolatunknak. A legjobb valamilyen semleges (txk15), vagy az üres, de láttunk már a belvárosban "Vége az ingyen netednek te kecsége" nevet is. Az antivírusokkal kapcsolatban is van pár elgondolkozni való. Ebből az egyik érdekesség, mennyiben hasznos a különböző AV cégek bevett gyakorlata, amely referencia listákat tesz közzé a weboldalán, ezen ügyfeleink használják a mi megoldásunkat. Mint az közismert, minden etikus hackelés (penetration teszt, audit de a valódi rosszindulatú célzott támadások többségénél is) úgy kezdődik, hogy első lépésként feltérképezik az adott cég infrastruktúráját, hálózatát, az interneten elérhető publikus konkrétumokat. [Ahogy az Aurora eset kapcsán is írták: "kiválasztják célpontjukat és alaposan tanulmányozzák azt: utánanéznek milyen és mennyire sebezhető alkalmazói programokat futtatnak a cégnél, mely gyártó\(k\) vírusvédelmét alkalmazzák, hogy azok megkerülésére kézzel tuningolt, "láthatatlan" támadó-kódot \(ún. exploit-ot\) és kártevőt készítsenek"](#). Látható, hogy egyáltalán nem előny ilyenkor, ha mindent biztosan lehet tudni, hiszen ezzel muníciót szolgáltatunk arra nézve, milyen válogatott exploitokat érdemes keresni egy esetleges támadáshoz.

Emberek, figyelem, én az xy antivírust használom ám

Hasonló a helyzet amikor a levelezésünkben szerepelnek azok a záró sorok, hogy az XY vírus 123456 adatbázissal ellenőrizte ezt a levelet. Ha ez minden kimenő levelünkben szerepel, ezzel is felesleges információkat osztunk meg mindenkivel. Az ingyenes antivírusoknál valószínűleg mindez nagyobb gondot okozhat, ha a nyilvánosságra került sebezhetőség és az azt befolyásoló biztonsági javítás reagálási sebességét nézzük. De még a fizetősök esetében is gondolkodhatunk úgy, nem kell a ház homlokzatának vagy a kerítésének hivalkodónak lennie, [elég ha mi tudjuk milyen biztonságos és szép a lakásunk belülről](#). Sokan "nem gondolták úgy", hogy az ilyen talkative magatartásból bármilyen hátrányuk származna, ezért sokan szórják ezt az alapértelmezetten bekapcsolt opciót minden címzettjük számára. Összefoglalva: dolgozzon csak meg a betörő, feltörő, ha akar valamit, ne mi nyújtuk a fejünket tálcán. Amikor amúgy is túl sok adatot tárolnak rólunk mindenfelé, mi magunk ne könnyítsük meg ezt. Másképpen fogalmazva ahogy Moldova György írja: **"a saját akasztásunkra ne vigyünk kötelet, legyen a hóhérnak is valami rezsije"**.

Lekáderezés for Dummies

Ha valaki megnézte a Kaméleon című magyar filmet, az azt is el tudja képzelni, hogy a következő áldozatot behálózni akaró, behízelgő modorú sármór először [a Facebookon néz körül](#): mit szeret a kiválasztott célszemély, operát, kiscicát, Horvátországot, hogy lehet a közelébe férkőzni, mik a kedvenc témái, milyen közös ismerőst kell behazudni a siker érdekében, stb. Egy igazi aranybányát talál itt. **Az ilyen kutakodás elleni védekezésnél komoly előny, ha valakit Kis Pálnak, vagy Kovács Józsefnek hívnak.** A név gyakoriságból adódóan viszont egy Hagyó Miklósnak, vagy egy Ottlik Lilla Leának már nincs ekkora szerencséje, **különösen ha előzőleg önként fel is töltöttek fel magukról, családjukról, sőt teljes családfájukról egy rakat személyes információt nyilvános weboldalakra.** Emellett nagy kérdés,

hogy közösségi oldalüzemeltető ezekből a részletesen információkból előbb vagy utóbb nem fog-e pénzt csinálni? Vajon tényleg megtörténhet ilyen?



Jó néhány alkalmazás jelent meg, amelyekkel ellenőrizni lehet az adatvédelmi beállításokat, például Reclaim Privacy, vagy a Facebook Privacy Check. A tömeges felzúdulás miatt várható, hogy előbb-utóbb itt is megjelennek majd a hamis antivírusok mintájára a hamis beállítás ellenőrző alkalmazások.

Az üzemeltetők erkölcsi érzékének diszkrét bája

Ehhez elég volt elolvasni az "[Újabb Facebook-botrány: felhasználói adatlapokat küldenek a hirdetőknél](#)" című cikket, és máris meglehetősen hozzáférhető láthattunk a Facebook részéről. Egyértelműen beazonosítható felhasználói adatokat ugyanis nem szokás, sőt kifejezetten etikátlan továbbadni a hirdetőknél. A kérdés, hogy milyen erkölcsi aggály tarthatna vissza egy olyan Mark Zuckerberget, aki a hírek szerint [már az induláskor az egyetemi adatbázisba betörve szerezte meg a szükséges kezdeti személyes adatokat](#). Jelenlegi vagyonát mintegy 4 milliárd dollárra becsülik. **Bár ez nem menti fel a felelősség alól, de nem árt tudni, hogy ilyen szemérmetlen személyes adatok hirdetőknél való eladására más közösségi oldalak is vetemedtek már**, például a MySpace, a Digg vagy a Hi5. "Természetesen mindenkinek joga van kényelmetlenül érezni magát, hiszen [a Facebook modelljében a felhasználó nem fogyasztó, hanem maga az áru](#), amit a cég valódi fogyasztóinak, a hirdetőknél ad el." - írja a Webisztán nagyon találóan.

Profil építenek belőlünk

Statisztikusokat, elméleti matematikusokat alkalmaznak a biztosítók is. Korábban a piros színű, fővárosi illetőségű, 20-30 év közötti férfiak által vezetett gépjárművek biztosítási díját akarták beállítani a legmagasabb biztosítási díjra. Ha valakinél árvíz kár volt, és sokba került, akkor meg nem szeretik vele a továbbiakban szerződni. Sok-sok éve dolgoznak már nekik a szakemberek, nem nagyon lehet olvasni olyat, hogy egy biztosító veszteséggel zárt volna.

<http://www.elemzeskozpont.hu/content/komoly-nyeres%C3%A9ggel-z%C3%A1rta-2009-es-%C3%A9vet-az-allianz%E2%80%A6>

<http://www.vg.hu/penzugy/nem-csokkent-a-biztosito-nyeresege-az-elso-negyedevben-279938>

<http://www.euroastra.info/node/38172>

http://hvg.hu/gazdasag/20090514_union_Erste_profit

Profil építenek belőlünk part two

Sajnos mindenki "az én csak egy hétköznapi átlagember vagyok, nincsenek értékes titkaim" téveszmében él, és ontja a muníciót magáról. Aztán meglepődik, ha ráuszítják később a kompromittáló kommandót, vagy kellemetlenül érinti, ha matematikus-statisztikus [szakemberek profilokat építenek](#), ki kire fog szavazni nagy valószínűséggel a következő választáson, milyen biztosítást érdemes a nyakába sózni, stb. **Amerikában már komoly kutatások folynak, és a ruha márkákból, az autó típusból, a cigaretta fajtából, és további jellemzőkből próbálják megjósolni, demokrata vagy republikánus szavazóként lehet-e azonosítani valakit pusztán a begyűjtött adatai alapján.**



A cégek imáznak, rajongói klubjaik építése során olyan kétése eszközöket is bevetnek, mint a bérkommentelők alkalmazása, rendszeresen lehet ilyen állásajánlatokat találni a freelancer.com oldalon.

De a rajongói klubok építése, imázskialakítás is komoly üzleti tényező, a fanpagelist.com oldalon például egyes üzleti márkák, politikusok, sportolók pillanatnyi helyzetét lehet figyelemmel követni. Így az sem meglepő, hogy a cégek olyan kétése eszközöket is bevetnek, mint a bérkommentelők alkalmazása, rendszeresen lehet ilyen állásajánlatokat találni a freelancer.com oldalon. **Érdekes módon a népszerűség listát a Texas Hold'em Poker rajongói klub vezető közel 22 millió taggal**, de Lady Gagának is van 7 millió. Olyan neveket is találunk itt, mint Dr. House, Coca Cola, Vin Diesel vagy Barack Obama. Az is jól látszik, hogy napi több ezren csatlakoznak folyamatosan a legnépszerűbb kluboldalakhoz.

<http://nymag.com/news/features/51170/>

<http://www.fanpagelist.com/>

http://index.hu/tech/net/2010/05/28/rabszolga_voltam_az_orosz_internetmaffiaban/

...folytatjuk...



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



Tweet

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2197910>

Trackbackek, pingbackek:

Trackback: <https://uevegfal.atlatszo>, 2011.07.14. 00:10:25

-- alapvetően csak idézgetek egy szupertrendi/hiper-cool nagyvállalati szoftverről szóló cikkből [Girnt József cikke, ld lejjebb a linket] --
"a kiemelt felhasználók, ha régebben nem is mindig, de ma már kizárólag titkosított protokollok..."

Kommentek:

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

[flegman](#) • <http://usazzunk.blog.hu/> 2010.08.04. 19:41:54

hónapokkal ezelőtt leléptem faszbúkról. I rule!

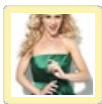
[Higany](#) 2010.08.04. 19:46:31

A poszt hatására újból átfésültem a beállításaimat, amit egyébként rendszeresen megteszek. Ismét rá kellett döbbennem, hogy időnként átállítodnak az adatvédelmi beállításaim, pl a képeimnél egészen biztosan nem volt beállítva "mindenki", mert ez volt az első amit átállítottam. Nem először.

Továbbá az "Adatvédelmi beállítások/Alkalmazások, játékok és honlapok / Nem kívánt és levélszemetelő alkalmazások Eltávolítása" pont alatt ugyan ki lehet jelölni eltávolításra az összes alkalmazást, de egyszerre az összeset nem hajlandó törölni. Úgy csinál, de végül kitöröl mondjuk 8-10-et.

[Higany](#) 2010.08.04. 19:49:57

Elszállt a kommentem, a lényeg, hogy célszerű gyakran, heti rendszerességgel ellenőrizni az adatvédelmi beállításainkat, mert tapasztalataim szerint önálló életet élnek.



[\(Nemzeti Takarékszövetkezet\) THY Rökk *n* Troller](#) [2010.08.04. 20:37:39](#)

"Emberek, figyelem, én az xy antivírust használom ám"

Kedves Rambo! A munkahelyed által képviselt írtó alapértelmezésben fűzi a levelekhez. Egyszeri jüzer képes órákat keresni, mire letiltja a funkciót.

Elnézést az off-ért!

[Oknyomozó](#) 2010.08.04. 21:07:39

Gratulálok és köszönet.

Soha nem voltam és most sem vagyok tag az IWIW-en és a Facebookon. De a vérem nem tudom megtagadni, ezért végigolvastam.

Küldöm a feleségemnek, hadd okosodjon.

Akikről szól, sajnos azok az otthoni, munkahelyi gépeikkel is hasonlóan körültekintően bánnak.

Ennyi újszülött azért nincs.



Gondolom, ez volt a check, hogy ki olvassa el végig a cikket. :D

- Ha egy kicsit kiegészíthetem a posztot – vajon mennyien tudják, hogy ha lájkolnak egy oldalt vagy belépnek egy csoportba, akkor egy "network"-be tartoznak majd a tagokkal, ennek megfelelően akikkel azonos csoportba tartoznak, azok úgy látják az adataikat, mintha az ismerősük lenne? /*pontosabban régebben még így volt*/

- Végül, ha szabad, dobnék ide két linket, ami pár – nem is túl kackiás – forgatókönyvet vázol azzal kapcsolatban, hogy hogyan férhetők hozzá mindenféle bug kihasználása nélkül az olyan adatok, amikről a felhasználók azt hitték, hogy pontosan szabályozva vannak:

bardoczi.blog.hu/2009/12/09/facebook_adatvedelem , bardoczi.blog.hu/2009/12/10/facebook_2_01 valamint bardoczi.blog.hu/2009/12/11/uj_fb_privacy_lehetoseg_stilusosan_eldugva



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.08.04. 21:29:05](#)

Szia TIGRIS!

Bár én nem vagyok piros színű, meg budapesti sem, de javítottam, köszi, hogy szóltál :-)

Terjedelem ügyben meg én húzom magamnak, és ez kb olyan hatékony, mintha saját magamnak adnám át a nokiás dobozt. De az már szentigaz, hogy tényleg arany minden szava :-)

[b. á. 2010.08.04. 21:29:19](#)

Ehh!!

tudtátok, hogy a bloghú a bitly hivatkozásokat kibontja? Én eddig nem tudtam.



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.08.04. 21:31:07](#)

@peetmaster:

Hát ez a totális tiltás nem menne szerintem, nézz vissza pár hónapot, hogy belistázták a pártok például a szavazókat, azaz minket. Lenne jobb ötletem, miért járjon inkább halálbüntetés...



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.08.04. 21:41:15](#)

Kedves b.á,

Jók a linkek, és tényleg sajnos sokaknak csak a subba, puruttya debütálás után van AHA élménye. A beállítások azonban nem csak túlbonyolítottak, hanem folyamatosan átszerveződnek és átállítódnak.

Azért ha próbaképpen Zuckerberg anyjukáját betennénk a víz alá egy bűvárharangba, csak egy nagy levegőt vehetne, és azalatt kellene Marknak jól beállítania a privacyját, akkor rögtön át tudná tervezni a felületet. De nekünk gyökereknek, vidékre addig így is jó lesz :-)



[T1GRIS 2010.08.04. 21:42:31](#)

@Csizmazia István [Rambo]: Igen, én is így gondoltam a húzást, és ismerem a nehézségeit. :) Magamról tudom, hogy baromi terjengősen írok, úgyhogy mindig egy SS tiszt mentalitásával kell végigmennem egy cikken, ha már átlép egy kritikus hosszt. És még így sem mindig sikerül. :)



[Chaoyang • http://xiongyali.blog.hu](http://xiongyali.blog.hu) **[2010.08.04. 23:37:32](#)**

Erdekes, 3 éve amikor beleptem a Facebookra, nem voltak napirenden ilyen adatvedelmi problémák.....

Egy dolgot hanyolok a Facebookrol.. egy teljes backup lehetoseget a profilomrol... anno ket napig csak a profil boxokat rendeztettem, tokeletesre sikerult, az info oldal is, azota szazaval vannak fent kepek, nem orulnek ha elszallna a szerveruk es nekem nem lenne semmi backup-om... Szerintem javasolni kene nekik.



Gépember • <http://gepembernaploja.blog.hu/> **2010.08.05. 11:43:35**

[@Csizmazia István \[Rambo\]](#):

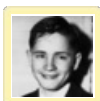
Gratulálok a cikkhez.

Viszont aki ezt végigolvassa, minden szavát érti, sőt, fel is fogja, az már nem 1.0-ás felhasználó.

A téma végtelenségig elemezhető, Te nagyon alaposan elkezd(t)ed körüljárni. Az átlag felhasználó számára - ha végig is olvassa - túl sok és túl összetett információ van a cikkben.

Javaslom, hogy vázlatosan 5-10 pontban írd össze (pl. a cikk végére), hogy mire figyeljenek a felhasználók az adott oldal(ak)on.

Idéztelek, és megtoldottam egy személyes tapasztalattal is.



manson karcsi • <http://goo.gl/FVvVX> **2010.08.06. 19:22:10**

valahogy így kellene kinéznie a beállításoknak: noob.hu/2010/08/06/faszbuuk.png

az a baj, hogy ez kb 15-20 perc. az egy pontnullás júzer pedig leszarja. de nem baj, az internet nem felejt, "dumb fuck"-ok meg mindig is lesznek.

msdng • <http://barikad.hu> **2012.08.10. 00:15:39**

szerintem is voltak, vannak bérkommentelők, másként nézvést ép ésszel felfoghatatlan hogyan lehet valaki még mindig mszp-s vagy akár fletó-fan xD

Minden, amit a privacy-ról tudni akartál... II. rész

2010.08.05. 14:15 | [Csizmazia István \[Rambol\]](#) | [7 komment](#)

Címkék: [privacy](#) [facebook](#) [privátltét](#)

... de sosem merted megkérdezni, éppen hiányoztál vagy mást csináltál. **Háttér információk a Facebook előéletéről, gyűjtemény eddigi privacy incidensekről, temérdek példa linkkel,** megymás, és még több megymás. Összefoglalva: az életben csak egy szép dolog van, de az most épp nem jut eszünkbe ;-) [Tegnap elkezdett írásunkat folytatjuk](#) a második, befejező résszel.



Kollektív vagy egyéni harakiri?

Sokan már gyűjtötték az erőt és a harcostársakat, [hogymajd kollektíven eltűnjének a Facebook közösségből tiltakozásul](#) annak nem megfelelő adatkezelési gyakorlata miatt, de palota forradalom aztán még sem lett belőle. Ha bármi miatt végleges távozásunkat fontolgatjuk, **ne a fiók felfüggesztését (Profilom -> Fiókom -> Beállítások -> Fiók felfüggesztése), hanem ehelyett a teljes törlését válasszuk.** (Persze csak ha jól meggondoltuk). Az inaktív fiók adatai megmaradhatnak, azok beállítása a folytonosan változó alapértelmezett felhasználói szerződéssel publikussá állítható át. A biztos módszer az "Adatlapom törlése", **erre nem is mutat közvetlen menü link, úgy kell rákeresni a Helpben - nyilván az üzemeltetők nem akarják ezt könnyen elérhetővé, pláne nem szemmagasságban elhelyezni -** de íme itt a közvetlen link hozzá:

https://ssl.facebook.com/help/contact.php?show_form=delete_account

Ekkor megjelenik egy figyelmeztető üzenet: "Ha úgy gondolod, hogy nem fogod újra használni a Facebookot és szeretnéd törölni a fiókot, ezt elvégezzük helyetted. Azonban ne feledd, hogy nem fogod tudni sem újra aktiválni a fiókot, sem visszaállítani az általad hozzáadott tartalmat vagy információt. Ha ennek ellenére is törölni szeretnéd a fiókot, akkor klikkelj az "Elküld" -re." És dönthetünk. Azonban ha már jelentek meg általunk feltett kompromittáló bejegyzések, fotók, **ne feledjük, arról időközben bárki készíthetett screenshotot, feltölthette akárhová, vagyis nem biztos, hogy ezzel minden gondunk megoldódott, mindent végleg megsemmisítettünk** De maga az üzemeltető sem törli ám kérésünk nyomán az adatokat, hiszen ezt olvashatjuk: "4. Even after permanent deletion, Facebook says that copies of your photos may remain on their servers for technical reasons." Vagyis késő bánat, eb gondolat, az adatok a legnagyobb biztonságban akkor vannak, ha egyáltalán fel sem töltjük őket.



Nekik adnál a névjegyedből, ha az utcán találkozónátok? Képeinken a Kevésbé Foglalkoztatott Babysitters :-). Ugye nem igazán. Bármelyikük megnézheti viszont a nyilvános profilodat, mazsolázhat a hozzászólásaidból, ha nem kérdezted meg orvosodat, gyógyszerészedet, és másként nem rendelkezél.

Mit csinál a szél, amikor nem fúj?

Hancu kolléga az Indextől volt olyan kíváncsi, és utánanézett olyan alapkérdéseknek, mint például hogy a hókezezetők reggel hogyan jutnak el a munkahelyükre, illetve ha a repülőgép feketedoboza tényleg mindent kibír, miért nem készítik az egészet ebből ;-) "[Tényleg megtartja az Iwiw és a Facebook a törölt képeket?](#)", vagy mi történik azokkal a leveleinkkel, amiket látszólag törölünk? "[Törölt levelek nyomában a neten](#)" címmel. Nos, akit érdekel, olvassa el ezeket az igen izgalmas cikkeket, **röviden csak annyit mondunk, a törlések sosem történnek meg azonnal, ha meg történnek egyáltalán.** Ha valaki ismeri azok korábbi linkjét, még hónapokkal később is meg tudja jeleníteni, illetve volt, ami nem hogy késve, de sosem tűnt el véglegesen. Ami az internetre egyszer felkerül, annak annyi. **Az akváriumból lehet halászlevet csinálni, de a halászléből már nem lehet akváriumot.**



A Google keresőbe begépelve a delete szót előkelő helyen szerepel a "Delete Facebook account" kifejezés. [Sokan kampányoltak is emellett, hogy 2010 május 31-én minél többen lépjenek ki tiltakozásul.](#) A dolognak körülbelül csak akkora hatása volt, mint a Vatera bojkottjának, de mindenesetre felhívta a figyelmet a visszasságokra. Egy Twitterrel összehasonlítva ott azért nincs lázadás, mert a kezdetektől fogva minden nyilvános, míg a Facebook esetében kampányszerűen változnak a ki tételek az alapértelmezetten megosztott adatok köréről.

Privátltét és vidéke Takarékszövetkezet

Jól látható, hogy igen szerteágazó ez a dolog, mindennek meg van, vagy meg lehet a következménye. [□ űőben űlő rabok is fenyegették már meg az ellenük valló tanúkat a Facebook oldalon](#) keresztül (később a profiljukat Gordon Brown kérésére törölték), de maguk [a politikusok is kapnak néha itt életveszélyes fenyegetést](#). □ **Google történetében pedig volt olyan, hogy valaki gázolt, majd segítségnyújtás nélkül elhajtott a helyszínről.** A gyanúsítás során lefoglalták a számítógépét, valamint kikérték az internetszolgáltatótól is a forgalmi adatait. Ott bukott meg, hogy a helyszín közelében lakott, autója (piros Jaguár) megfelelt a körözött színnek, illetve típusnak, [és pont a baleset napján, azt követően ütötte be a keresőszóként](#) az "autóüveg javítás" és a "cserbenhagyásos gázolás következményei" szavakat. Ezen elgondolkodhatnak azok is, akik miatt az "áram" szóra keresve a Google találatok között ennyire előkelő helyen szerepel az "áramlopás" kifejezés.



Komoly előny, ha valakit Kis Pálnak, vagy Kovács Józsefnek hívnak. A név gyakoriságból adódóan viszont egy Hagyó Miklósnak, vagy egy Ottlik Lilla Leának már nincs ekkora szerencséje, különösen ha előzőleg önként fel is töltöttek magukról, családjukról, sőt teljes családfájukról egy rakat személyes információt nyilvános weboldalakra.

Minden szavadat számon tartjuk

Volt a Rolls Frakciónak egy [Minden nagyon szép című száma](#):

"Kezemet, a szememet a szádon tartom

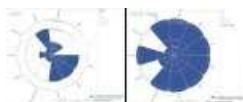
Ezt hallani sem akarom

Minden szavadat számon tartom

Ezt hallani sem akarom"

Valahogy ennek kellene beugrania, ha valaki túlságosan sok személyes információt oszt meg magáról. De természetesen az is jelzés értékű, ha [az Egyesült Államok Kongresszusi Könyvtára egyszer csak váratlanul begyűjti és learchiválja az összes eddigi Twitter üzenetet](#). Bár ezek mérete csak 140 karakteres, de így is 55 millió keletkezik belőle naponta. Mindenesetre [biztosan lehet benne terhelő adatokat bányászni, ha egyszer úgy hozza a szükség](#), a nemzetközi helyzet fokozódik vagy Bástyá elvtárs azt megrendeli.

De vegyünk még egy gondolat kísérletet. **Legyen tökéletes az adatvédelmi beállítás, minden fotónkat, bejegyzésünket csak és kizárólag a barátaink láthatnak. Mit felejtünk ki még a képletből? Igen, az üzemeltetőket, akik mindent látnak.** Sokan vélelmeznek világméretű összeesküvést [a Google túlságosan erős befolyása](#), személyes adataink, kereséseink túlságos ismerete miatt. Igaz, ott kikapcsolhatjuk a Keresési előzmények-et. Nos, minden aktivitásunk itt is látható a Facebook rendszer számára, és aki jelszó hack-kel szerezte meg az első adag egyetemi ember adatait, annak emelkedett erkölcsi nivójára ne tegyünk majd túlságosan sok tétet a jövőben sem, ha fogadni kell rá. Lásd még vírusszerzőket nem alkalmaznak az antivírus cégek sem - esetleg csak Kínában. **Az Electronic Frontier Foundation összegyűjtötte a 2005 óta alkalmazott felhasználó szerződéseket, és itt jól nyomon lehet követni a "fejlődésnek" nevezett változásokat.**



Az évek során így változott a megosztott adatok aránya. Jól láthatóan egyre terebélyesedett a kör, amelynek középpontja a barátok, afölött a barátaink barátai, azt követi a minden Facebook tag, végül a külső kör pedig a teljes internet. Minden személyes dolgunkat nem igazán szeretnénk ennyire közkinccsé tenni.

Balekók, rajongók, csalók, megtévesztők

Amikor egy ismerősünket keressük, vagy egy érdekes ember mikroblogjára szeretnénk követőként feliratkozni, nem árt alaposan megnézni, valójában kinek az adatlapját is nézzük éppen. Nem ritka ugyanis, hogy egy-egy nagy név mögött nem az van, akinek a neve oda van írva. Sőt, **a gyakori nevekből, vagy a híres emberekből több tucatnyit is találhatunk**, például az Ubuntu disztribúció készítőjének nevével is visszaélnék tömegesen a Twitter-felhasználók. Persze lehetünk annyira megengedők, hogy némely Mark Shuttleworth esetében jótékonyan esetleges névazonosságot is feltételezhetünk. Ennél is tovább mennek egyesek, ha például Bill Gatest keressük, [nyomban temérdek ilyen nevű szereplő tűnik elő, közülük jó néhányan pedig ráadásul hamis fotóval](#) adják ki magukat másnak, mint akik valójában.

A Facebookon már tíz Zimány Linda van!

A Facebook esetében a híres emberek köré néha rajongói kört szerveznek, így itt sokszor könnyebb felismerni [a sok szereplő között, hogy valójában ki is az igazi](#). Ezt továbbgondolva kimondottan kellemetlen forgatókönyv lehet azonban, ha valaki a nevünkkel visszaélve – esetleg a közösségi oldalunkról kinézett személyes adatainkat felhasználva – lejárató blogot indít valaki vagy valami ellen a nevünkben. 2009 augusztusban indult el egy [per egy blogger ellen, aki Liskula Cohen topmodellről írt állítólag kedvezőtlenül](#), és emiatt milliós perrel fenyegetik.

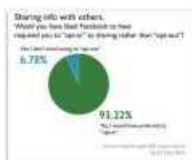


Egy 26 éves brit férfi azt a viccesnek gondolt [üzenetet küldte ki Twitteren, hogy felrobbantja a repteret, ha késik a gépe](#). A rendőrség azonban nem tartotta ezt viccesnek, Paul Chamberst letartóztatták, végül aztán csak pénzbüntetést kellett fizetnie.

□ gyenge és a még gyengébb láncszem

Ha felnőtt fejjel mindezt már belátjuk, akkor jön a család, a gyerekek kérdése. Sokan esnek abba a hibába, hogy alábecsülik a szülők viselkedésének mintaadási funkcióját. Pedig óriási jelentősége van ennek. Ha például a gyerek rendetlenséget lát a szülő íróasztalán, lehet, hogy hiába kérleljük majd a játékpolt elpakolására. De ugyanígy érdemes □persze a saját korának megfelelően □válaszolni is a kérdéseire az egyszerű tiltások helyett, amelyek értetlenségre, □csakazértis□ típusú dacra vezethetnek. [Meg kell értetni vele, miért nem tesszük közzemlére az összes személyes adatunkat](#), mik a veszélyei a bárki által nézegethető kihívó, furdóruhás képeknek, milyen honlapoktól jobb, ha óvakodik, **miért nem plakátoljuk ki, mikor utazik el a család nyaralni stb.** Persze ez a nehezebb út, sok türelmet igényel, de hosszú távon mindenképpen célravezetőbb. Tudniuk kell azt is, hogy nem mindenki az, akinek látszik. A közösségi oldalakon is vannak olyan rejtőzködő bűnözők, pedofilok, akik adatlapjuk alapján látszólag gyerekek, de valójában az a céljuk, hogy kikérdezzék, és behálózzák a gyanútlanabbakat, akár az elkotyogott információkkal történő zsarolással. Sose adjuk meg minden személyes adatunkat a közösségi portálokon, mert mások visszaélhetnek vele! Csak ha már valóban ismerősünk valaki, elég akkor odaadni a telefonszámunkat, lakcímünket vagy e-mail címünket.

Bár sok felnőtt is elköveti ezt a hibát, de **a gyermekek esetében ez sokkal veszélyesebb, ráadásul ők hajlamosak naivan mindent elárulni, ezért kiemelten a szülő feladata, hogy megbeszélje a gyerekekkel ezen dolgot**, illetve tanácsot adjon. Tanulságos történet lehet az is, amikor [a MI6 brit titkosszolgálat főnökének felesége óvatlanul még a lakcímét is közzéteszi a Facebookon](#). Egy felelőtlen családtag nagyon gyenge láncszem lehet. **Egy amerikai felmérés szerint a 12 évesnél idősebb gyerekeknek már a fele (48%) tagja a közösségi portáloknak, és azt naponta többször is használja.** Ez az a korosztály, akik szerint az e-mail már lassú és körülményes. Az újság és a televízió helyett is jelentős mértékben támaszkodnak inkább ezekre a pörgő, hihetetlen tempóban növekvő, és villámgyors web2 lehetőségekre.



A józan ész, de a Sophos miniszavazás szerint is a "zárt, és majd mi engedélyezzük, ha akarjuk" modell lenne a kívánatos. Természetesen a Facebook üzemeltetők pont ennek az ellenkezőjét gondolják nekünk jónak és alapértelmezettnek.

A statisztikák is ezt mutatják

A Webroot egy átfogó felmérés keretében mintegy ezeregy száz Facebook-, MySpace-, Twitter-, Linkedlin-felhasználót kérdezett ki a webhasználati szokásaikról. Az eredmények alapján elmondhatjuk, az óvatosság sajnos nem igazán jellemző. A válaszadók kétharmada egyáltalán nem korlátozza a személyes profiljában olvasható részleteket, amelyek így akár egy Google keresővel is láthatóak. [Több mint a felük \(59%\) nem tudja biztosan, kiknek is engedélyezte pontosan profilja megtekintését.](#) Körülbelül egyharmaduk (32%) adott meg legalább három személyes azonosításra alkalmas információt, egyharmaduk (36%) ugyanazt a közösségi portálon használt jelszavát máshol is használja, egynegyedük (28%) fogad el barátkérőt idegentől. Más mutatók sem festenek szebb képet. Az igaz, hogy 78% aggódik személyes adatai miatt, de ugyanakkor 30% nem rendelkezik vírus- és kémprogram elleni védelemmel. A korosztályok közt a fiatalok számítanak a legvesélyeztetettebbnek, az átlagos 28 százalékos értékkel szemben náluk 40 százalék fogad el barátkérőt idegentől, és náluk sokkal jellemzőbb az összes személyes adat, elérhetőség megadása is.

Ott fent majd megmondják, mi a jó nekünk

"A magánélet a múlt társadalmi normája. A személyiség jogainak védelme felett eljárt az idő" - [véli Mark Zuckerberg](#). Az emberek egy része, különösen az IT biztonsággal foglalkozó szakemberek, a felhasználók biztonságtudatos csoportjának azonban inkább negatív erről a véleménye. **Mindent részletesen megosztani az életünkből körülbelül annyi értelme van, mint atombunkert építeni Kocsordon.** Nem tévedünk sokat, ha úgy gondoljuk, [sokan fogják megbánni később, hogy meggondolatlan képeikkel, üzeneteikkel felelőtlenül kitérültek](#), vagy éppen munkahelyüket, karrierjüket, barátaikat, családjukat szidalmazták. **Nem egyszerű hát minden szempontot, összefüggést és ehhez az adatvédelem módjait saját életünkben kiépíteni, megőrizni, és ha valamire áll, akkor erre igazán: [az egyensúly egy élethosszig tartó tanulási folyamat](#)** eredménye.



[Az Openbook egy szemléletes jó példája](#), mennyire könnyű terhelő adatot gyűjteni. A publikus megjegyzésekből - és lassan már csak ilyen van - olyan kényszerítő gyűjt ki, mint például ki mondott olyat, hogy utálja a főnökét, elvesztette a szüzességét, tett-e rasszista megjegyzést vagy ismerte be egy gyenge pillanatában, hogy csalt a vizsgákon.

Mellékhatások tekintetében olvassunk kommenteket

Itt akár le is lehetne zárni, megvolt a katarzis, a tanulság, úgy gondoljuk azonban, érdemes egy picit oldottabban, vidámabban elköszönni a

témától. **Em szabad ugyanis kihagyni a közösségi oldalak olyan előnyeit, amire sokan nem is gondolnának.** Például ha valakinek van kiadó lakása, itt nem csak a hirdetést tudja feldobni az üzenőfalra, de **a leendő bérlő lekáderezése is könnyebbé válhat: ["Ha hirdetsz egy albit, egyből le tudod ellenőrizni, hogy a leendő albérlő vajon rakott-e fel magáról hányós képeket, és tart-e mini állatkertet"](#).**

Természetesen ami vesztét okozhatja egy-egy munkavállalónak, ha dehonesztáló megjegyzésekkel illeti azt, **első kézből származó információ lehet annak, aki pedig éppen állást keres,** és a jó álláskereső nem csak eltűri, hogy őt a személyzetis lekáderezze a neten, hanem ő is utánanézi, **[hányan lettek a héten öngyilkosak a cégnél](#),** nincsenek-e az APEH feketelistáján, illetve az ott dolgozók többsége a közösségi oldalakon miként vélekedik munkaadójáról.



A fanpagelist.com oldalon egyes üzleti márkák, politikusok, sportolók pillanatnyi Facebook helyzetét lehet figyelemmel követni. Minden be van árazva, akár a tőzsdén.

Egyszerűbb beállítások, változatlan megosztás alaphelyzetben

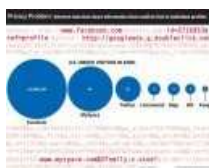
Időközben - talán a kollektív Facebook öngyilkossági akció nyomására - **[mégiscsak életbe léptek bizonyos egyszerűsítések a biztonsági beállításoknál](#).** Nyilván a viszonylag néhány ezer kilépő miatt kevésbé fáj a menedzsment feje, de az üzletmenetnek nem tett volna jót a sok negatív cikk, bírálat, kritika, így emiatt léptek. Maga a lépés természetesen pozitív, kicsivel könnyebb ellenőrizni, mit láthatnak a barátok, és mit mások. Annyi mindenesetre igaz - és **[ebben Graham Chueleynek adunk maximálisan igazat](#)** - hogy **ha valóban a felhasználók igényelnék azt a fene nagy megosztást mindenről, akkor most a fejlesztők meglephetnék volna a jelenlegi opt-out (nekem kell korlátozni, kizárni a jogokat, mert alapértelmezett a megosztás) helyett az oly trendinek beállított opt-in (alaphelyzetben nincs megosztás, mindenki maga állítja be, mit szeretne mások tudomására hozni) rendszert.** Nyilván ehhez nem volt bátorságuk, mert akkor **bebizonyosodott volna, hogy nem a felhasználók tömegei akarják ezt, és főleg üzletileg sem lett volna jó a Facebooknak.**



Elég perverz dolog arra vágyani, hogy minden mozdulatunk egy nyilvános tacepaora legyen kiírva. Most bekapcsoltunk a gépet, most entert nyomtunk, most feltöltöttünk egy képet, most éppen a leveleinket olvassuk, most a társskereső oldalt nézzük, stb. Letiltani persze le lehet, de ugye mi az alapértelmezett értéke? Igen, jár a hangszóró.

Az ember vagy megoldja, vagy előidézi a problémát, különben csak szimpla tereptárgy

Természetesen az emberi tényező ott van mindenhol. Most sem tart senki töltött pisztolyt senki fejéhez, hogy az önkéntes közösségi oldalakra regisztráljon be. Most sem tart senki töltött pisztolyt senki fejéhez, hogy a bizalmas adatait, képeit, magánvéleményét gépelje be és ossza meg a világgal. Valószínűleg **[a megváltoztatott biztonsági beállítások a felhasználók egy nagy részét így is hidegen hagyja majd: nem érdekli, lusta rá, nem is hallott róla, nem ért hozzá](#)** illetve fogalma sincs, hogy az ő személyes adatai is nyilvánosak. És ezzel a hozzáállással pontosan ők azok, akiknek adatai, képei, megnyilvánulásai egyszer majd Szalacsi Sándor módra valamilyen kínos helyen kötnek ki. Remélhetőleg azért az új egyszerűsített beállítások miatt összességében többen fordítanak majd figyelmet adataikra.



Nem Mózes kőtábláit nézzük, az biztos. Szinte havonta változik a felhasználói szerződés, és egyre tágabb teret enged az információk áramlásának. A Facebook ezt "fejlődésnek" hívja, az Electronic Frontier Foundation inkább rombolást emleget.

Őnök a HÉT Facebook különkiadását látták :-)

Sok példát láttunk a Facebookról, de a tanultak, a megfelelő hozzáállás ugyanígy vonatkozik az Iwiw, Tumblr, Flickr, Twitter vagy bármilyen más közösségi oldalra is. **Három nagy területre lehet szétszedni az adatvédelemmel kapcsolatos kétségeket.** Az első a **személyes adataink véletlen megosztása a nagyvilággal.** A másik az ismeretlen háttérű (akár trójai) alkalmazások saját kezű telepítése gépünkre. Míg a harmadik **magukkal az üzemeltetőkkel, például a Facebookkal szembeni aggályok.** A Facebook **kihatalmítja a szakadékokat az átlagemberek korlátozott számítógépes ismeretei és a fejlett internetes marketing között.** Lehetetlen megjósolni egy-egy óriásivá nőtt cég esetében, hogy mindez hová vezet majd, például a **[Microsoft feldarabolását célzó döntés is végül csendben lekerült a napirendről](#),** a Google háza táján úgyszintén mindennaposak az adatvédelmi aggályok - legutóbb **[a Street View autói gyűjtötték be mellesleg a WiFi forgalmat több országban is](#).**

Egy biztos, ami nem a kapitalista cégek profitért vívott machinációin múlik, **[legalább azt a részt csináljuk okosan, tudatosan, átgondoltan](#)** - ennyi múlik rajtunk. Öveges professzor szerint "nincsenek nehéz vagy könnyű dolgok, csak megértettek és meg nem értettek vannak". **Talán ez az írás is segített gyarapítani a megértett dolgokat.** Közben az internet világában a nemzetközi helyzet fokozódik, és

kafferbivalybalamber egyik remek kommentjét idézve: "Az optimista angolul tanul. A pesszimista kínaiul tanul. A realista lőni tanul." Azt hiszem, emellett [a személyes adatainkkal való bánásmódot mindannyiunknak folyamatosan kellene tanulnia](#). Ehhez lehet egy [jó kis záró adalék az alábbi !\[\]\(a3ea015cc5581cad732d1eb81613fe7b_img.jpg\)outube videó](#) is.

További ajánlott linkek:

Facebook: a magánélet tündöklése és bukása

http://hvg.hu/Tudomany/20100518_facebook_maganszfera_bukasa

Kivonulás a Facebookról

http://index.hu/tech/2010/05/21/kivonulas_a_facebookrol/

FaceBook Scam Alerts DataBase

<http://www.fbsaonline.com/forumdisplay.php/4-FaceBook-Scam-Alerts-DataBase>

<http://www.allfacebook.com/tag/scams/>

Facebook Scams Growing With Site's Popularity

<http://www.kcbs.com/Facebook-Scams-Growing-With-Site-s-Popularity/6073739>

További ajánlott filmek:

- [Supersize Me](#)
- [The Corporation I-II.](#)
- [The Social Network](#) (2010. október)

További ajánlott könyvek:

- [Herbert Schiller: Tudatipar made in U.S.A.](#)
- [Szabad adatok, védett adatok 2.](#)



31 személy kedveli ezt Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.



 [1 trackback](#)

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrző 8.](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2198774>

Trackbackek, pingbackek:

Trackback: <https://uevgfal.atlatszoz>, 2011.07.14. 00:10:25

-- alapvetően csak idézgetek egy szupertrendi/hiper-cool nagyvállalati szoftverről szóló cikkből [Girnt József cikke, ld lejjebb a linket] --
"a kiemelt felhasználók, ha régebben nem is mindig, de ma már kizárólag titkosított protokolloko..."

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](#).

Lúdtalp 2010.08.05. 16:54:10

A kisebbség vigyáz csak az adataira, így nekik mindig lehetőségük lesz észrevétlenül kutakodni mások életében.

agyvihar • <http://agyvihar.blog.hu/> 2010.08.05. 17:07:16

Érdekes, hogy egy meglehetősen Facebook ellenes cikk végén azért ott van a Like gomb. :P

Sixx! Anyádat is nyuggernek hívod? • <http://orbanfan.blog.hu> 2010.08.05. 17:29:32

[agyvihar](#): hol? Én csak twitter és gúgli readert látok...



prof. Perselus Piton 2010.08.05. 18:57:14

Mint mindent, ezt is ésszel kell csinálni...

b. á. 2010.08.05. 21:15:48

Ismét hiánypótlók cikk, riszpekt!

Egy kis okoskodás - az olvasók közt könnyen lehet, többen nem tudják, de extrém nagy adathalmazból hatékonyan törölni nem olyan triviális művelet. Azaz ha normálisan akarják csinálni, akkor az komoly többletterhelést róhat a szerverfarmra, persze, hogy nem szeretnek költeni ilyenre.

Viszont van valami, ami vagy elkerülte a figyelmet, vagy kimaradt, de nem tudom: a T&C-ben van olyan rész, hogy profil törléssel garantáltan nem tudják az összes adatot eltávolítani. Azaz pl. mi történik azzal a kommenttel, aminek a szerzője törölte magát? Szerintem szinte 100%, hogy megmarad, csak nem lehet kattintani a nevére.



Gépember • <http://gepembernaploja.blog.hu/> 2010.08.06. 12:26:33

Ha már szóba került a Google:

A Google és a CIA közös vállalkozása:

gepembernaploja.blog.hu/2010/08/03/google_es_a_cia



manson karcsi • <http://goo.gl/FVvVX> 2010.08.06. 21:27:12

a microsoft is - mint minden óriásira dagadt cég - az ibm sorsára fog jutni: kihal, mint a dinoszauruszok. megeszik a kicsi, mozgékony rágsálók.

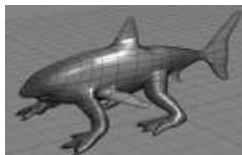
a cikkért köszönet rambónak. szigorúan terjesztendő!

Márkanévét kegyelettel lejáratjuk

2010.08.09. 17:30 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [hamis antivirus sysinternals wireshark](#)

Ha az ember semennyire nem konyít a számítógépes biztonsághoz, az akár jó is lehet abban az esetben, ha ezzel önmaga is tisztában van, és ezért inkább mástól kérdez. Ennél kicsit rosszabb lehet az a szituáció, amikor már kialakult egy fajta alapkép, és ettől valaki úgy érzi, meggy ez már neki egyedül is, tud ő itt kérem disztigválni a dzsunka himi-humi hamis programok és a valódi, ismerős nevű alkalmazások között.



A baj csak az, hogy éppen erre találták ki a hamis antivirus programok készítői a kreatív névadást. Néha [valódi, létező vírusvédelmi termékek](#) kinézetét és [nevét hamisítják](#), illetve meglévő más biztonsági alkalmazásokból "kölcsonöznek" szavakat a frappáns csali elnevezéseikhez.



Azok után, hogy [már ennyiszor írtunk, beszéltünk erről a témáról](#), a mostani helyzetben elmondhatjuk, hogy aki manapság egy [Windows Antivírus 2010](#) nevű programot feltelepít a gépére, az magára vessen. De mi a helyzet ugyanakkor [egy Wireshark Antivirussal](#) vagy egy [SysInternals Antivirussal](#)? Természetesen [sem a Wiresharkot fejlesztő CACE Technologies-nek](#), sem pedig a SysInternalsnak **semmi köze** ezekhez a kártevőkhöz.



A [Wireshark valójában egy jó kis multiplatformos hálózati csomagfigyelő](#), míg a SysInternals az a cég, amelyik a később a [Microsofthoz csatlakozó Mark Russinovits](#) vezetése alatt több tucatnyi jó kis programot írt (File Explorer, Process Explorer, ZoomIt, stb.). Annak idején [ő leplezte le ezek segítségével a Sony DRM-be rejtett rootkitet](#). Most azonban mélyen szánalmas módon a "sysinternals" szót beírva a Google keresőbe már ötödiknek jön fel a "How to remove Sysinternals Antivirus" találat.



A [kreatív névadás](#) mellett a hamis vírus bűnözőknek viszont egyáltalán [nincs szüksége ezzel együtt kreatív könyvelésre is](#), hiszen **ők az egész semmiért kicsalt pénzt zsebbe, feketén szerzik, és nem is keveset**.



És végül azt sem árt tudni, [az igazi vírus programoknak mindig van időkorlátos \(2 hét, 30 nap, stb.\) és INGYENESEN használható letölthető változata](#), amely teljes értékű, irtani is tud, nem "How to remove"-val kezdődik róla a történet a keresőkben, és elsődleges célja nem a bankkártyánk megpumpolása, hanem a valódi környezetben való kipróbálás.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Majdnem mindenki átverhető adatahalászával](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2209624>

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](#).



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.08.11. 20:01:03

Az ilyeneket szerintem csak a számítógéphez és annak világához abszolút analfabéta felhasználók töltenek. Aki kicsit is tájékozott biztonsági szempontból, az maximálisan figyelembe veszi az utolsó mondatodat. Mivel az internet és a számítástechnika egyre csak terjed, ez a réteg sajnos egyre vastagabb lesz, akár a belőlük élő cyberbűnözők pénztárcája.

[Dagadt Botsáska 2010.08.12. 08:36:13](#)

A gondok ott is tetten érhetők, hogy nem csak az interneten terjednek ezek a dolgok, hanem sokszor azzal kell szembesülnöm, hogy az általam a jüzernek feltelepített kiváló antivírus mellé még felrak a jüzer magától vagy 2 másikat, mert a szomszéd kőműves szerint az sokkal jobb mint amit én tettem fel... aztán ilyenkor jön az ordenáré szívás... és nem értik, nem értik!



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.08.12. 09:07:54

Szia Dagadt Botsáska!

Eddig én is mindig csak a rend kedvéért írtam, hogy elég egy valósidejű víruskereső a gépre, nem kell kettő, gondoltam ilyen azért nem csinál senki, ez csak amolyan kötelező említeni való.

Most találkoztam egy ismerőssel egy komoly cégnél, ahol a melóhelyen kötelező hármat!!! futtatni egyszerre és ki is öltik a nyelvüket a pc-k, meg belassultak atomra. De az ukaz az ukaz, a főnökség utasítását ugye kell tartani.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.08.12. 09:12:54

@Yann Le Pentrec:

"Az ilyeneket szerintem csak a számítógéphez és annak világához abszolút analfabéta felhasználók töltenek"

Viszont mindent elemésztő többségben ők vannak. Lehet egyébként tapasztalatlanságból, meg véletlenül, kapkodásból is ilyenre kattintani.

[Dagadt Botsáska 2010.08.12. 09:21:23](#)

@Csizmazia István [Rambo]: Hát nem tudom... én vagyok annyira tökös, hogy az ilyen hülyeségeket azonnal visszadobom. Azért alkalmaznak mert érték hozzá, és ha nem fogadja el amit én mondok/teszek informatika témában, akkor keressen mást. Nyilván nem fogom a nevem adni ilyen amatőr marhasághoz, ahogy gondolom Te sem tennéd. Azt vallom, hogy az a jó (biztonsági) szakember aki nem köt kompromisszumot.

Örök élet, két ingyen sör, plusz 100 év

2010.08.10. 18:25 | [Csizmazia István \[Rambol\]](#) | [4 komment](#)

Címkék: [facebook](#) [mcdonalds](#) [csalás](#) [kattintás](#)

Kiábrándító látni, hogy [mennyire egy kaptafára mennek a Facebook oldal vonzó címes csalásai](#). Ennél már csak az a kiábrándítóbb, hogy mégis mennyien mozzgatják gondolkodás nélkül a phalanx proximalist.



Bármit lehet ígérni a Facebookon, ahogy olyan érdekességet is, amelynek a címe: ["Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót"](#). Ez elég sikeres tudott lenni. Aki bedőlt ennek, és rákattintott a captcha-nak álcázott képre, [az akaratlanul is megosztotta ismerőseivel a kártékony linket](#). Azonnal a csoport rajongói közé került, és nevében ismerősei üzenetet kaptak, melyben a fenti videót ajánlja figyelmükbe. Tulajdonképpen semmilyen **videó nem létezett, helyette viharos sebességgel nőtt a kártékony oldal rajongói tábor**a, az augusztus 2-i hétfőn több, mint ezer fővel óránként. Az első figyelmeztetés megjelenésekor 2010. augusztus elsején még 7000 felé járt, a másnap esti kártékony Facebook csoport lekapcsolása előtt 63 ezernél sikerült utoljára képernyőképet csinálnunk.



Akkor is gyanítható volt, **ez amolyan főpróba, egy PoC, egy kísérlet, és olyan mámorító eredménye lesz a készítőknél, hogy máris szerelik a gépsort és öntik az illet mostantól százasaival a nyakunkba**. Nem is kellett sokat várnunk, jött a ["OMG the worlds worst mcdonalds customer \(shocking video must see\)"](#). Sajnos, mindig lesz elegendő rosszfiú, aki kielégíti ezt az ígéretet és frappáns címek iránti olthatatlan intellektuális igényt, és a "kattints ide és soha többet nem kell adót fizetned", meg hasonló típusú Taigetosz pozitív bulvár címekkel bevonzza az 500 millió felhasználó 5 százalékát.



Nem is érti az ember, az ilyenek helyett **miért nem egy bejelentkezés nélküli Youtube-on néznek emberek videót például a Gördeszkás pap Lentiből címmel**, de lehet, hogy ez egy új extrém sport, szándékos adrenalin túra: bungee jumping helyett Facebook linkre kattintás vakon. Mindenesetre érdemes lenne [betartani néhány ököl szabályt](#), talán ez segíthet elkerülni a hasonló eseteket, amik egészen biztosan sokasodnak majd.



Ha egy rettentően shocking, és nagyon must see Facebook videót csak akkor lehet megnézni, ha előtte lájkolni vagy csatlakozni kell, dugják fel maguknak! **Ha egy Facebook videót csak akkor lehet megnézni, ha előtte engedélyeznie kell egy alkalmazás telepítését, amely természetesen hozzá akar férni az üzenőfalhoz, ismerőseinkhez, személyes adatainkhoz, Gyehennára vele!** Na, valami ilyesmi lenne jó, kedves Róbert Gida - morfondírozott Micimackó, majd közelebb húzta magához a mézescsuprot.

Tetszik 21 személy kedveli ezt [Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.](#)

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [A kiknek a Captcha kinszenvedés](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

- [25-ször több a mobilos kártevő](#)

A bejegyzés **trackback** címe:

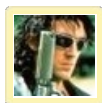
<http://antivirus.blog.hu/api/trackback/id/2212417>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.08.10. 22:31:14

De Mijaza faszbúúk?
És mér nincs ottan az antivirusblog?
És én miJért nem adom meg minde' adatom a faszbúúkon?

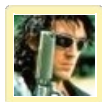


Yann Le Pentrec • <http://lnk.bz/t7c> 2010.08.11. 19:47:45

Húúú, de könnyelműek az emberek...

Dagadt Botsáska 2010.08.12. 08:43:44

Aki fosbúkra jár meg is érdemli. Mindenesetre én a cégnél tiltólistára tettem, volt is háborgás... :)



Yann Le Pentrec • <http://lnk.bz/t7c> 2010.08.16. 10:55:32

Ezt nem lehet így kijelenteni, hogy aki közösségi oldalra jár, "meg is érdemli". Egyéne válogatja, ki mire kattint rá: magam is láttam ezt az említett videora mutató linket (az emberek 98 százaléka... blabla), és nem nyomtam rá, viszont az ismerőseim közül jónéhányan. Akkor mi most mind egy kalap alatt vagyunk?

Conficker rulez

2010.08.12. 12:12 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

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

Bár a Conficker már tizedik hónapja uralkodik a magyarországi vírustoplista első helyén, az elmúlt négy hónapban a lista öt követő további három helyzetét is mozdulatlanul őrzi szokásos helyét: Agent trójai, Autorun vírus, OnlineGames trójai.



Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik a hazai felhasználók számítógépeit. A magyar lista első helyét már **2009 októbertől az a Conficker féreg tartja**, amely az operációs rendszer frissítéseinek hiányát, a gyenge jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed. Kitekintve a nagyvilágba **sok helyen ugyancsak a Confickert láthatjuk első helyen** - például Franciaországban vagy Angliában - ám néhány helyen már egy újonc, a Win32/Oficla trójai tudta magát beverekedni a második helyre - mint például Ausztriában.

Az előbb említett és 2010 áprilisában felbukkanó Win32/Oficla trójai a szokásos módon a rendszerleíró-adatbázisban elhelyezett kulcsokkal gondoskodik arról, hogy minden indításkor lefuttassa saját kódját. Ám ezen felül a \Documents and Settings\Application Data és Local Settings mappájában is különféle kártékony állományokat hoz létre. A megtámadott számítógépen **hátsó ajtót nyit, amelyen keresztül oroszországi weboldalakról további kódokat igyekeznek letölteni** a megfertőzött számítógépre. A magyarországi listán a hetedik helyet sikerült neki megszereznie.



Ugyancsak új versenyző ebben a hónapban az ötödik HTML/ScrInject trójai, amely egy RAR segédprogrammal tömörített fájlt, és telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a böngészőben a fertőzött számítógépen. Hátsó ajtót is nyit a megtámadott rendszeren, és ezen keresztül **további kártékony javascript állományokat kísérel meg letölteni és lefuttatni** a háttérben. Persze aki Firefox böngészőt és NoScript plugint használ, az hívós nyugalommal olvashatja mindezt.

Lassan érdemes lesz fogadások kötni tétre, helyre, befutóra arra is, hogy **vajon meddig képes elsőségét a havi listán megőrizni a Conficker féreg**. A külföldi adatokat vizsgálva a Win32/Oficla trójai jó eséllyel pályázhat majd a helyére, hacsak a következő hónapokban nem jelenik meg még nagyobb számban valamilyen még újabb kártevő. A **Conficker változatos és bonyolult fertőzési mechanizmusa (blokkolja a Windows Update és egyes antivírus weboldalak elérhetőségeit)**, számtalan variánsa és gyakori előfordulása miatt az ESET fejlesztői egy külön Conficker mentesítő segédprogramot is elérhetővé tettek, ezt pedig az alábbi linkről lehet letölteni: <http://www.eset.hu/tamogatas/viruslabor/eltavolitok>



A trójai programoknál egyébként az a fő veszély, hogy mivel **maga a felhasználó telepíti azokat a saját szabad akaratából**, így nehézkes ellene a védekezés. Ha előzetesen nem tájékozódunk, könnyen belefuthatunk valamilyen rosszindulatú, kártékony vagy kifejezetten bűnözők által készített, terjesztett alkalmazásba, aminek a nevét a Google keresőbe írva csupa "How to remove..." kezdetű találatot kapnánk. Az új programok, alkalmazások, segédprogramok **telepítés előtti információgyűjtéssel, óvatossággal párosuló biztonságtudatos viselkedés hozhatna csak érdemi változást**, javulást ezen a területen.

Vírustoplista - 2010 július



Az ESET több százezer magyarországi felhasználó visszajelzéseire alapuló statisztikai rendszere szerint 2010 júliusában a következő 10 károkozó terjedt a legnagyobb számban, és volt felelős együttesen az összes fertőzés 28.60%-ért.

1. Win32/Conficker féreg

Elterjedtsége a júliusi fertőzések között: 8.06%

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 válnak a megfertőzött számítógépen.



A számítógépre kerülés módja: Változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható a külső meghajtó fertőzött Autorun állománya miatt.

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

2. Win32/Agent trójai

Elterjedtsége a júliusi fertőzések között: 5.16%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (például Temp mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett kulcsokkal gondoskodik arról, hogy minden indításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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

3. INF/Autorun vírus

Elterjedtsége a júliusi fertőzések között: 3.52%

Működés: Az INF/Autorun egyfajta 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/autorun>

4. Win32/PSW.OnLineGames trójai

Elterjedtsége a júliusi fertőzések között: 2.34%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. Az ide tartozó károkozónak rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. 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/ScrInject trójai

Elterjedtsége a júliusi fertőzések között: 2.32%

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



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



6. INF/Conficker vírus

Elterjedtsége a júliusi fertőzések között: 1.68%

Működés: Amennyiben böngészés során az autorun.inf fájl valamely egység főkönyvtárába kerül, akkor a betöltő eléri, hogy a kártévő kódja elinduljon. Vagyis az INF/Confickernek az a szerepe, hogy betöltse magát a Win32/Conficker kártévőt.



A számítógépre kerülés módja: Fertőzött weblapról, vagy külső eszközön keresztül.

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



7. Win32/Oficla trójai

Elterjedtsége a júliusi fertőzések között: 1.62%

Működés: A Win32/Oficla 2010 áprilisában bukkant fel először, és a szokásos módon a rendszerleíró-adatbázisban elhelyezett kulcsokkal gondoskodik arról, hogy minden indításkor lefuttassa saját kódját. Ám ezen felül a \Documents and Settings\Application Data és Local Settings mappájában is különféle kártékony állományokat hoz létre. A megtámadott számítógépen hátsó ajtót nyit, amelyen keresztül oroszországi weboldalakról további kártékony kódokat igyekszik letölteni a megfertőzött számítógépre.



A számítógépre kerülés módja: A felhasználó maga telepíti

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/oficla-gn>



8. Win32/Mebrook trójai

Elterjedtsége a júliusi fertőzések között: 1.56%

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 hoz létre, illetve módosítja azokat, ha már léteznek. Ezenkívül megkísérel a google.com webcíme 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/%21mebroot>



9. Win32/VB féreg

Elterjedtsége a júliusi fertőzések között: 1.20%

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>



10. Win32/Packed.VMProtect trójai

Elterjedtsége a júliusi fertőzések között: 1.14%

Működés: A Win32/Packed.VMProtect trójai bemásolja magát a Windows/System32, a Temp és/vagy a Windows mappába, ahol különböző DLL állományokat hoz létre. Ezek automatikus lefuttatásáról úgy gondoskodik, hogy a Rendszerleíró adatbázisba bejegyzéseket készít. Ezzel biztosítja magának a betöltődést a rendszer indításakor, illetve a legtöbb esetben külön szolgáltatást (szervízt) is létrehoz. Különböző portokon képes hátsó ajtót nyitni, melyen keresztül távoli weboldalakhoz csatlakozik, és a háttérben fájlokat tölt le.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Ez történik a weben egy perc alatt](#)
- ["Szösölmédia" és nyaralás](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Nyári tanácsok utazáshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2213168>

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](#).

Nincsenek hozzászólások.

Pókerarcok: nem kerültek hangulatba

2010.08.13. 12:05 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [adatok](#) [bankkártya](#) [lopott](#) [adathalászat](#)

Már jó sok éve az iparszerűen, kémkedéssel végzett pénzszerzésből élő [profi bűnözői csoportok a mozzatái](#) a kártevőterjesztésnek, adathalászatnak. Ahogy [a lopott hitelkártya adatoknak is meg van a maga helye ebben a jól megtervezett táplálkozási láncban](#).



Korábban már boncolgattuk, országa válogatja, [milyen bankkártya adat mennyit ér](#), sőt időnként [az online játékokhoz tartozó jelszavak is értékes](#) hasznát hozó árucikknek számítanak. És azt is emlegettük, [ha egy nemzetközi bűnbanda tevékenykedik](#), illetve ha olyan országban végzik az illegális tevékenységet, ahol a hatóságok némileg megengedőbbek, kevésbé felkészültek, vagy mások a törvények - **akkor a bizonyítás alaposan feladja a leckét a nyomozóknak**.



Most egy ilyen régebbi történetre kerülhet pont [a 27 esztendőös BadB, vagyis az ukrán-izraeli Vladislav Anatolieviech Horohorin elfogásával](#), akit Franciorszámban tartóztattak le, épp egy Moszkvába induló repülőgépre igyekezett. **A CarderPlanet alapítóinak egyike volt, amit még 2001 májusában indítottak a lopott hitelkártyák kereskedelmére.** Az eredeti csapat feloszlása után BadB önállósította magát, és saját weboldalain folytatta a bankkártyaszámok adás-vételét. **Pénzt ajánlott a hackereknek biztonsági sebezhetőségeket kihasználó exploit kódokért is.** Ténykedéséről több [flash alapú rajzfilm is készült](#), amelyek bizonyára viccesek lehetnek mindenkinek, akinek nem csapolták meg a számláját.



[2005-ben történt már egy CarderPlanetes letartóztatás](#), akkor Ukrajnában az amerikai hatóságokkal együttműködve a szintén alapítónak számító Dimitrij Golubovot vették őrizetbe. Most a [lebuktatás tetten érésével Nizzában sikerült, amerikai beépült titkosügynökök ugyanis vásárlónak álcázva magukat keresték meg Horohorint](#). Mivel 2009-ben már vádat emeltek ellene az Egyesült Államokban **egy másik ügye miatt**, így valószínű a kiadatása, ahol a korábbi tíz év börtön mellett újabb néhány várhatja.



Persze örüljünk ennek az eredménynek, de ettől ez a biznisz sajnos nem fog megszűnni. Ezért csak [ismételni tudjuk magunkat azzal a kis összefoglalóval](#), amely [segíthet ha arra gyanakszunk, betörték a gépünkbe vagy a postafiókunkba](#).

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

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kényszerűvé](#)
- ["Szösölmédia" és nyaralás](#)
- [Mai szavunk pedig: keyjacking](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2218587

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Dr. Fusher és Gány professzor módszere

2010.08.16. 21:21 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [facebook](#) [alkalmazás](#) [kártévő](#) [csaló](#)

Jó pár évvel ezelőtt a mindig kéretlen, néha kártékony reklámok, semmit érő alkalmazások, **popup és popunder ablakok** tudták egy böngésző kilens előtt ülő életét megkeseríteni. Aztán ebből is [kialakult a hamis vírusirtók mostani vérvonala](#), de a mai korunk sláger célpontja kétségtelenül a Facebook közössége.



A nagy különbség a "mindenre kattint, ami mozog" mentalitásnál az, hogy míg egy böngészőben a fenti képhez hasonlóan csak a gépünknek vagy saját magunknak adunk mattot, **míg a Facebook esetében ismerőseinknek is próbára tesszük a türelmét, kárt vagy gondot okozhatunk nekik.** Ez lehet akár azzal is, ha hamis bejelentkezési - adatahalász oldalon - lépünk be. Ebből is jött ma egy, és aki ezen belépett, az nem csak magát, de az ismerőseit is kitette a későbbi csaló, vagy kártékony linkre mutató üzeneteknek.



[A hamis alkalmazások - amelyek azt ígérik](#), megmutatják ki bannol téged, ki szeret a legjobban, mik lesznek a jövő heti lottószámok, **shocking videó** lejátszása bármilyen tetszőleges érdekesítő témakörben - aztán szétdúlják a címlapot, orvul lájkolgatják magukat, orvul szétküldik magukat a nevünkben ismerőseinknek, elküldik adatainkat a nagyrabecsült fejlesztőknek, [kéretlen programot telepítenek gépünkre vagy emeltdíjas SMS játékokra invitálják](#) a nagyérdeműt. Persze nagyon is **velős filozófikus kérdés felvetés lehet, hogy mennyire is "kéretlen"** mindez, ha maga a user (persze mélyen megtévesztve) de mégiscsak kattintgat bőszen a vártán.



És ezek a cuccok - [Az emberek 98%-a nem tudja 17 másodpercnél tovább nézni ezt a videót](#) - mindig célt érnek a felhasználók egy részénél. Mostanában van [terítéken a Like/Dislike gomb körüli szemantikai vita](#). Van azonban ennek emellett egy nagyon is gyakorlati vetülete is: [kezdenek jönni az ezzel kapcsolatos átverések](#), hamis alkalmazások, csalások is.



Ma pedig ismét felbukkant egy új becsapós Facebook alkalmazás, amely az alábbi üzenettel próbálja felhívni magára a figyelmet: "The hidden message behind the Google logo, that Google was hiding from us." **Erre kattintva egy alkalmazást látunk, ami szépen megkér bennünket, hogy amennyiben szeretnénk megtudni a titkos üzenetet, lájkoljuk az alkalmazást.** [A tavasz 17 pillanatánál megismert csali captcha-szerű kérdés](#) itt is megjelenik, aztán ez vagy egy My Web Search Toolbar nevű kéretlen programot tölt a gépünkre, vagy egy fizetős, magyar nyelvű SMS játékokhoz vezet.



Egészséges lelkiületű felhasználó egyikre sem vágyik ezek közül. Egy vadonatúj profil készítésekor már az is izgalmas kérdés lehet, hogy nulla ismerettséggel és kapcsolattal miért pont ezt dobja a gép ajánlott oldalak címszóval, de nekünk most inkább a SocialBuzz miatt lehet több aggodalmunk.



Ezenfelül világlátott emberek elmondása alapján az is csekély élvezetre lehet garancia, hogy [a domain bejegyzése mindössze csak pár napja](#) történt. Inkább ez lehet a shocking, ha már.



Akit érdekel, olvasgathatja a facebook.com/biztonsag lapot, amelyen sok, **a közösségi oldallal kapcsolatos veszélyre hívják fel a figyelmet**. Amelyekből láthatóan a jövőben sem fogunk hiányt szenvedni - Fülíg Jimmy őszinte sajnálatára. Az alaphelyzet persze továbbra is az, hogy **senki nem tart töltött pisztolyt a haléntékunkhoz, hogy mindenféle szedett-vedett alkalmazást telepítsünk, megbízhatatlan fejlesztőkben mégis megbizzunk, ismeretlen sudribunkóknak lájkoljunk**. Ez mindenkinek a saját egyéni döntése, aminek időnként következménye is van. Hiába no, az Élet kegyetlen ;-)

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

 Megosztás  +1  0

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2225986>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Android is watching You

2010.08.18. 09:45 | [Csizmazia István \[Rambol\]](#) | [4 komment](#)

Címkék: [trójai android kémprogram](#)

Na jó, a cím valóban nem elég pontos. Valójában arra gondolunk, ahogy a PC-n is, **itt sem lehetünk soha biztosak abban, amit telepítünk, az pontosan mi is.** Meglepetések - még ha ritkán is - azért itt is vannak.



[Ahogy növekszik az Android népszerűsége](#) - nem kell feltörni, bármit telepíthetünk rá, násztánc nélkül USB kulcs, [tetszőleges szolgáltatóval használható](#), könnyebb vele a sört nyitni, stb. - úgy kerül [egyre jobban a kártevőszervezők érdeklődési körébe is](#). Ahogy az új autónál is csak az első karcolás fáj, lassan [már itt is rezignáltan hallgatjuk a híreket a következő, kémprogramot vagy trójai kártevőt rejtő ingyenes alkalmazás leleplezéséről](#).



Lassan itt a telefonos applikációk esetében is **egyre nehezebb lesz eldönteni, mi a kártevő és mi nem az**, milyen funkciók gyanúsak, kétesek és legálisak. Ugye az [iPhone 4.x egyik nagy újítása a felhasználók koordinátáinak begyűjtése](#), és ezek az - állítólag névtelen - adatok a fejlesztők, reklámozó cégek felé elérhetőek, ezt kell el fogadnunk az IOS telepítés előtt az új felhasználói szerződésben.



Most épp [egy androidos kígyós játékban találtak kémprogramra jellemző funkcionális](#): a háttérben futva figyeli a telefont a GPS Spy segítségével. Klasszikus besorolás szerint ez nem vírus, de trójainak bátran nevezhető. **Az egyetlen amit tehetünk minden okostelefon esetében, az az óvatosság, gyanakvás, gondos tájékozódás még a programok telepítése előtt**, de akár imádkozhatunk is, vagy [aki minden hétfőn hármat köp kelet felé egy barna kavicsra, azt nem érheti](#) megrontás ;-)



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



0

Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- ["Szósölmédia" és nyaralás](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2229907>

Kommentek:

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

vrtx 2010.08.18. 10:53:25

Érdekes, üde és jó kis cikk! thx

nyos 2010.08.18. 17:50:48

Elvileg minden program telepítésekor kiírja, hogy milyen jogosultságot kér magának. Ha egy kigyós játék GPS hozzáferést kér, az gyanús. Ha mégis engedélyezzük, akkor meg ki a hülye?



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.08.18. 21:55:26**

Szia vrtx és nyos!

A trójai telepítéssel kapcsolatos PEBKAC dologgal egyetérték.

Sajnos még nem volt személyesen dolgom Android telefonnal. Talán majd a következő készülékem ilyen lesz?

Érdek Lődő 2010.08.19. 12:59:12

Nekem ez a link működik: mek.oszk.hu/01000/01038/01038.htm

Antivírusburgi Ünnepi Játékok

2010.08.18. 23:59 | [Csizmazia István \[Rambol\]](#) | [15 komment](#)

Címkék: [iwiw játék](#) [xbox](#) [facebook](#) [évforduló](#) [kamuprofil](#)

Sajátos módon [szeretnénk megünnepelni az Antivírus blog harmadik születésnapját](#). Kamuprofil vadászatot hirdetünk, a cél, hogy minél egyedibb módon buktassanak le hamis iWiW profilekat és facebook adatlapokat a versenyzők.



Kamuprofil vadászat a facebookon és az iWiWen - Több mint 20 SP közül melyik az igazi? Ez a címe az akciónak. Egyes felmérések szerint a közösségi oldalakon található [adatlapoknak közel 40%-a hamis](#). Rengeteg ember szeretne sztárok bőrébe bújni, és így ismerkedni másokkal. A facebookon és az iWiWen együttesen körülbelül 20 Éder Krisztián adatlap van, ezek közül 19 biztosan nem az igazi SP-hez tartozik.



Mégis, mindegyik rendelkezik néhány ismerőssel, és akad közöttük több, amelyiket már 6-700 felhasználói jelölést kapott - többnyire fiatal lányoktól, akik rajonganak az énekesért. Úgy tűnik, **Talmácsi Gáboros** is népszerű játszani, hiszen az iWiWen hárman is a motoros világ bajnoknak adják ki magukat, de Steiner Kristófból, Benkő Dánielből, Zimány Lindából, valamint SP barátjából, **"Fluor"** Karácson Tamásból is több van.



A közösségi portálok felhasználói szabályzatába ütköző profilhamisítás ugyan jópofa játéknak tűnhet, de **valójában visszaélés egy sztár hírnevével és a felhasználók bizalmával**. Komolyabb esetben a hamisító olyan pszichológiai játékba is belemehet, ami egy rajongóban hosszú távú sérüléseket okozhat, de [akár megpróbálhat pénzt kérni tőle, mondjuk arra hivatkozva, hogy külföldön van, és kirabolták](#).



Most meghirdetett játékunknak az a lényege, hogy a versenyzők legális eszközökkel igazolják egy-egy profilról, hogy az hamis. Az eredményhirdetésnél nem a lebukott adatlapok száma dönt, hanem az számít, hogy a hamis profil hány ismerőssel rendelkezett,

és mennyire volt érdekes a bizonyítás.



A beküldési határidő: 2010. szeptember 10. 23:59 perc, eddig fogadjuk el a kamuprofil KUKAC eset PONT hu címre érkező, valódi feladónévvel érkező pályázatokat, melyhez minden esetben linkeket és képernyőképeket is kérünk mellékelni.



A versennyel a közösségi oldalak biztonsági kérdéseire kívánjuk felhívni a figyelmet, a játékot az [ESET magyarországi képviselőjét ellátó Sicontact Kft.](#) szponzorálja és a [PS:PROvocative pr](#) ügynökség koordinálja. **A legérdekesebb nyomozást lebonyolító versenyzők értékes ajándékok - például Xbox 360 játékgép, 50 ezer forintos Swarovski vásárlási utalvány és újság előfizetések szintén 50 ezer Forint értékben - közül választhatnak. A verseny eredményhirdetésére 2010. szeptember 17-én, az Antivírus blog születésnapi posztjában kerül sor.** Sok sikert a pályázóknak!

 Tetszik  55 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

• [1 trackback](#)

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2231639>

Trackbackek, pingbackek:

[Trackback: Kamuprofil vadászat a Facebookon és az iWiWen](#) 2010.12.04. 22:18:55

Kommentek:

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



[kártékony 2010.08.19. 16:30:20](#)

Az iwiw crew -becsületükre legyen mondva- már évekkkel ezelőtt indított projectet arra, hogy a kamu regisztrációkat automatizált eszközökkel kiszűrjék, illetve hogy a klubként működő accountokat áttéreljék a klub rendszerbe. Higgyétek el, nem egyszerű a dolog algoritmizálása! Nagyon sok kamu account már kiszűrésre került, de sok lúd disznót győz sajnos... :(

Jó ötlet lehet közösségi összefogással küzdeni az idioták ellen, bár én kétlem, hogy megvalósítható a dolog. Egyrészt azok a retardáltak, akik létrehoznak ilyeneket, azok ennyi erővel valódi accountokat is jelenthetnek kamunak (mert mondjuk haragszik az illetőre).

Innentől kezdve pedig érdekes kérdés, hogy megéri-e akár egyetlen valódi személy adatlapját is "tévedésből" kitörölni cserébe azért, hogy 100 hamis profil eltűnjön...

[PS:PRovocative pr ügynökség 2010.08.19. 17:44:45](#)

Néhány tipp, hogyan lehet azonosítani egy hamis facebook profilt:

www.hellboundbloggers.com/facebook/identify-fake-facebook-profiles/

[Boorisz 2010.08.19. 20:38:24](#)

Bármilyen profil lebuktatása számít vagy csak híres ember másolat?



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu 2010.08.19. 20:51:37](#)

@Mr. Pickles:

A kamuprofil az a kamuprofil. Nyilván érdekesebb, ha egy ál Sylvester Stallone-n ütsz rajta, mint egy John Doe-n vagy Üzmürü Tükmüty török alsómosón.

PS. A blog oldalad látszólag nem működik, ez direkte van így?

[50-es anyuka 2010.08.20. 12:23:31](#)

Nagy Testvér nagyon ideges, amiért zavart okoznak a kamuemberek. Szerintem jó sok kell, amióta az emberek saját nevükön vannak fent a neten (amit már a 90es években is kiröhögött mindenki, akinek egy csöpp esze volt) aztán ezzel saját magukat és másokat, ismerőseiket, barátait, rokonaikat is veszélybe sodorhatják, majd utóbb meg megy a sírásrívás...

[detwebprog 2010.08.20. 19:09:13](#)

Sziasztok!

Először is díjazom mindazok fáradságát akik megpróbálják felderíteni a kamu profilokat,de.....!

Nem akarok senkit elkeseríteni de ez "hiábavaló" fáradság lesz!Még egyszer hangsúlyoznám díjazom az ötletet!Általában ezeket a profilokat vagy marketing szempontjából vagy a cikkben leírtak miatt hozzák létre,de számos oka lehet!Azt gondolom hogy egy profi "játékos" tudatosan hozza létre ezeket a profilokat!Az én tapasztalatom szerint nagyon nehéz lenyomozni ezeknek a profiloknak a tulajdonosait (mármost a kamu tulajokat)!Ezek az emberek általában proxy mögül vagy egy internet kávézóból irányítják ezeket!Természetesen a csalókra gondolok akik pénz és egyéb módon próbálnak hatni a rajongókra! Szóval nem tudom mi lehet a legjobb megoldás ebben a helyzetben de egy biztos!A legjobban látogatott oldalak nem tudják kontrollálni a helyzetet!Tehát ha sikerül is valakinek kinyomozni egy profilt abban biztos lehet,hogy pár héten belül újabb és újabb jön létre!Ez egy ördögi kör!

Én csak annyit javasolnék mindenkinek,hogy nagyon vigyázzon az ilyen csalókkal és ne adja ki adatait ezeken az oldalakon

keresztül!

Írta egy webmester!

ivrilider 2010.08.22. 14:39:48

Én a játékba nem nevezek be egyelőre, de oldalvállról talán majd gyűjtögetek néhányat, mert ebben jó vagyok. (Nem motivál eléggé a díjazás - sem.) Tehát most csak azt tenném föl, hogy szerintetek ilyen kamuprofil miért csinál valaki? Nem is az, hogy miért, mert annak pszichológiai magyarázatai lehetnek. Hanem hogy mi lehet a célja vele? www.facebook.com/profile.php?id=100001334315192

Boorisz 2010.08.23. 23:20:50

@Csizmazia István [Rambo]: elfelejtettem kiszedni a törölt blogom ciki :S .

No akkor neki állok nézelődni, majd ki kell találnom, milyen formában küldöm majd el. :D

Wyzard 2010.08.24. 10:03:45

Sziasztok !

Mi számít legális ill. nem legális eszköznek ?

Üdv



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.08.24. 11:52:51**

Hello Wyzard!

Örülök, hogy felkeltettük az érdeklődésedet :) Mivel nem hacker versenyt hirdettünk, így például nem ér feltörni valakinek a postafiókját, vagy kémprogramot telepíteni valakinek a gépére.

ethicalhacking.hu/btk300.aspx

Ha ezeket nem sérted meg, akkor nincs gáz. Azt persze aláírom, hogy a legális - illegális határ eldöntése nem mindig könnyű feladat, na meg az ember nem mindig szeretné az öreg szabálykövető legkisebb fiának érezni magát :-)

Wyzard 2010.08.24. 13:22:25

@Csizmazia István [Rambo]: köszönöm a választ. Persze a delikvens gépének buherálása meg sem fordult a fejemben, de nem volt világos, hogy amúgy mi lehet illegális.

Most már letisztult bennem, köszönöm. :)

atila68 (törölt) 2010.08.31. 23:35:04

Azt az egyet nem értem miért pont egy mainstream ratyit és a párját kell példának felhozni, ha már olyan fontos, hogy a rajongóban ne keletkezzen hosszú távú sérülés?
Nem, nem Talmácsira (reszpekt) gondolok.

atila68 (törölt) 2010.08.31. 23:36:05

@ivrilider: Miheztartás végett.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.09.11. 20:14:07**

Ma hajnali 00:00 órakor véget ért a játék, most jön a zsűrizés nehéz feladata :-)

Jarod1 2010.09.18. 12:56:22

még nem vagyok a Arckönyvben de nem is akarok még az iwiw is sok...

Hordozható Threat Center iPhone-ra

2010.08.24. 08:15 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [apple](#) [ingyenes](#) [iphone](#) [app](#) [store](#) [center](#) [threat](#)

Megjelent az ESET ingyenes alkalmazása az App Store-ban, amellyel naprakész vírusinformációkat, Randy Abrams podcast bejegyzéseit, a vírusvédelmi cég munkatársainak Twitter, Facebook és Youtube üzeneteit kísérhetjük naprakész figyelemmel.



[A iPhone-ra készült programot](#) a "threat center" vagy "antivirus" szavakra keresve találhatjuk meg az iTunes felületén, és ingyenesen telepíthető. Az alkalmazás augusztus 21. óta érhető el angol nyelven.



Segítségével a fent említett információkon felül **biztonsági tippeket**, **termékinformációkat is olvashatunk**, nézegethetjük a Threat Center világtérkép pillanatnyi helyzetét, Malware reportokat hallgathatunk meg, illetve az aktuális, **friss céges blogbejegyzéseket is egybegyűjtve** kaphatjuk kézhez okostelefonunkra.



 Tetszik  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.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Majdnem mindenki átverhető adathalászattal](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2242270>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Közelg a perc, jön a Hacktivity 2010

2010.08.25. 11:01 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [hacktivity hacker kert 2010 durer](#)

2010. szeptember 18-19-én kerül sor a Hacktivity 2010 konferenciára a Dürer kertben. Kelet-Közép-Európa legnagyobb hackerkonferenciájára az eddigi regisztrációk alapján akár 2¹⁰ fő is érkezhethet, köztük sok külföldi, mivel idén először az előadásokat folyamatos szinkrontolmácsolás kíséri.



Két nap, 28 előadás, 2 workshop, 3 tréning, egy kerekasztal vita, Wargame, Capture the Flag, Hack the Vendor játékok 100.000 ft-os nyereményekkel, Wall of the Sheep, Hardver workshop Mitch Altman-nal, egész nap sör, hot-dog, pizza, jó beszélgetések, falmászás és este fergeteges buli. Körülbelül így lehetne leírni egy mondatban a legrégebbi hazai független IT biztonsági rendezvény 2010-es évi programját. Az esemény túlzás nélkül rendkívül sokszínű lesz. **A szombati keynote speaker nem más, mint Bruce Schenier Amerikából, aki a világ egyik leghíresebb IT-biztonsági szakértője.** Bruce reggel nyitóelőadást tart, majd a nap végét is ő zárja azon a könyvbemutatón, ahol dedikálja HVG Kiadó és a Kancellár.hu Zrt. közös gondozásában magyarul is megjelent Schneier on Security című könyvét.



Vasárnapi keynote speakerünk "FX" Lindner a "Hogyan Lopjunk Kontinentst" hacker kultuszkönyv társszerzője, aki 2001-ben elsőként írt Cisco IOS Exploit-ot a világon.



Feltűnik ismét a színen Alexander Kornbrust Oracle guru, és egy vírusszakértő, [Robert Lipovsky is ideérkezik az ESET laborból, Pozsonyból.](#)



Idén a jogi előadók egy egész szekciót kitesznek, és 3 előadás erejéig bepillantathatunk az informatika hőskorába is. Téma lesz idén a wifi hotspot „használat”, az IT SEC Compliance, a password cracking és az egghunting is. Két workshop is színesíti a szakmai programot, ahol **a szimpla prezentáció helyett az előadók által bemutatott technikák laptopokon azonnal kipróbálhatók lesznek.**

Persze nem maradhat el a szokásos kikapcsolódás és buli sem, a kancellar.hu mászófallal készül, este pedig ismét lesz Balabit kontinens party italtúrával és rock koncertekkel. **Örömmel jelentjük, hogy a szponzorok között az ESET neve is megtalálható.** A biztonságos wifi infrastruktúrát a Biztribútor biztosítja, a technikai támogató pedig a SilentSignal lesz. További információk és előregisztráció szeptember 5-ig a www.hacktivity.hu weboldalon.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás

+1 0

Tweet

Ajánlott bejegyzések:



- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [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/2246055>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Ismétlés a tudás jó édes anyukája

2010.08.27. 15:35 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [stalker](#) [facebook](#) [alkalmazás](#) [hamis](#) [fancheck](#) [profilspy](#)

Szeretnél örökké élni? Esetleg nyerni a lottón? Vagy csak azt megtudni, pontosan ki is nézte meg a Facebook adatlapodat? **És ez most nem csak vicc, tudom, eddig tényleg csak csupa csalás, meg kártevő terjesztés volt ezekben, de ez mostani már tutira működik.** Ugye elhiszed tesó, napróbáldkimárgyorsan, lécci-lécci-lécci!



[A Fan Check, Stalker, és a többi hasonló alkalmazás](#) akár egy jól nevelt fénix madár, hamvaiból újra és újrászületve feltűnik a színen, új névvel, de régi ígéreteket újra megígérve. És sajnos a "Hány éves is vagy te királyfi, és még mindig hiszel a mesékben..." módon rendre van közönsége is.



Ezúttal [a Sophos hívta fel a figyelmet az újabb ProfilSpy nevű Facebook alkalmazásra](#), amiben az a mókás, az előző trükkbeli üzenethez csak hozzá kellett fűzni pár mondatot: **"Óh Istenem, ez hihetetlen, ez most tényleg működik. Most már tényleg lehet látni, ki nézte meg a profilodat!"**.



Ennyi erővel [a hamis Antivirus 2010 elé is oda lehetne szúrni](#), hogy "Eddig ez tényleg egy zsaroló, vírusokat egyáltalán nem irtó pánikprogram volt, de most már nem az, kisdobos becsszó, ez az új Antivirus 2010 ez most már aztán tényleg irtum-burgum irtja a vírusokat, jobb mint a Norton, a NOD32 meg a Kaspersky együttvéve, komolyan, óh, jaj, nem, hát ez hihetetlen, nézd George, már tiszta is gépem, és milyen gyorsan, ezt meg kell nézned, OMG a négyzetten vagy a köbön!"



A gondolkodás nélkül végzett ténykedések, például az így telepített alkalmazások mindig jó táptalajai voltak-vannak-lesznek a csalóknak, kéretlen reklám- és kártevő terjesztőknek. Mindent elhinni jó, [mindent elhinni szép](#). Retorikailag úgy tűnik, [ez a hárombetűs szó mostantól minden Facebook csali alkalmazás neve elé be fog majd kerülni](#). OMG, OMG és még egyszer OMG. Hát lehet ennek ellenállni? Na jó, ez csak amolyan költői kérdés volt.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP él, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés [trackback címe](#):

<http://antivirus.blog.hu/api/trackback/id/2251693>

Kommentek:

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

sydneyboy 2011.04.23. 22:10:02

remelem a vírusokhoz jobban konyit e fenti sorok szerzoje, mint a fogalmazashoz...

Rettenetes gyenge poszt, informaciot meg csak nagyon nehezen sikerult belepreselni. Lathatoan lekototte az energiakat a barokkos fogalmazasra torekves, melyet messzirol sikerult elkerulni...

Kártékony antivirus linkek - villám őrjárat 2.

2010.08.31. 12:20 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

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

Egyfajta röpke "Link Patrol" keretében teszünk **időnként kisebb őrjáratot hamis vírusok, a hamis antivírust terítő linkek nyomában**, különösebb sallangok, terjedelmesebb tiszteletkörik nélkül. Most egy **a nevében már 2011-es évjáratú antivírussal foglalkozunk**.



Közeledik az új esztendő, [itt az AV Defender 2011](#) program. Már [a domain foglalás is aranyos](#), 2010 július 29-i dátummal bír ez a végretekint megfizethető, világhíres cég, ahol **a kapcsolattartási email cím is meg ér egy misét**.



És amelynek weblapján a nyájas olvasók még nyájasabb bejegyzései olvashatóak. A londoni Garry Lyuis életét szinte egy csapásra megváltoztatta az AV Defender 2000, **amit el is hiszünk neki**, ha arra gondolunk mit érzett, mikor eltűnt a pénz a számlájáról. Hasonló elragadtatással beszél a biztosan létező ausztriai Nicholas Salzburg és a párizsi Elena K. is, csak ajánlani tudják ezt a velejéig mesterművet, ami kevesebb mint öt perc alatt kitisztította a bankszámlájukat öööö izé a számítógépüket. A magyar Malyomváry Armandó Zombáról is csak dicsérni tudja ezt a kiváló programot, őt azonban valamilyen homályos okból, színelig helyhiányra hivatkozva lehagyták a testimonials oldalról.



Szerencsére, [a telepítőt már keresztnévén szólítják a valódi vírusirtók](#), így legalább ők nincsenek óriási meglepetéseknek kitéve.



Kedvenc részeink a FAQ-ból. Honnan tudjam, hogy az önök oldalán végzett tranzakció biztonságos? Hehe, hát mert 128 bites ultramodern NASA titkosítás van itten kérem tisztelettel - válaszolja a főcsaló :-). Na és persze mint leglényegesebb vírusproblémát, részletesen és szájbarágósan elmondja, honnan kell a CVV három karakteres biztonsági kódot leolvasni a bankkártyáról, amivel a bűnözők azonnal pénzt vehetnek le.



A cég címe és hamis telefonszáma már bukkant fel [korábban egy oroszországi weboldalon](#), most ugyanez egy Hollandiában hosztolt gépről köszön vissza.



Bár a Google Maps alapján **maga a cím létezik ugyan, de azért a világhírű AV Defender Inc. személyes meglátogatása okán ne fecséreljük értékes szabad időnket repülőjegy foglalásra.** Cégük ars poetica-ja szerint ők a biztonságos számítástechnikát kívánják szolgálni világszínvonalú szoftvereikkel és különleges ügyfélszolgálatukkal.



Küldetésükkel kapcsolatosan nekünk viszont inkább más jut az eszünkbe, mi hova küldenénk őket sokkal szívesebben ebben a zord hidegben, amely éghajlaton bizonyára kevésbé fáznának.



Zárni minden villám őrjázatunkat egységesen ezzel az okossággal fogjuk: **"Soha ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google szinte összes találatát „How to remove...” szófordulattal kezdődik."**



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



Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

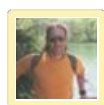
<http://antivirus.blog.hu/api/trackback/id/2260882>

Kommentek:

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

[bolhabetu 2010.08.31. 20:05:45](#)

Az mitől van, hogy a Virustotal tanúsága szerint több vírusirtó is azt írja oda a felismeréshez, hogy "Not a virus"?



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.08.31. 21:28:42](#)

Egyrészt sajnos valóban jó sok különböző néven emlegetik, ami nagy knockout a szakma hön áhított egységes név konvenciók törekvéseinek.

De visszatérve a kérdésre ez egy kártékony pánikprogram (scareware), ami nem klasszikus fertőző vírus.

Fő célja inkább a pénztárcád megcsapolása, a nem létező fertőzés állítólagos mentesítéséért, vagyis a semmiért kifizetendő x dollárod bánhatja, és ehhez megtevesztve ugyan, de te magad nyomod meg az entert.

[Tomi1977 2010.10.06. 14:34:31](#)

Tanácsot szeretnék kérni Tőled Rambo, de bárki más is segíthet, ha tud.

Sajnos úgy állok anyagilag, hogy nem tudok antivírus szoftvert vásárolni, de olyan programot sem akarok használni, amelyek csak a nevében vírusirtók, a valóságban kártékonyak.

Elegendő lehet valami ingyenes program?(Pl. Avira, Panda Cloud, Avast, Avg.)

Vagy telepíthető 30 naponta a NOD 32 teljes funkcióval?

Köszönöm válaszod!

Tamás



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.10.06. 17:33:10](#)

Szia Tomi1977!

Ha Chip vagy PCW újságot olvasol, akkor abban is szokott lenni havi telepítési kód NOD-hoz. Ha nem, akkor lehet Avast vagy AVG antivírust feltenni, de én még tennék mellé külön ingyenes kémprogramirtót is, például A-Squared, SpywareTerminator is, sőt tűzfalból is van például a Comodo.

De akár mindez égi jel lehet arra is, hogy a spórolást összekösd a Linux-szal való ismerkedéssel :-)

[Tomi1977 2010.10.06. 20:58:26](#)

Köszönöm a válaszod, megfogadom!

Hello Barát

2010.09.02. 12:15 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [email holland család 419](#)

Akarol te sok pénzt ottan máma? Mindössze annyit kell tenni, hogy "álljon, mint a legközelebbi hozzátartozó a halál, én ügyvéd folyamatot". Sima ügy. Akinek ilyen barátai vannak, annak már is nincs szüksége ellenségekre.



Hogy, hogy nem, a főcsalók többnyire valamilyen cirkalmas feladóval jelentkeznek, mint akik megirigyelték az extra hosszúságú Waszlavik Petőfi Velorex Ullman Mónika Sámán László és hasonló csengésű neveket. Aki még emlékszik [Peter Lee meleghangú levelére](#) Hongkongból, vagy [Mr. Patrick K. W Chan jövedelmező üzleti](#) javaslatára, valamint [Mr. Peter Wong Tung Shun "Üdvözetek és bókákat"](#) tárgysorú szívmengető írására, annak most is felcsillanhat a szeme: az idő folyamán mindig egyre hosszabbra hízott a feladói név.



Ezúttal Mr. Arjen Van Dirk Martinus Sebastiaan írt egyenesen nekünk, hogy magyarul-e, annak eldöntését az Olvasóra bízunk. Mindenesetre ebben a [220 felett száguldú átértékelt svájci frankkal terhelt](#) válságos pénzpiaci világban végre akad valaki, aki önzetlenül anyagi biztonságot nyújtó mentőövet dob felénk. Köszönjük! **Szemlátomást a Batáviában közös cellában raboskodó Fülíg Jimmy, Csülök, Tuskó Hopkins és Török Szultán ismét ceruzához és papírhoz jutott valamilyen furmányos módon a nem megfelelően őrzött mosodai hátsó raktár jóvoltából**, és megpróbálták görcsös igyekezettel összehozni egy épkezláb levelet. Bár hidegló nincs benne, hitelesebb ajánlatot el sem tudunk képzelni.



Azt a korábbi kísérletekből megtanulták, már régen [nem afrikai császár nevében kell nigériai üzenetet írni](#), mert az a mai világban széles körben lejáratódott, és bizalmatlanságot szül. **E félelmetes hősök - akiknek a helyesírásuk is félelmetes - ezúttal egy holland pénzügyminisztériumi dolgozó bőrre bújva mixelték össze a 419-es szakma fontos elegyeit**: állítólagos kimentendő hatalmas vagyon, örökös nélkül elhalt ausztrál milliomos, AOL-os privát emailcím.



Megnyugodhatunk, minden precízen elő van már készítve számunkra: **"lehetővé teszi a pénzeszközök átutalását a bankszámláját jogilag egy rántás, vagy a probléma"**, így semmi nem áll az útjában annak, hogy a vállalkozó kedvű nyájas olvasó jelentkezzen a tetemes summáért. Ha már a bankszámla is jogilag rántás, akkor nincs is ebben semmi kivetni való, elhárult immáron minden földi akadály. Vajon megtanulnak egyszer rendesen magyarul is? Talán sosem tudjuk meg. **Mindenesetre jó látni, hogy vannak, akik mindig inkább csavarnak egyet a dolgokon, de fel nem adják sohasem :-)**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Akiknek a Captcha kényszerűsége](#)
- [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/2266159

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Fejlett Facebook ficsörök

2010.09.06. 15:10 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [biztonság](#) [facebook](#) [távoli kiléptetés](#)

Ha lassan is, de jól alakulnak a biztonsággal kapcsolatos fejlesztések. Ezúttal a **bejelentkezési adatokkal kapcsolatos ellenőrzést erősítették meg a Facebooknál** távoli kiléptetési lehetőséggel.



Nem a legkellemesebb élmény, ha az embernek [a feltört postafiók remedyt kell követnie lépésről lépésre](#). Az, **hogy ezt a lehetőséget elkerüljük, azért mi magunk is tehetünk**: használhatunk erős jelszót, egyedi jelszót amit sehol máshol, valamint időnként - für alle fälle vagy rendszeres időközönként is - lecseréljük egy még vaddisznósabbra, plusz futtatunk védelmi programokat. Ez kb. nagyjából a mozgástere a felhasználónak.



Ezt hányan eszik meg: add meg nekünk egy másik helyen használt jelszavadat, mi pedig szívesen és készségesen segítünk neked, hogy megnyerd a Guinness legtöbb ismerőssel rendelkező homo sapiens kategóriát, mert mi szeretünk téged :-)

Amit viszont az üzemeltető segíthet - a https belépés alapkövetelmény (lenne) mindenhol - **az a bejelentkezések egyszerű monitorozása, az esetleges illetéktelen belépők távoli kiléptetése**. Na és persze fogás esetén haladéktalan jelszócseré. **Ez a kellemes kontrol már egy ideje szépen muzsikál a Gmailben**, ha valami egzotikus vietnami címről nézegeti valami köbgyök a postafiókunkat, akkor egy kattintással távoli kiléptetés, jelszóvált.



És persze imádkozás, hogy **nem törölt/töltött le semmit illetéktelenül, illetve a nevünkben** nem regisztrált pedofil weboldalakra, küldött halálos fenyegetést különböző politikusok részére. Ilyenkor ugye nem Fam Van Donghot fogják elővenni elsőre, hanem a postafiók nyilvántartás szerinti tulajdonosát, aki felkötheti, hogy sikerüljön bizonyítania, igazából nem is ő volt. Illetve [sokszor már a gyanú, a letartóztatási vagy bírósági hercehurca is elég például egy munkahely elvesztéséhez](#), még ha később ki is derül az ártatlanság. **De az is éppen elég, ha "csak" spamet terjesztenek a nevünkben**.



2010. május óta a Facebook account is hasonló kényelemmel tartható ellenőrzés alatt, ehhez a Fiókom -> Beállítások -> Fiókvédelem lépéseket kell csak megtenni, és ott a Bejelentkezési értesítők végzik el ezt a feladatot. Kifejezetten jó ötlet volt, hogy a preferált emailcímre ismeretlen helyről történő bejelentkezéskor értesítés érkezik, így minimalizálható lett a kockázati időtartam. **Mostantól azonban egy virtuális tockossal nyomban akcióba is lendülhetünk: szanzsén kipöcköljük az illetéktelen mukinyulat a levesbe**. Az IP címek már itt is olvashatóak, közelítő pontosságú földrajzi hellyel, és az oprendszer-böngésző típusával egyetemben.



Mindenesetre **ha esetleg ilyen történne velünk, van még egy kötelező plusz házfeladatunk: végiggondolni, mi is vezethetett ehhez**: a vállunk felett valaki kifigyelhette jelszavunkat, nincs-e kémprogram a gépünkön, nem léptünk-e be idegen helyen, nyilvános közös gépről vagy nem használjuk-e valahol ugyanazt a jelszót.



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



Ajánlott bejegyzések:

- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2274590>

Kommentek:

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

[Art Mooney 2010.09.07. 17:43:45](#)

borzalmas ez a "15 éves kocka bent maradt a szamtech teremben ora utan" nyelvezet, sokszor nem is lehet erteni h ez most jo-e v rossz v sechole, tessenek mar erthetoen, targyilagosan imi, kthxbai



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu>](#) [2010.09.07. 21:40:49](#)

@Art Mooney:

>sokszor nem is lehet erteni h ez most jo-e v rossz

Ez most jó történet, értünk van :-)

Hogyan mennek a dolgok?

2010.09.09. 13:22 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [spam itunes csalás nyeremény ping](#)

Ahogy az érdekes híreknek, tragédiáknak, sporteseményeknek, [ünnepeknek megvan az apropo szolgáltató szerepe](#) a spam küldési táplálékláncban, [az újonnan megjelenő, várva várt eszközök, termékek](#), szolgáltatások megjelenésekor is rendre megjelennek a hírverést kihasználó csalók és adathalászok.



A cím eredete a [Vitathatatlan című film](#), amiben az öreg maffiózó (Peter Falk) a börtönigazgatóval beszélget arról, hogyan mennek a dolgok. "Nézze, a boxmeccs mindenképpen meg lesz tartva, ez ellen nem tehet semmit. A kérdés az, hogy inkább meghal, vagy pár napra szabadságra megy, becsukja a szemét és elfogadja azt az összeget, amit a számlájára utalunk. Mondom mégegyszer, a meccs az így is, úgy is meg lesz tartva."



Amikor nagy várakozás előz meg egy olyan új szolgáltatást, mint a ["zene Facebookja és Twittereként" aposztrofált Apple Ping](#), akkor sokan még örülnek is az olyan közösségi üzenetnek, amelyik [kitöltött kérdőív fejében ingyen iPhone telefont ígér](#). A recept mindig beválik, a nyeremény ígérete mágikusan vonzza az adataikat felelőtlenül kiadókat. Amikor egy közösségen belül kapunk üzenetet, a feltételezett megbízhatósági indexe mindig nagyobbra gondolt, mint a valóságban. Az átlagember bízik, nyerni egy ingyen iPhone okostelefont=MENŐ, és erre van is szerinte komoly esélye.



Minden hír, újdonság mellett [ott voltak-vannak-lesznek a könnyű nyereménnyel kecsegtető átverések, megtévesztések](#).

Figyelemmel kísérve a csalások és kártevők statisztikáit jól látható, hogy egyre kíváncsiabb platformot nyújt a bűnözőknek a több száz milliós közösségi felhasználói kör, amelyhez sok esetben elégtelen és lassú ellenőrzés, kései reakció társul az üzemeltetők részéről a biztonsági incidensekre.



Mekkora számokról is beszélünk? Facebook 500 millió felhasználó. Twitter 105 millió felhasználó. iTunes 160 millió felhasználó. És a spam áradat így is, úgy is el lesz küldve. Ezért minden közösségi oldalon jobban, gyorsabban, többet kellene foglalkoznia a biztonsággal, a spam, a megtévesztő és a kártevőket terjesztő üzenetek hathatós kiszűréssel. Meg [persze nekünk felhasználóknak is fejlődnie kell, gyanakvóbban és óvatosabban kellene viselkednünk](#). Hát reméljük, egyszer majd tényleg így mennek a dolgok.

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 őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kinszenvedés](#)

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/2282259

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 2010.09.09. 14:08:18

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.



Csizmazia István [Rambo] • http://antivirus.blog.hu
2010.09.11. 20:13:12

Szia Atko!

Jó a példa, tetszik :-)



atko 2010.09.14. 21:04:43

Kösz!

Sajnos hiába téped a szád! :-(

A vírusvédelem művészete magyarul

2010.09.14. 14:21 | [Csizmazia István \[Rambol\]](#) | [5 komment](#)

Címkék: [könyv bemutató](#) [péter szőr](#) [vírusvédelem](#)

Ezzel a címmel jelent meg magyar nyelven [Szőr Péter The Art of the Computer Virus Research and Defense](#) című világhírű kötete. A könyv nemcsak a víruslaborokban dolgozóknak biblia, de a [finnszági vírusvédelmi kurzusban a tananyag része is](#).



Magyarul is megjelent a legátfogóbb mű, melyet eddig a számítógépes vírusokról írtak. [A vírusvédelem művészete 650 oldalas](#) terjedelmének köszönhetően nem csupán tudományos súllyal bír, leginkább informatikusoknak és önjelölt hackereknek ajánlott.



A könyv egyik legérdekesebb tulajdonsága szerzője, a magyar származású Szőr Péter. A szakember Pápán született, Balatonfüreden nőtt fel, majd a Veszprémi Egyetemen vált informatikussá. **Az 1990-es évek elején még az OTP is az ő, Pasteur névre keresztelt vírusirtóját használta**, de Szőr Péter nemzetközi szinten szeretett volna a vírusirtással foglalkozni.



[1996-ban Finnországba, a mai F-Secure elődjéhez, a Data Fellowshoz került](#), ahol a kártevők megismerésén és szoftverfejlesztésen dolgozott. Emellett a számítógépes vírusok kutatásával foglalkozó CARO (Computer AntiVirus Researcher's Organization) szervezetben **olyan szakemberekkel működött együtt, mint John McAfee, Mikko Hypponen vagy Eugene Kaspersky**. 1999-ben átment a Symantechhez, ahol egészen a közelmúltig tevékenykedett vezető mérnökként, az **antivírus szoftverekkel kapcsolatban 38 szabadalom fűződik a nevéhez**.



A most kiadásra került könyv eredetileg az Addison Wesley kiadónál jelent meg 2005-ben, The Art of Computer Virus Research and Defense címen. A szakterület bibliájának számító művet **először cseh, majd kínai és lengyel nyelvre fordították le, míg végül hazaért, és a tegnapi napon a Károly körúti Alexandra könyvesház kávézójában a magyar közönségnek is bemutatkozott**.



A vírusvédelem művészete **két részben, tizenhat fejezetben tárgyalja a támadók és a védekezők lehetséges stratégiáit**. Bevezet „az élet játékaiba”, megmutatja a rosszindulatú programok elemzésének módszereit, és foglalkozik a kártékony kódok környezetével. Részletesen **elemzi a fertőzési és az önvédelmi stratégiákat, megismertet a kód evolúciós eljárásokkal és a vírusgenerálás eszközeivel**.

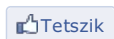




Ezután bemutatja a védekezési módszereket, a férgek blokkolásának eszközeit, végül a **hálózati szintű védekezés lehetőségeit**. Mindezt olyan alapossággal, hogy az olvasónak módja van mikroszkóp alá venni az egyes kártevők kódreszleteit is. Akit részletesebben is érdekel, itt [beolvashat az első fejezetbe](#).

Nézz meg a könyvbemutatón készült videót!

A vírusvédelem művészetének **kiadását Magyarországon az ESET magyarországi képviselőjét ellátó Sicontact Kft. támogatta**. A vírusvédelem művészetét [magyar nyelven a SZAK Kiadó adta ki](#), a könyv 9900 forintos áron került a boltokba, de [kedvezményes áron megvásárolható a kiadó honlapján](#).



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



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Akiknek a Captcha kínszenvedés](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2295322>

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](#).

GHost (törölt) 2010.09.14. 14:26:47

Belenéztem a tartalomjegyzékbe:

- API-hurok-módszer
- A szekciótábla és a leggyakoribb szekciók
- Behurkoló rutinok INT 13h

Ezek mind mind olyanok amiket nagyon felesleges volt magyarítani :)
Olyan kiskapu érzésem lett



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.09.14. 15:55:58**

Ne felejtse el azért, hogy az eredeti mű 2005-ben jelent meg. Azonban vitatkoznék veled ezeknek az említett részeknek a hasznosságát illetően.

Szerintem, aki vírusok iránt érdeklődik, ezekről mindet tudni szeretne, vagy víruslaborban dolgozik (korábban én is), az nem teheti meg, hogy megszakításokról, fat ablakokról, közvetlen lemezkezelésről, TCP/IP-ről, ilyesmikről ne tudjon mindent. Nálam akkor volt az a pillanat, amikor átkoztam a korábbi selejtezéseimet, és újból megvettem a Norton: az IBM pc assembly nyelvű programozása, és hasonló régi könyveket az antikváriumban. Ha könyv nélkül próbálnád ezt a sok mindent összeszedni, úgy vagy húsz év vírus bulletin újságot, konferencia anyagot, biztonsági publikációkat kéne végiggrágnod.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.09.14. 18:55:13**

Szia Ghost!

Egy cimborám hívta fel a figyelmet, hogy lehet úgy értetted, a "hook routines" vs "behurkoló rutinok" okozta nálad a felemás érzetet. Ha így van, akkor megértelek. Sok esetben nem alakult még ki elfogadott szóhasználat széleskörben bizonyos szak kifejezésekre, és néha inkább használjuk sokszor az angol eredetit. Pl. Barta Csaba hacktivitys rootkit előadása, ahol maradt a "hookolás":

hacktivity.hu/portal/downloadable/presentations_2009/Hacktivity_2009_Barta_Csaba_Rootkitek_hu.pdf

GHost (törölt) 2010.09.14. 20:05:29

Igen a fordítás volt a gondom, nem a tartalom, most kerestem meg eredeti angolban a könyvet az sokkal olvashatóbb. Én úgy gondolom, hogy felesleges erőltetni a szakszavak magyarítást, aki nem tudja mi az a hook annak valószínűleg nem való a könyv.

Bumika 2010.09.18. 22:17:13

Csatlakozom, én sem szeretem bizonyos kifejezések magyar fordításait. Gyakran csak a szöveggörnyezetből jövök rá, mit is akartak mondani.

Egyébként úgy gondolom, hogy szakmai lektor alkalmazása még ennél is fontosabb lenne a fordítások publikálása előtt. Csak egyetlen példa a Háló kalózzai című könyvből: a C nyelvű programkódban vélhetően a szövegszerkesztő automatikusan byte-ról bájt-ra javította a típusmegnevezést, amely egy fordítónak (kivétel ha C fordító :) nyilván nem tűnik fel...

Villáminterjú Szőr Péterrel

2010.09.15. 13:05 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [könyv péter szőr vírusvédelem művészete villáminterjú](#)

A [tegnapelőtti vírusvédelmi könyvbemutató](#) előtt lehetőségünk volt arra, hogy [Buherátor kollégával](#) közösen egy röpké pár perces villáminterjúban feltehessünk néhány kérdést az Egyesült Államokból hazalátogató Szőr Péternek.



Rambo: Szia. Bemutatom Buherátort, ő mindenféle exploitokkal, hackeléssel kapcsolatos témáról ír a blogjában, ami nem melleleg tavalaz az IT kategóriában megnyert egy hazai blogversenyt, de szokott előadni például a Hacktivityn is, én pedig az antivírus.blog-ot viszem, ami az antivírus, számítógépes biztonság témában próbál meg informálni. De tavaly már találkoztunk is a budapesti [CARO 2009 konferencián](#).

Szőr Péter: Sziasztok. Igen, most hallottam, hogy ez a Hacktivity egy ilyen ezres szintű jelentős konferencia lesz a hétvégén, de későn tudtam meg, így sajnos nem tudok maradni, már holnap utaznom kell vissza.



Rambo: Első kérdésem az lenne, hogy a Macintosh esetében mennyiben állt be változás szerinted az utóbbi időben? Konkrétan arra gondolok, hogy elvileg a FreeBSD alapok, a biztonságosabb struktúra, a Windowshoz viszonyított kisebb felhasználói tábor, a korábbi csak poweruserek színvonalának felhígulása - ma már divat a Mac, státusz szimbólum lett, egyre többen vesznek - valamint a dupla áron vehető Macnél még a felhasználók bűnözők által feltételezett értékes banki accountja mit változtattak a néhány évvel ezelőtti helyzethez képest, mit jelenthetnek a közeljövőre? Exploitok ugyebár vannak mindenhol, lásd a Secunia éves jelentéseit, vagy a CanSecWest versenyeket, ahol percek alatt törnek ezt is. Kell-e szerinted biztonsági program, vírusirtó Macre?

Szőr Péter: Már öt éve Macet használok, és pont az volt a motivációm, hogy amíg több millió kártevő van Windowson, addig itt nincs. Ez segít is egy darabig, de hosszú távon biztosan nem. A lényeg az, hogy amíg a Macos tábor viszonylag kicsi, nem éri meg rá kártevőket fejleszteni nagy üzemben, a támadás szempontjából egyszerűen nem éri meg, lényegesen jelentősebb profit van a Windowsos gépeken. A Unix alapra simán lehetett eddig is rootkíteteket csinálni, de az igaz, hogy fájlfertőző programok nem terjedtek el igazán sosem. [Igazi perspektívája a trójai programoknak van](#), mert ha a felhasználót megtevesztik, és ő megadja az ismeretlen program telepítéséhez a jelszavát, akkor bármi történhet. Jó példa erre a [tört iWork programokkal terjedő kártevők](#). Az igazi nagy előny oka emellett az is volt, hogy kevesen tudták programozni. Az utóbbi 2-3 évben viszont már Intel processzorok vannak, és ez az Intel kompatibilitás az exploitok terén mindenképpen hozott változást. A kártevő készítőket egy idő után ez a platform mindenképpen elkezd érdeklni, aztán ahogy a Macosok táborára nő, ez is nőni fog. Éppen itt az ideje a fejlesztéseknek, szerintem ez egy jó ötlet. De jelen pillanatban az a véleményem, sokkal olcsóbb PC-t támadni, mint Macet. Majd ha ez arány 30% lesz, akkor jelentős különbséget is előidézhethet ez a helyzet.



Buherátor: Akikkel beszélgetek, mind biztonsági témakörben mozgó emberek, és egyöntetűen az a véleményük, hogy a szignatúra minta alapú keresés egy vicc. Szerinted mi a jövője ennek a technológiának?

Szőr Péter: Könnyű kijátszani, és azt mindig is tudtuk, hogy csak a vírusokra működnek ezek igazán jól, a trójai programokra pedig nem. A jelenlegi helyzetben több millió program nagyon kevés embert érint, és ezek ellen olyan technológiát próbál meg erőltetni az antivírusgyártóknak egy része, amelyik elvesztette a hatékonyságát. Hatékony heurisztika nem jelent meg a trójai programok ellen, mert ezt sokkal nehezebb megcsinálni. Kellenek más módszerek is, és ezek közül az egyik egyébként már 1992 óta létezik, ez a virtuális kódemuláció az antivírus programokban, amellyel igyekeztünk megállítani a vírusokat. De visszatérve a kérdésre, szignatúrákkal védekezni muszáj. Az a véleményem, hogy csak úgy lehet valamit megállítani a legkorábban a belépési ponton, ha ezt előre tudjuk, hogy ez egy kártékony program. Ha egy szignatúra alapú védelmet egy ismert, széles körben elterjedt féreg ellen használjuk, mondjuk ott a Blaster, ami ott van tízmillió gépen percek alatt, akkor nagyon hatékony. De ha van egy millió program, és mindegyik millióra egy másik szignatúra, és ez a millió csak kevés számú, 2-3 gépen fut, akkor a hatékonyság csökken. De a tény, hogy igyekeznek kijátszani a víruskeresőt, hogy írnak egy másik verziót, ez mindig is ott volt. Én a szignatúrákban alapvetően hiszek, ám ha nincsen kombinálva különböző egyéb védelemmel, nincs tűzfal, nincs viselkedés alapú

kereső, stb., akkor a hatékonyságát tényleg elveszti.



Rambo: Már nagyban integetnek, hogy lejárt az időnk, ezért utolsó kérdésként azt tenném fel, hogy mennyire látod a levelezésre, böngészésre, facebookozásra is használt okostelefonokat veszélyben? Néhány platformra - Windows Mobile, Symbian - létezik ugyan néhány fajta vírusirtó program, de szerintem egyre inkább hiányzik a komplett - tűzfal, antivírus, kémprogram irtó, lopásgátló, titkosítást nyújtó, spamszűrő, stb. modulokat egyben tartalmazó - mobil biztonsági security csomag.

Ször Péter: Igen, ezt kérdezte már más is és ez valóban szükségesnek látszik. Attól félek azonban, hogy például az iPhone esetében az Apple egyszerűen nem fogja engedni, hogy antivírust fejlesszenek rá. Amíg az API-ban nincs meg ez biztonságilag, addig az OS-t fel kell törni, hogy víruskeresőt tudjál rá csinálni. De ugyanakkor akik pedig támadják, azok meg fogják ezeket csinálni, és ez egy elég nagy probléma.



Rambo, Buherátor: Köszönjük a beszélgetést, sok sikert az új projektedhez és kérünk szépen egy dedikálást a könyvbe.



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



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szósölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2297552>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 félj a holnaptól!

2010.09.16. 14:30 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [blog születésnap beszélgetés rambóval](#)

2007. szeptember 17-én [jelentkeztünk a legelső bejegyzésünkkel](#). Ezúttal nem feledkeztünk el az évfordulóról, és a [kamuprofil vadászat](#) végeredményének kihirdetése előtti napon a blog házigazdájával beszélgettünk.



Mikor, és miért indítottad a blogodat? Na jó, ez csak olyan ál bemelegítő kérdés, hiszen éppen abból az alkalommal beszélgettünk, hogy holnap lesz kerek három éves a blog. Milyen célod volt-van az oldal működtetésével?

Valóban, 2007 szeptemberében nyitottam. Munkahelyem, a magyarországi NOD32 képviselte is bőségesen ellát információval, de korábban is csináltam már hasonló "információs őrzőjratot", amikor az F-Secure és Kaspersky programok magyarországi supportja mellett a Vírus Híradó weboldal főszerkesztője voltam, vagy a Virusbuster víruslaborban angol és magyar híreket szerkesztettem a weblapra. A blog mellett külsőként a PC Worldbe, és időnként más lapokba (Chip, HVG, Elektronet, Playboy, CKM, stb.) is írok több kevesebb rendszerességgel vírusvédelmi témában cikkeket. Az lenne a legjobb egyébként, ha olyanok is olvasnák, akik nem szakemberek, hanem "csak" egyszerű hétköznapi felhasználók, emiatt pedig potenciális áldozatok. Egyelőre sok szakmabeli olvasót sejték a háttérben, és folyamatosan azon töröm a fejem, hogy lehetne a szélesebb, rászoruló "nongeeek" réteghez is eljuttatni a mondanivalót. Bár Antivírus a blog neve, abban persze már van változás, hogy amikor az antivírus programok úgy huszonöt éve elindultak, eleinte valóban csak klasszikus vírusok voltak. Ma már a kénytelen reklámoktól kezdve a hálózati férgek, kémprogramokon, trójaiakon, zsaroló titkosítás, személyiséglopáson keresztül az adathalászat, gyermekeink védelme a net ragadozóitól a botneteken át, a hamis letöltések, mindenféle kártékony kód, kártékony tevékenység is idetartozik, emellett a személyes adataink védelme is egyre fontosabb terület.

Kik segítenek az oldalad működtetésében? Mennyire fárasztó a blogolás?

Igazi one man force, Rambo egyszemélyes kommandója. Néha már eszembe jutott, talán jó lett volna egy kiegészítő társ, de végül így meg igazából a magam ura vagyok, és mindenért, jóérett-rosszért egy személyben lehetek büszke és felelős: ez a műfaj fekszik nekem a legjobban. Maga az írás nálam viszonylag lassan megy, sokat gondolkozom rajta, még többet újraolvasom és még ennél is többet javítgatom. Csak amikor már tökéletesnek érzem, akkor teszem ki végül.



Naponta mennyit foglalkozol a blogoddal?

Van pár száz RSS-em, pár tucat twitter csatornám, aztán kedvenc Google Alertjeimmel folytatom, és néhány szokásos netes forrást is átböngészek minden nap. A hírforrásokat blog nélkül is körbejártam, olvasgattam rendszeresen korábban is. Ezek kötelező násztáncok annak, aki képben akar lenni-maradni, tájékozódni akar. Konzolidáltan ezt úgy mondják, hogy "úszni és száraznak maradni egyszerre nem lehet" - rá kell szánni az időt. Áldott-átkozott szakma ez, hiszen a jó pap holtig tanul alapján mindig lehet-kell újat tanulni, és ez szinte minden idejét elveheti az embernek, ha hagyja. Ha benzinkutas lennék, akkor otthon ugye már "nem töltenék a kredenche", ha lejárt a műszak, akkor lejárt. A számítógépnél ez sosincs így, mindig van, aminek éppen utána kell nézni, ki kell próbálni, meg kell javítani vagy "csak" be kell fejezni. Persze ad ez rengeteg örömet is, kalandot, kihívást, hogy a "szellem emberének" érezhetem magam. Azért a családi békét és egyensúlyt mégsem egyszerű kibalanszírozni. A pap fejfájára egyébként ez van írva: "Befejezte tanulmányait" :-)

Honnan jött az ihlet, hogy ilyen témájú blogot indíts?

Igazából kollégáim javasolták, és eleinte kicsit tartottam is tőle, mert még sosem csináltam ilyet. Korábban más ősblogokat olvasva sokszor láttam a szórást, voltak nagyon jó, de nagyon gyenge webnaplók, és olykor a kommentelők szigorú hangneme is félelmetes képet mutatott. Szerintem egy szakmai blog, ha valaki benne él egy témában a munkája miatt, jó alap lehet a sikerességre. Olyasmi, mint egy diploma, ami papír önmagában ugyan jó ha van, de az igazi tanulás ezután kezdődik annak, aki valóban érdeklődik és el akar mélyülni benne. Itt pedig aztán van miben. Lenyomtam 12 évet programozóként nagyvállalatoknál, számtalan átvirrasztott éjszakával, megoldandó problémával, és állandó időzavarral a belefeledkezés miatt. Írtam már számítástechnikai szakkönyvet is, és úgy érzem, megtaláltam a helyem az alakzatban.



Egy-egy poszt megírása mennyi időt vesz igénybe? Mennyire kell megdolgozni az Index cimlapos sztorikért? És megértik-e az olvasók a

mondanivalódat?

Ezt nagyon remélem. Kicsit furcsa, de van, hogy beesik egy-egy idióta spam a postafiókomba, és amikor gyorsan megírom ezt, néha azonnal Index címlapos lesz. Míg amikor valami kísérletezőtől, nyomozgatótól felfedezést teszek vagy egy külföldi cikk állításait saját kezűleg leellenőrzöm, akkor az sokszor hiába fél nap, megmarad a néhány száz törzsolvasóknak. Nem kesergek ezen, de érzem, a bulváros események manapság szemléltetőbbek, ezzel szemben magamban igyekszem egy másfajta értékrendet is ébren tartani, és jó érzéssel tölt el, ha valaminek sikerül a végére járni. Ekkor úgy érzem, tudtam újat letenni az asztalra és ez a fontos. Nem az iskolának, hanem az Életnek tanulunk, és ugyanígy nem az Index címlapnak írjuk a blogunkat. Sokszor alapul a poszt valamilyen külföldi híren, amit először lefordítok, ellenőrzök, és gyakran igyekszem azt saját gondolataimmal, és a véleményemmel is - akár korábbi posztokra hivatkozva - kiegészíteni, így abban a hitben ringatom magam, több ez így, mint egyszerű hírfordítás: remélhetően értéktérítés. Megtalálni a "nap híré" egyébként sokszor nem is olyan egyszerű, de ebben a folyamatban is sokat tanulok belülről.



Ami elromolhat, az el is romlik. Például Mandelbrot neve az emléktáblán.

Talán annyit szoktam oldani a szigorú szakmai dolgokon, hogy igyekszem néha kicsit markánsan, viccesen is fogalmazni, valamint sokszor hozok példát Rejtő Jenő műveiből, Murphy törvényekből, Moldova vagy Dilbert okosságokból, mozifilmekből. Öveges professzor mondása jut eszembe: nincsenek nehéz vagy könnyű dolgok, csak megértettek és meg nem értettek vannak. Hiszek benne, hogy a szemléletes, közérthető, illetve humoros példák segíthetik ezt a mindenki által való megértést, és miért ne tegyem így? Szóval igyekszem rendhagyóan, és érdekesen elővezetni a dolgokat, és szerencsére ebben semmi nem korlátoz.

A sok újdonságot honnan szeded össze, mi alapján szelektálsz, hogy melyik híreket jeleníted meg?

Említettem az RSS, Twitter és Alert forrásokat. Emellett az ESET közösségből is meríthetek, ott is minden fontos esemény szóba kerül, emellett pedig járatok még tucatnyi magyar és angol hírlevelet. Kedvelem még a The Registert és az ausztrál számítástechnikai oldalakat is, érzem rajtuk, hogy nagyon tevékenyek, mindig próbálnak valamilyen aktuális problémát hatékonyan megoldani, körbejárni. Sajnos olyan törzsközönség által beküldött hírdömping, mint más blogokon, itt ugyan nincs, de blogger kollégáktól és hébehóba a visszatérő olvasóktól kapok azért tippeket. Viszont minden esetben igyekszem leellenőrizni a hír eredetét, nem szeretnék afrikai magyar törzsről, vagy az igazi Maóról hírt adni :-). Büszke vagyok rá, hogy [az állítólagosan fejbőlolt orosz spammer, Alexey Tolstokozhev álhírt is itt a blogban sikerült először leleplezni](#), míg nagy, neves magyar és külföldi oldalak készpénznek vették az egészet és változtatás nélkül leközlötték a hamis forrást, sőt sokan jelzésemre sem javítottak.



Randy Abrams-szel

Próbálok puskázni a kérdésekkel a bloginterjú oldalról, remélem nem kopirájtosak :-). Szóval vannak kedvenc témáid, amelyekről szívesen írsz?

Szeretem és érdekel ez az egész témakör, már a C64 időszak óta követem a 1541 meghajtó fejét parkoló pályára állító, a PC-s lepotyogó karakterektől kezdve a trükkös EXE tömörítőkön át a mai exploitos javascriptes shellcode-ig. A social engineering talán egy olyan kedvenc téma, ami rengeteg érdekességet tud produkálni, ez sokszor lenyűgöz. Olvastam a Kevin Mitnick könyveket, nézem a Spectrumon a Svindlernek című ismeretterjesztő sorozatot, szintén ilyesmivel foglalkozik. És ez a PEBKAC trükk láthatóan minden oprendszer alatt bejön, például videokodeknek álcázva.

Egy átlagos napon hányan látogatják meg a blogodat? Összes látogatóid száma mennyi?

Passz, amit tudok is csak azért tudom, mert valakinek a kérésére külön megnéztem, magamtól nem sűrűn szoktam. Kicsi blog vagyok, nem kerülök be a leglátogatottabb blogként a Guinness Rekordok Évkönyvébe. Körülbelül napi 3-500 az átlagos látogatószám. Ha címlap van, akkor persze ez fel tud ugrani 2-6 ezerre is. A legjobb napomon 14948, míg a blog indulása óta 600 ezer Page Impression volt a blog.hu statisztika szerint. Őszintén szólva örülök ezeknek, de nem befolyásolnak a munkámban. Ezek nélkül is tenném a dolgomat belső meggyőződésből, bízva abban, hogy hasznos és érdekes, amit csinálók. Ami miatt a címlap mégis nagyon hasznos, hogy ilyenkor számos új olvasóhoz is eljutok, és talán olyan átlag felhasználók is idetalálnak, ideszoknak egy-egy érdekesebb írás nyomán, akik különben nem keresik a technikai forrásokat egyébként.



Napi szinten hány visszajelzést kapsz e-mailban? Milyen témákban keresnek meg?

Változó, nem túl sok, havi néhány. Sok hasznos észrevételt és javaslatot kaptam már, de néha segítséget is kérnek itt, ha beüt valakinél a mennykő. Igyekszem minden ilyen esetben segíteni, mindenkinek válaszolok, ha pedig nagyon NOD32 specifikus a probléma, a supportos kollégák is készséggel besegítenek.

Kaptál már csúnya, bántó akár irigykedő kommenteket, e-mailt? Mit reagálsz rájuk?

Hát ja, volt már elvétve pár ilyen eset is, de olyan ritka, hogy nyugodtan tudok aludni tőle. Több olyan is volt, amikor igazat is tudtam adni az éles kritikának, revideáltam a nézeteimet, illetve javítottam a címet vagy a posztot. De volt, hogy méltánytalan fikázásnak éreztem, és egyszerűen túlléptem a dolgon. Úgy érzem, szerencsés vagyok, hiszen nagyon kulturált olvasóközönség látogat ide, akik értik ezt az egészet, széles ismeretük van a témában, és kellően gyanakvóak ahhoz, hogy ők maguk ne menjenek könnyen lépre az internetes támadásoknál. Nem is miattuk aggódom elsősorban, hanem azok miatt, akik nem olvassák ezt a blogot, nem olvasnak szakmai folyóiratokat, csak közben áldozatul esnek csalásoknak, adathalászatnak, kémprogramoknak. Szándékosan igyekszem távol tartani a Windows-Linux, vagy a melyik a legjobb vírusirtó típusú eldönthetetlen flamewart. Mellesleg akit érdekel, érdemes elolvasni a ["Melyik legjobb vírusirtó" című Itcafe topik bevezetőjét](#), nagyon tanulságos.



Szeretnél valamilyen változást mostanában a blogon, esetleg egy új rovatot bevezetni, vagy egy megújult design?

Általában a blogban beérem a meglévő lehetőségekkel. Mindig bőséges képanyaggal dolgozom, és emiatt az egyenkénti sziszifuszi képfeltöltögetés az agyamra megy, de elviselem, ez van. Pár havonta szoktam revíziót tartani, és néha átszervezem a dobozaimat, és kiszórom a link blogból az inaktív oldalakat. Jó dolognak látom a videoblogot is, de az én időmbe egyelőre ez egyszerűen már nem fér bele. Stílszerűen elvárnám a blog.hu-tól, hogy biztonságos HTTPS kapcsolaton keresztül lehessen belépni és dolgozni, de hihetetlen módon nincs még ilyen. Vagyis a név-jelszó adat sima szöveggént utazik a neten, ez horror szerintem.

Mely blogokat olvasod szívesen, lehet külföldi is?

Sokféle van, szakmai pedig szinte csak külföldi. Néha hagyom magam sodortatni az Index címlappal is. Rendszeresen nézem például a Buhera, Vastagbőr, OMFG, IT Security blog, Netacademia blogoldalakat és a kártékony linkeket listázó gyűjteményeket, és újabban a forensics témák is nagyon érdekelnek. Persze a szakmaiból ott vannak az egészen kiválóak: Mikko Hypponen, Graham Cluley, Dancho Danchev, Randy Abrams, Kaspersky és még számos nagy név.



Meddig szeretnéd még írni a blogodat?

Remélem, még sokáig. Téma mindig van, az emberi természet is adott, platformok meg jönnek-mennek. Jó érzés az is, hogy már az elején ott lehettem a számítástechnikának, lyukasztottam lyukkártyát, csévélttem lyukszalagot, szobányi R20, R40 gépekkel is dolgozhattam, és az első megjelenő vírusok is közelről érdekeltek már. Úgy érzem, a helyemen vagyok. Remélem, ha tizenöt év múlva újra megkérdezel, akkor azt válaszolhatom, hogy "A jó harcot megharcoltam, a pályát végigfutottam, a hitet megtartottam".

Ha újra kezdenéd, belevágnál újra a blogod írásába?

Igen, a kezdeti félelem után beleszerettem a dologba. Jó pár hónapja már a Twitterrel és Facebookkal is szétkürtölöm a posztokat, illetve egyfajta saját szemüvegemen keresztül sajtófigyelőként további magyar és angol nyelvű rövid híreket is kipostázok a követőknek. Kellemes meglepetés volt, amikor egyszer csak a Twitter követőim között feltűnt Mikko Hypponen, vagy Andreas Clementi is :-)



Blogtalálkozót szerveztél már, vagy mostanában tervezel hasonlót?

Nem, nem volt ilyen. Szerencsére vannak alkalmak, például Buhera sörözésekre már többször sikerült eljutni, de az ITBN, Hacktivity, Ethical Hacking Konferencia is hasznos, mert közben vagy utána sokakkal össze lehet futni egy sörré vagy kávéra. A világmegváltó beszélgetések közben nagy csalódások szoktak érni. Nagyon sokszor derül ki, hogy aki itt a számítástechnikában spiller, az nem egy beszélkült szakbarbár, hanem egy világra nagyon nyitott, széles látókörű, minden iránt érdeklődő polihisztor, érdekes egyéniség, akivel csomó egyéb témáról is jól lehet beszélgetni: sok ilyen kellemes csalódásom volt.



Milyen hobbid van, mivel töltöd szívesen a szabadidődöt? Milyen sportokat szeretsz, mert hogy szereted őket, az látszik rajtad.

Szeretek utazni, emellett olvasni is szeretek, családommal gyakran kirándulunk, biciklizünk, sportolunk együtt. Mióta eszemet tudom, mindig sportoltam valamit: kerékpározás, foci, futás, judo, tenisz, pingpong, gyúrás, lövészet, görkorcsolya, görhoki. Volt 15 év versenyszerű tenisz, két év versenyszerű gyorskorcsolya, és a sérülésekből éppen elég is volt ennyi. Ma már csak az egészségemért csinálom az egészet. A mai adagomat is lefutottam már :-). És elindultam párszor a helyi amatőr darts bajnokságon is, begyűjtöttem pár második meg harmadik helyezést. Apámtól azt tanultam, hogy ép testben ép lélek, és ezt én is igyekszem megvalósítani. Aktív korában ő is szorgalmasan lefutotta mindig a kilométereit, talán ez is hozzájárult ahhoz, hogy idén töltötte be a 92-t. Néha piros betűs ünnepeken a Commodore 64 emulátor is előkerül egy kis múltidézésre. Hiába, végtére is csak egy számítógépes megszállottal beszélgetsz :-)

Goldenblogra szoktál pályázni? Milyen sikerrel?

Minden évben neveztek, és örültem, hogy aztán az első szűkített merítésekbe is még bekerülhettem, már ez is egyfajta elismerést jelent, de valamirevaló érdemi babérkoszorú sosem termett ott nekem. Idén hetedik lettem, ennyi. Régen az egyik Beatrice koncerten mondta Feró, hogy mindegy mit írnak az Ifjúsági Magazinban, az év zenekara nem a Neoton Família, hanem akkor is mi vagyunk a Rice és kész. Ezzel valahogy én is így vagyok, így hát büszkén jelenthetem be, az idei évezred Diamond-überultraszuper IT blogja mi vagyunk és kész ;-)



Mire számíthatnak továbbiakban az olvasók?

Most a Counter Strike VB újbóli megnyerése után ;-). először is [gyorsan be kell fejeznem Lady Gaga legújabb klipjét](#) ;-))) Na jó, teszem dolgom továbbra is, emellett szeretnék majd hosszútávon még több időt tölteni kártevő elemzéssel, forensics-zel, kutatással, könyvírással. Majd meglátjuk, mi valósulhat meg belőle. Kedvenc alapelvem: "Nincs múlt, nincs jövő, csak a határtalan jelen, a türelmes harcok legyőzhetetlen."

Köszönöm a beszélgetést. Boldog blogszülinapot, és izgatottan várjuk a holnapi kamuprofilos eredményhirdetést. Most a végén pedig - torta helyett - kérhetsz egy zeneszámot, mi legyen az?

Egyik nagy kedvencem, a felejthetetlen Tunyogi Péter (+) énekl az Örökmozgót a régi P. Mobil bandában az 1981-es lemezen. Küldöm mindenkinek, aki szereti :-)



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](#)

- [Tízből öt kártevő hátsóajtót nyit](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2297694>

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.

Kamuprofil verseny eredményhirdetése * Friss!

2010.09.17. 20:30 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [iwiw játék](#) [xbox](#) [facebook](#) [évforduló](#) [eredményhirdetés](#) [kamuprofil](#)

Lezárult az Antivirus.blog.hu harmadik születésnapja alkalmából rendezett [Kamuprofil vadászat a facebookon és az iWiWen](#), amelyben az volt a feladat, hogy minél eredetibb módon buktassanak le a versenyzők hamis profilekat a közösségi oldalakon. Megszületett a végeredmény is.



A zsűri különdíjban részesítette Jagados Rolandot ötletes leleplezéséért, a verseny győztese pedig alapos mérlegelés után Bogdán Péter lett, aki ezzel megnyerte a fődíjat.

A jövő héten **egy külön posztban részletesebben is beszámolunk** majd a legérdekesebb pályázatokról, az alkalmazott módszerekről, a levonható tanulságokról. Minden pályázónak köszönjük az érdeklődést, és a részvételt. **Ezúton gratulálunk a nyerteseknek**, akiket a jövő hét folyamán hivatalosan is értesítünk, és felvesszük velük a kapcsolatot.

*** FRISÍTVE!**

Áadtuk a nyertesnek a főnyereményt, ami nem volt kamu, hanem egy valódi Xbox 360-at vihetett haza Bogdán Péter.



Mivel Jagados Roland sajnos nem tudott személyesen Pestre jönni, így az ő nyereményét kérésének megfelelően futárral küldtük el számára. Mindenkinek mégegyszer gratulálunk!



[Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [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/2297837>

Kommentek:

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

Cat alk 2010.09.18. 10:39:24

Ezek szerint azért van olyan, aki nem kamu, hanem valódi profillal nyomul a fészbukon? hihetlen:D
ilyet is tudnátok majd mutatni párat? :))



kündü 2010.09.18. 11:56:58

[@Cat Walk](#):

WAN!

Példul eéééén !!!!

Hacktivity 7DA

2010.09.20. 17:45 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [hacktivity konferencia kert 2010](#) [kancellár durer](#)

Túlélünk a Hacktivityt, amely új helyszínen, a Dürer kertben került megrendezésre, a beléptetésről pedig vagy jót vagy semmit. A hatalmas kiülős teraszt viszont nagyon díjztuk, és magának az épületnek is volt egy az eseményhez jól passzoló, Fonós időket idéző feelingje.



Az időjárás - különösen az első nap reggelén az utcán sorban állókat tette próbára, ahol jó szokás szerint ;-) az Apu hogy megy be az a nagy elefánt az oroszán barlangjába időre és előadás kezdésre című játék okozott némi nemű torlódást és fennakadást. A zsúfolásig megtelt nagyteremben az első előadást Bruce Schneier tartotta, illetve egész pontosan beszélgetett a közönséggel, és a kérdéseikre felelt.



Szerinte a felhasználók hozzáállásán van még mit fejleszteni, és a magyarul is megjelent "Schneier a biztonságról" című könyvét kézbe véve viccesen megjegyezte, ez a kép róla nem is ismerős neki, és hogy **nem muszáj ám megvenni, angolul le is lehet tölteni a netről ;-)** De ha valaki mégis megvenné, annak délután szívesen dedikálja a kötetet. A könyves standokon 30%-os alkalmi kedvezménnyel lehetett ezt is, de más könyveket isvásárolni, volt például a Hogyan lopjunk kontinenst című kötetből is bőven az asztalokon.

Szemes Balázs a nemzetközi szerzői jogvédelemmel kapcsolatos jelenlegi és várható történéseket vázolta fel a HADOPI és az ACTA kapcsán.



Sokaknak biztosan beugrott erről a ["Csigát eszik, filmet tölt le, börtönbe megy, ki az?"](#) című remek írás.

Páncsél Zoli és Spala Feri buffer overflow workshopjára annyian voltak kíváncsiak, hogy a terem zsúfolásig megtelt, bejutni szinte képtelenség volt. Talán ez volt a másik említendő szűk keresztmetszet, hogy a kis, vagyis Mitnick teremben néha kétszer annyian szerettem volna bejutni, mint lehetséges.



A kint rekedtek még választhatták az előtérből nyíló fotelbárt is, ahol nagy kijelzős plazmatévéen is figyelemmel lehetett követni az eseményeket. Illetve emellett az IT Cafe is volt olyan kedves, hogy a tavalyihoz hasonlóan streamelte élőben a weboldalán az előadásokat.

Az udvaron Mitch Altmann hardver workshopján vehettek részt az érdeklődők, ismerkedhettek a forrasztás rejtelmeivel. Mitch a [magyar Hacker Space meghívására](#) érkezett Budapestre, és maga is társalapítója egy San Francisco-i független tudásközpontnak.





A Brain Machine első látásra a Relaxomat szemüvegre hasonlító cucc, de még számtalan más buherált eszközt is meg lehetett csodálni.

Kabai Andris folytatta ezek után a **buffer overflow** bemutatót.



ROP (Return Oriented Programming) exploit elkészítésével demonstrálta az ASLR (Address Space Layout Randomization) és DEP (Data Execution Prevention) megkerülési technikákat.

Ezután Buherátor következett egy Metasploit Workshoppal, amelyben saját Metasploit modul megírását mutatta be lépésről lépésre.



Ennél az előadásnál is kicsinek bizonyult a terem az érdeklődők számához képest.

Utolsóként - legalább is az általunk látogatott előadások sorában - **Neumann Róbert beszélt az exe tömörítőkről**, milyen tulajdonságaik vannak, hogyan lehet őket csoportosítani, valamint hogy a malware fejlesztők is mennyire előszeretettel használják ezeket.



A sok fajta program, és változat közül úgy vélte, a legális és kártevő célokra egyaránt használt tömörítők okozzák a legnagyobb fejtörést, ugyanis pusztán az exepacker kódjának felismerése még nem dönti el azt, kártékony vagy ártalmatlan állományt konvertáltak vele.



ESET terrárium, gépek védelemel és anélkül ;-)



A hivatalos program végeztével **az udvaron folytatódott az élet**, amelyet az előadók által feltett kvízkérdések, **sör, rakott krumpli sőt**

ráadásként egy **kis lockpicking workshop** is színesített, ezen még női résztvevő is volt, igaz nézői minőségben. A záraz és lakatok kulcs nélküli nyitogatásának aztán csak a csepergő eső vetett véget.



Kis szocreál panoptikum, fekete-fehér Tavaszi tévével, borosüvegekkel...

Itt vérmérséklet és életkor függvényében alkoholos befolyásoltságú italok fogyasztása, és némi nemű alvás időszak következett, majd ráánk virradt a második nap. A belépés itt már olajozottan működött, és ezúttal már minden előadás csúszás nélkül, pontosan tudott indulni.



Csókolom, itt tessék aláírni ;-)

Hornák Zoltán indította az új napot a set-top boxok biztonságáról, és öröm volt látni, hogy mennyire igaz a régi mondás, amit a katonaságnál belénk neveltek: nincs lehetetlenség, csak tehetetlenség.



A lenti kép egy olyan box teszteléséről készült, amelynél titkosítás, induláskori egyedi ID ellenőrzés és az alkatrészek lábaihoz való fizikai hozzáférést gátló ragasztó is igyekezett megnehezíteni a kíváncsi kutatók dolgát - ugye mondani sem kell, hogy végül a józan ész diadalmas zárult a menet.

Fóti Marcell előadásának bár az volt a címe, hogy "Nincs új a nap alatt", azért mégis tudott újat mutatni.



Egyszerű, látszólag fapados eszközökkel (netcat, elitewrap) adott elő mikromágiát, amelynek jutalma a művelet végén domain admin jogosultság eredményes megszerzése volt.

Farmosi István múltidéző előadása a régi, DOS-os idők vírusait elevenítette fel, milyen problémákkal és technikai nehézségekkel kellett megküzdeniük vírusvédelmi termékeik fejlesztésénél.



Aki még emlékezett a potyogós, péntek13 és egyéb régi vírusokra, esetleg a PrgDoki című programra, vagy a SAFE Kft hardveres vírusvédelmi kártyájára, az most jókat nosztalgiaázhatott.

FX előadása a Cisco routerek kihasználásáról, biztonságáról szólt, és kétségkívül a leglazább volt az egész rendezvényen.



Jó hangulatú, hogy úgy mondjuk laza nyelvezetű volt ;-), de klassz. Nem sok tűt lehetett leejteni a teremben.

Major Marcell saját jelszótörő alkalmazás fejlesztéséről beszélt, illetve szóba került a grafikus kártyával elérhető nagyobb hatékonyság is.



Az általa GeForce kártyára fejlesztett alkalmazás képes több jelszót törni párhuzamosan, valamint a folyamat leállítása után a félbeszakítás előtti pontról folytatódhat a munka.

Tevesz Andris ismét rootkites témát választott, ezúttal a rootkit felismerést ígérő antivírus csomagokat tesztelte saját fejlesztésű programjával, és többek közt azt is vizsgálta, hogy az egyes vírusvédelmi, illetve komplett internet biztonsági csomagok mennyire tudják a gyakorlatban megvalósítani az önvédelmet, saját moduljaik, fájljaik, processzeik, hookjaik törlését vagy módosítását.



Az előadásból és tesztekéből az derült ki, hogy ezt a feladatot szinte egyetlen antivírus termék sem végzi el megfelelően, hibátlanul pedig egyik sem.

Robert Lipovski az ESET víruslaborjából érkezett, és szintén rootkites témával foglalkozott.



IAT és SSDT hookok és egyéb trükkökkel élő mai kártevők bemutatása került terítékre, köztük a Mebroot, Rustock és Olmarik.

A zárás előtti **utolsó előadás Tomcsányi Domonkos Pál** nevéhez fűződött. A legfiatalabb előadó érdekes témát választott, lehet-e érdemes-e régi okostelefonra, PDA-ra Linux telepítéssel hackereszközöket telepíteni.



Agyzsibbasztó ár, átszámítva 800 ezer HUF! Akkor inkább buheráljunk!

Amelyek ugyan egyelőre jelentősen lassabban működnek, mint egy valódi PC, de ennek ellenére működésre lehet őket bírni egy kabátzsebből indított WEP törésre, és hasonlókra.

Megint többször is volt olyan érdekes párhuzamos előadás egy időben, amikre szívesen elment volna az ember, de Révész Sanyival szólva **sajnos nem lehattunk egyszerre két helyén**. A teljesség igénye nélkül Kovács Zsombor, Veres-Szentkirályi Andris, Dr. Ormós Zoli, Illési Zsolt, Dr. Dudás Ági vagy éppen Alexander Kornbust sajnos ezúttal nekünk kimaradt. De szerencsére fájdalmas hiányukat **azért jól be lehetett pótolni velük egy-egy kötetlen beszélgetés formájában a büféudvaron pohár redbull/kávé/sör italokkal a kézben**.



to antivirus.blog.hu

A szinkron tolmácsok az angol előadásokat magyarra, a magyarokat pedig angolra fordították, így az ide látogató számos külföldi, például szlovák, koreai látogatók is végig élvezhették a szakmai rendezvényt. [A helyszínen dolgozó rendezők mindent megtettek](#), hogy a jelenlévők problémáit segítsenek megoldani, nekik ezúton köszönjük meg lelkes munkájukat.



Ha lett volna szárazpoló verseny, nálunk Tamásé lett volna az aranyérem :-)

Aki pedig a fentiek fényében esetleg kedvet kapott ahhoz, hogy a következő Hacktivityt már ne hagyja ki, az máris karistolhatja be az emlékeztetőt **a naptárába a 2011 évi teendőihez**.



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



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2309786>

Kommentek:

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

[John:Smith 2010.09.20. 18:35:00](#)

Hát az első napi bejutás az tényleg katasztrófa volt. És a hely. Feeling az volt. No de bejutni néhány előadásra... Lássuk be, jövőre nagyobb helyet kell választani!



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.09.21. 10:06:21](#)

Egy csokos további adalék, beszámoló, interjú, wahetever:

Biztonságportál:

biztonsagportal.hu/hackivity-2010.html

IT Cafe:

itcafe.hu/hir/interju_bruce_schneier_hackivity_2010_budapest.html

Caracalla:

caracallablog.blog.hu/2010/09/20/hackivity_2015

Index:

index.hu/tech/2010/09/21/az_internet_az_uj_rock_and_roll/

Kamuprofilok több ezer ismerőssel

2010.09.22. 13:15 | [Csizmazia István \[Rambo\]](#) | 17 komment

Címkék: [iwiw játék](#) [xbox facebook](#) [évforduló](#) [eredményhirdetés](#) [kamuprofil](#)

Lezárult az [Antivírus blog kamuprofil vadászata](#). A versenyzők tucatnyi hamis iWiW és Facebook adatlapot buktattak le. **Akad közöttük olyan, melyet több mint 36 ezren jelöltek vissza, ismert hivatalban lévő politikusokat és közéleti személyiségeket is beleértve.**



Egy hónappal ezelőtt az Antivírus blog harmadik születésnapja alkalmából kamuprofil vadászatot hirdettünk. A versenyre tucatnyi pályázat érkezett. Tulajdonképpen elmondható, hogy **aki nagyon akart, könnyen tudott hamis profilt találni**. Még ha a verseny szellemében nem is tudta eldönteni, melyik az igazi, akkor is látta a területen uralkodó káoszt. [A nyertes egy olyan kamuprofil leplezett le](#), melynek 36 322 ismerőse van az iWiW-en, közöttük számos politikussal és közéleti személyiséggel. **A csinos női fotók mögött azonban nem egy valódi személy áll**, hanem egy belvárosi sztriptíz klub jól megtervezett marketingakciójának profiloldala, mely a rég letűnt S Club 7 tiniegyüttes énekeseinek, Rachel Stevensnek fotóit használja fel a rajongók gyűjtésére.



Bármilyen hasonlóság a valósággal nem csak a véletlen műve

A hamis adatlapokat gyakran több ezer rajongó jelöli be, akik elhiszik, amit a kamuprofilok tulajdonosai mondanak nekik. Ez biztonsági problémát jelent, hiszen a hamis profil tulajdonosa így hozzáfér a rajongó adatlapján szereplő információkhoz. Ezenkívül [a kamuprofil létrehozó személy különböző akciókra is ráveheti a rajongókat](#): más oldalakat ajánl a figyelmükbe, vagy akár pénzt gyűjthet tőlük.



Gyűjtögető életmód: strigulabajnokság rulez ;-)

A kamuprofil vadászat versenyzői a hamis profilok azonosítására kizárólag legális módszereket alkalmazhattak. **Ezek közül az egyik legnépszerűbb a TinEye webes szolgáltatás használata volt**, melynek segítségével egy adott fénykép további internetes előfordulásait lehet ellenőrizni, a nyertes is ezt a módszert alkalmazta. Több versenyző próbálta meg **ellenőrizni az egyes profilokhoz tartozó kapcsolati hálót is, a sztárok menedzsere és családtagjai** ugyanis csak a valódi profil mögött lévő személyt szokták visszaigazolni. Olyan is akadt, aki kamuprofil adatlapon megadott **iskolához tartozó öregdiák-keresőben ellenőrizte, hogy valóban járt-e az iskolába adott nevű személy**, és így derítette ki, hogy legalább részben hamis adatokat adott meg valaki. Jól látszott a kamu adatlapoknál, hogy **nem csak képeket másoltak, hanem az eredeti személy személyes adatait is nagy bátran át kopi-pésztették az elkövetők, klónozták**. Ez ellen igazából sokat nem lehet tenni, az üzemeltetők felé jelentheti az eredeti profil tulajdonosa.



Abszolút hiteles adatok :-)

A versenyen **technikai-különdíjas lett egy leleplezés, mely Andy Whitfield színészhez, a Spartacus: Blood and Sand sztárjához kapcsolódik**. Egy 19 éves rajongó hamis Facebook profilt készített, és a népszerű színésznek adta ki magát, így több ezer rajongót gyűjtött.

Egy magyar felhasználónak azonban gyanús lett a profil, és **törbe csalta a hamisítót: egy olyan weboldal linkjét küldte el neki, mely regisztrálja, hogy milyen IP címekről keresik fel.** A csaló rákattintott a linkre, és így egyértelműen bebizonyosodott, hogy nem lehet Andy Whitfield-el azonos, a színész ugyanis Ausztráliában, illetve Új-Zélandon dolgozik, míg a csaló IP címe gibraltári volt. A csaló aztán nyilvánosan bocsánatot kért, és oldalát átalakította rajongói oldallá.



A verseny eredményei kapcsán érdemes figyelni arra, hogy a közösségi oldalakon is vigyáznunk kell a személyes adatainkra, és csak a **valódi, ellenőrizhető ismerősöket érdemes visszajelölni.** A közösségi oldalak pedig jól tennék, ha a rajongói oldalak számát is ellenőriznék, mint ahogy egy technikai fórumon is átteszik a szoftver kérdést a hardver szekcióból, ha véletlenül oda érkeznek, vagy ha új topikot nyitnak már létező témában, akkor áthelyezik azt a jó topikba új hozzászólásként. Nem normális dolog, hogy egy létező híresség nevében akár több tucat különböző rajongói klub is létezzen azonos névvel, megnehezítve egy átlagember számára a hiteles választást.



Kavarják ezek vagy nem kavarják?

Ha esetleg mégis rajongói csoporthoz akarunk csatlakozni, **az a legszerencsésebb, ha a hírességnek olyan a weboldala, amely tartalmazza a hiteles linket a közösségi oldal autentikus profiljához: ekkor biztosan a jó helyre jutunk.** Ez szerintünk a rajongóknak is **jó fogodzó lehet a jövőre nézve,** a zenészeknek, hírességeknek pedig **megfelelő módszer, amivel segítik helyesen kiválasztani a közösségi oldalakon található saját profilt, és megóvják a gyanútlan rajongókat a csalóktól.** **Mindenféle csatlakozás előtt érdemes áttekinteni, és ha kell módosítani a saját biztonsági beállításainkat,** hogy csak azok a személyes adataink kerüljenek megosztásra, amelyeket valóban szeretnénk láthatóvá tenni.



A versennyel a közösségi oldalak biztonsági kérdéseire kívántuk felhívni a figyelmet, lássa mindenki, hogy a személyes adatunk érték, bánjuk velük hát ennek megfelelően, vagyis óvatosan.

 Tetszik  83 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2314299>

Kommentek:

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

Hozzá Szóló 2010.09.22. 16:35:41

☐Nem normális dolog, hogy egy létező híresség nevében akár több tucat különböző rajongói klub is létezzen azonos névvel, megnevezve egy átlagember számára a hiteles választást"

Na kérem, erre külön minisztériumot kellene létrehozni :D
Ezek ám a fontos dolgok...



Rhythmeen 2010.09.22. 16:40:07

LOL végkövetkeztetések vannak ebben a posztban, mintha csak Meki bácsit hallanám: "A drog rossz. Ne drogozz! Értem? AZ alkohol is rossz. Ne igyál alkoholt. Értem?"

garage 2010.09.22. 16:41:35

Éder Krisztián kicsoda?

BushDoctor 2010.09.22. 17:09:40

garage : egy nulla, ne is foglalkozz vele !

BÁNYAI 2010.09.22. 17:15:39

Éder? Nem ő az a hekker, akit a volt miniszter megbízott, hogy y a saját Nemzetbiztonsági Hivatalába törjön be?



sebien 2010.09.22. 18:00:55

ebben mi a leleplezés, hogy kitakarod a leleplezett kamuprofilon a nevet?



sebien 2010.09.22. 18:05:43

@garage: enyhe túlzással olyan nekünk sp (éder krisztián), mint a külföldnek jb (justin bieber): mindenki utálja. de senki sem ismeri...

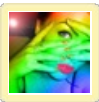
ramika14 2010.09.22. 18:43:18

@garage: Nem ő az itten a Chios-reklámban? www.youtube.com/watch?v=aWcXzQ_R6NY



radiris 2010.09.22. 21:11:35

@Jencike12: nem mennél te a jó édesanyád spammelő bús nagyjakai közé?



Myta • <http://www.stylebyme.blog.hu> 2010.09.22. 21:24:53

Én minap Csonka Bandi-t jelöltem meg. Nyugtassatok meg, hogy az ő fóka képe nem csak illusztráció!

teddyde • <http://ezmegigyhogytumblr.com/> 2010.09.22. 23:31:56

@Myta: Csonka Bandi nem fake, csak mindenkit visszajelöl, válogatás nélkül. Érdekes tanulmány az adatlapja.



szbszig 2010.09.23. 00:46:08

Ki az az Éder Krisztián?...

Akitlosz • <http://honunk.blog.hu/> 2010.09.23. 06:02:08



Ez a "közösségi oldal", legalábbis a példában szereplő rég nem arról szól, hogy hús-vér emberek kapcsolatot tartsanak ott hús-vér valódi ismerőseikkel.

Ebből kifolyólag mi is a gond a kamu profilokkal?

A rajongókat talán ismerik a hírességek? Ugyan.

A klubozás egyszerű marketing tevékenység.

Ráadásul mindenféle trükköket bevet ez az oldal, hogy szaporítsa az adatlapokat.

Például primitív játékok működnek rajta, amelyekkel csak és kizárólag akkor lehet normálisan játszani, ha a játékos begyűjt egy halom "szomszédot".

Ha nem akarja a valódi ismerőseit ilyen bugyuta játékkal nyaggatni vagy azok nem állnak kötélnek, akkor vagy mindenféle vadidegennel "ismerkedik össze" - akik jó része ugye kamuprofil - vagy maga hoz létre pár új profilt "szomszédnak".

Ennek a fészbuk projektnek már nem sok köze van pl. régi osztálytársak összegyűjtögetéséhez, szóval kár a cikkírónak ennyire felháborodni.

Ha csak a való világból ismert valódi ismerőseivel akarja tartani a kapcsolatot, akkor nem valószínű, hogy átverik, legfeljebb tévedésből jelöl be hasonló nevűt, tulajdonságait.

Ha meg a "rajongói klubok" érdeklik, akkor meg is érdemli.

Azt kellene felfogni, hogy egy ilyen "közösségi oldalt" tömérdek ember használ tömérdekféle célra, és a céljuk nem az, hogy a cikkíró kedvének, ízlésének eleget tegyenek.

A következő cikk szólhatna Budapesten a piroson átsétáló gyalogosok szenzációs leleplezéséről.

Milyen emberek vannak!

Döbbenet!



**Csizmazia István [Rambo] <http://antivirus.blog.hu>
2010.10.04. 18:13:49**

Nyilvánvalóan nem ez az emberi élet legnagyobb problematikája és annak csimborasszója. De egy a sok közül, és kapcsolódott a játékunkhoz is. Valószínűleg te is másként látnád, ha a gyereklányod tudtán kívül nem az aktuális sztárnak, hanem egy piti csaló rajongója lenne Facebookon.

Nemrég egyébként a saját szememmel láttam egy olyan embert, aki már látott olyan embert, aki látott egy piroson átsétáló gyalogost is ;-) Szóval ez megvolt, ki is húztam a listámról.



Akitlosz • <http://honunk.blog.hu/> 2010.10.04. 19:51:07

"Valószínűleg te is másként látnád, ha a gyereklányod tudtán kívül nem az aktuális sztárnak, hanem egy piti csaló rajongója lenne Facebookon."

Gyereklány nem fészbukolhat. 13 év az alsó korhatár.

Ennyit a "piti csaló" témáról.

[Hozzá Szóló](#) 2010.11.02. 15:15:31

@Akitlosz: Miféleképpen a 13 éves gyerek is gyerek, nem tudom, felétek ez hogy megy.

De akinek agya van, az saját magát meg a 18, különösen a 14 évet be nem töltött családtagjait a lehető legtávolabb tartja ettől az örülettől. Ugye nem kell magyarázni még, hogy miért? Remélem...



Akitlosz • <http://honunk.blog.hu/> 2010.11.03. 07:22:20

@Hozzá Szóló: Nálunk fiatalok.

Már nem gyerek, de még nem is felnőtt.

Kamasz, bakfis.

Ezek az oldalak már rég nem közösségi kapcsolattartásról szólnak, leírtam a korábbi hozzászólásomban.

Cenzúrázzák az SMS üzeneteket

2010.09.24. 14:40 | [Csizmazia István \[Rambol\]](#) | [48 komment](#)

Címkék: [amerika](#) [fcc](#) [cenzúra](#) [sms](#) [text](#) [jóváhagyás](#) [t](#) [moblie](#) [eztext](#)

A T-Mobile elismerte, hogy **cenzúrázza a forgalmazott szöveges üzeneteket a hálózatában**. Az ügyben egy marketinggel foglalkozó EZ Text [cég indított keresetet](#) a New Yorki szövetségi bíróságon.



Mint kiderült, mindenféle **külön értesítés, jelzés nélkül törölhetnek** a szöveges üzenetek közül, amiről a küldő fél sokszor egyáltalán nem is szerez tudomást. Sőt, **indoklás és fellebbezés sincs**. Az amerikai T-Mobile úgy véli, **szükséges ez az előzetes jóváhagyási procedúra, mert ezzel kívánják megvédeni ügyfeleiket** a jogellenes, megtévesztő vagy sértő marketing üzenetektől.



Volt már hasonló eset **2007-ben, akkor végül per nélkül zárult a Verizon abortusszal kapcsolatos üzenetek továbbításának megtagadása** miatt kirobbant botrány. Létezik ugyanis [egy olyan FCC \(Szövetségi Kommunikációs Bizottság\) szabályozás](#), amely a vezetékes szolgáltatókkal szemben a vezeték nélkülieknek ad lehetőséget arra, hogy megválogathassák a forgalmazott tartalmakat. Azonban ezt a más elbánást [hálózati semlegességre hivatkozva](#) az előbbiek támadják, és emiatt három éve már petíciót is nyújtottak be. Minden esetre az ügy végkimenetele amiatt is **érdekes lehet, mert ez az első olyan eset, amikor vezeték nélküli szolgáltatót fogtak perbe szöveges üzenetek cenzúrázása miatt**.



Érdekes gondolat kísérlet, ha mondjuk az internetszolgáltató is hasonlóképpen **tudtunk, beleegyezésünk, és jóváhagyásunk nélkül elolvassa helyettünk**, előttünk ilyen indokkal az e-mailjeinket, természetesen szigorúan "csak a mi érdekünkben", nehogy a végén még nem megfelelő üzeneteket kapjunk kézhez ;-) **Sokan egyetértettek, még többen vitatták korábban azt is, jó módszer lenne-e az, ha az internet szolgáltató kitiltaná a vírusfertőzött számítógépeket**, amihez valamilyen szinten [bele kellene néznie](#) a forgalmunkba, ez pedig sérti a felhasználók jogait, meg igazából egy ilyen jellegű szűrés elvégzése nem is feladatuk.

Tetszik 121 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

• [1 trackback](#)

Ajánlott bejegyzések:

- [Majdnem mindenki átverhető adathalászzal](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [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/2319883>

Trackbackek, pingbackek:

[Trackback: A Google, a semleges net és a válasz](#) 2010.09.24. 18:11:24

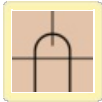
Az elmúlt hetekben - nem kis port kavarva - olyan híresztelés kapott szárnyra, miszerint az informatikai óriáscég, a Google megegyezett egy vezető internetszolgáltatóval és távközlési céggel, jelesül a Verizonnal, hogy bizonyos szolgáltatásait gyorsító...

Kommentek:

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

[BruceTheHoon 2010.09.24. 18:09:38](#)

A címlap épp hitelrontást követ el: ez itt a T-Mobile *USA*, miközben a nem minősített T-Mobile-ról mindenki a magyarra gondol. Ebben bűnrészes vagy, mert te sem írod ki sehol, bele kell kattintatni a cikkbe, vagy nagyon csodálkozni, hogy miért a New York-i bíróságon döntenek ilyesmiről.



[ergerberger 2010.09.24. 18:25:55](#)

[@BruceTheHoon](#): Olvasni bizony tudni kell. Ha te nem tudsz, fellebbezzél anyádhoz, amiért nem verte el a seggedet, hogy tanulás helyett a pöcsöddel játszottál.

[kvadrillio 2010.09.24. 18:33:13](#)

Mi van hozzászólók !
Most olvassátok egymást ??? :O))))))

[mqqq 2010.09.24. 18:41:04](#)

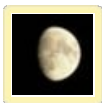
Márpedig ez így tényleg kibaszott félrevezető.

[SÜN 2010.09.24. 19:00:16](#)

a zsindexen mi nem az?

[SÜN 2010.09.24. 19:00:48](#)

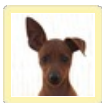
eleve nincs, nem letezik 1 olyan cikk sem amiben nem lenne legalabb 3 helyesírási hiba



[movhu 2010.09.24. 19:08:54](#)

Azért gondoljunk bele a másik oldalba is.
Ha ma az internet szolgáltató nem szűrné a bejövő leveleket, akkor az ügyfél 10* annyi levelet kapna legalább, mint most. Volt már olyan, hogy kis cégnél a levelező szerveren néhány napig nem ment a spamszűrő, és az ügyfelek nem győztek az ügyfélszolgálatra telefonálni.
Az sms spam csak azért nem terjed annyira, mert pénzbe kerül, de ettől még idegesítő lehet.

(Zárójelben jegyzem meg, hogy a h*lye Vodafone miatt rendszeresen problémás a netbankos bejelentkezésem, mert az a szokásuk, hogy mikor amúgy is sms-t kapnék, előtte a rendes sms helyett a saját spamjüket küldik, és majd csak percek múlva a netbankos bejelentkező kódszót. Ez most megoldódik, mert átmegyek a C*t*bankhoz, és ott nincs sms a bejelentkezéshez :))



[Jaffar 2010.09.24. 19:19:52](#)

[@movhu](#):
Létezik olyan, hogy C*t*bank?
Nem Citybank véletlenül?
Ne legyünk már ilyenek. Nevezzük nevén a dolgokat.

A poszt címe valóban félrevezető :(

Az meg elég nevetséges, hogy egy 3.-ik személy dönti el, hogy mi való nekem és mi nem. Márpedig itt erről van szó.

- Rendi - 2010.09.24. 19:27:27

[@Jaffar](#): Citibank :]



sonance • <http://www.sonance.hu> 2010.09.24. 19:28:12

[@Jaffar](#): Citibank hogy pontosítsak :)



Kozmokrator • <http://www.tudtad.com> 2010.09.24. 19:37:21

Ejj-ejj. BULVÁROSODUNK?



ave 2010.09.24. 19:37:44

Egy antivirus blog ilyen trehany posztot nem írhatna szerintem.
KURVARA oda kell írni, hogy az amerikai t-vel van a gond.
Majd ha a magyarral is lesz, akkor lehet így írni.



Almaspite 2010.09.24. 19:38:41

Tíz évvel ezelőtt is volt már SMS-szűrés, ráadásul kis hazánkban is. Pld. egy rendezvényen a nagy, projektoros üzenőfalra csak cenzúrázott szavak mehettek ki. Nem egy nagy kaland, a karakterláncban megkeresi a tiltott szavakat és kicsillagozza.

A védekezés ellene: szándékosan rosszul kell írni azokat a szavakat, amik valószínűleg fennakadnának a szűrőn.

"Bhazd meg a khurva nénikéd..." Minden ember érteni fogja, de a szűrő nem fogja felismerni. Egyfajta CAPTCHA-ként is felfogható...



movhu 2010.09.24. 19:40:15

Citibank Citibank Citibank

:)

d.z. • <http://masikmagyarország.blog.hu> 2010.09.24. 19:48:18

[@ergerberger](#): Pedig igaza van.

adamekp • <http://adamekp.blog.hu> 2010.09.24. 19:57:55

Ha Chicagóban a MÁVot perelik (?), még simán lehet new yorki bíróságon a magyar T is, nem?



Luxa • <http://blog.luxa.hu> 2010.09.24. 20:15:23

[@Almaspite](#): Lehet, de itt nem a szolgáltató szűrt, hanem az a gép, ami a kapott sms-eket kirakta a kivetítőre.

- Rendi - 2010.09.24. 20:16:41

[@Almaspite](#): Az üzenőfal más térsza, ott akár a "fogadó" fél is ráengedheti a cenzúrázó szoftvert.

szita szita péntek 2010.09.24. 20:21:41

@Almaspité: Már bocs, de a cikk nem arról szól, hogy a trágárkodást szűrjük... Vélhetően a marketing sms-eket kapkodják ki, ha másért nem, hát azért, hogy hasonló szolgáltatást csak az ő érdekelttségükbe tartozó cégnél lehessen megvenni. Kicsit olyan ez, mintha a posta nem vinné ki neked a levelet, mert abban egy futárcég reklámja van. Ez még vélhetően tetszene is a felhasználók többségének (hisz nem kell annyi kéretlen reklámot olvasgatni) viszont a gond ott van, hogy ez csak úgy tehető meg, ha egy bot olvasgatja az sms-eimet. Ez meg már a levéltitok védelme kategória. Én pld. nem veszem szívesen, ha az én érdekeimre hivatkozva belepiskálnak a privát szférámba. No? Átért?



after80 • <http://sasfeszek.blog.hu> 2010.09.24. 20:28:17

Ez nem éri! Mi közük az sms-ek tartalmához!?

[megmondoember] 2010.09.24. 20:38:57

Ez a cikk szakmailag nulla. Nem csak azért, mert nem említi már a címben, hogy az amerikai T-Mobile-ról van szó (így relevanciája számunkra nagyjából nulla), de mert az angol "censors" szót teljesen tévesen "cenzúráz"-nak fordítja, mikor itt és ebben az összefüggésben "vizsgál"-t, "szűr"-t jelent. Ráadásul meg sem említi azt a történetek helyes értelmezéséhez elengedhetetlen tény, hogy Amerikában nem (csak) a küldő, hanem a fogadó fél (is) fizet az SMS-ekért, aminek tükrében máris más felhangot kap az, hogy egy szolgáltató előzékenyen kiszűri a minden valószínűség szerint kértetlen üzeneteket (pedig anyagi érdeke inkább ahhoz kötődne, hogy minden szutykot továbbítson, hiszen annál többet kaszálhatna a címzettől is).

Szóval gratulálok a Nod32-nek, de ha az antivírusuk is olyan dilettáns és tájékozatlan emberek munkája, mint a posztoló, akkor jobb ha mindenki messze nagyívben elkerüli!

[megmondoember] 2010.09.24. 20:42:59

@szita szita péntek: "Ez még vélhetően tetszene is a felhasználók többségének (hisz nem kell annyi kéretlen reklámot olvasgatni) viszont a gond ott van, hogy ez csak úgy tehető meg, ha egy bot olvasgatja az sms-eimet. Ez meg már a levéltitok védelme kategória. Én pld. nem veszem szívesen, ha az én érdekeimre hivatkozva belepiskálnak a privát szférámba. " És mit gondolsz a spamszűrők, amelyekből valószínűleg több is védi az email-es postafiókjaidat, hogyan működnek? Technikai értelemben azok is "beleolvasnak" a leveleidbe, és megvizsgálják a tartalmukat, hiszen (részben) ez alapján tudják eldönteni, hogy spam -e vagy sem. Mégsem félsz gondolom, hogy belelátnak ennek révén a magánszférádba.

Na, az SMS-ek szűrése is valami hasonló, teljesen gépi módszeren alapulhat, ami semmivel sem jelent nagyobb veszélyt, mint az email-spam szűrése. Viszont a fent említettek miatt (ti. hogy Amerikában az SMS fogadásáért is fizetni kell) komoly pénzt is meg tud megszórolni a bosszúság mellett.

esmein 2010.09.24. 21:05:57

megmondoember: egy idegesítő pocs vagy. Gyere legközelebb is, de csak akkor ha fele ennyi értéket már létrehozta mint eddig.

Idiota trolllok...

szita szita péntek 2010.09.24. 21:16:53

@[megmondoember]: "És mit gondolsz a spamszűrők, amelyekből valószínűleg több is védi az email-es postafiókjaidat, hogyan működnek?" - Nem használok spam szűrőt. Nyilván akkor is véd néhány, ha nem akarom - ezért nem is használok az e-mailt gyakorlatilag semmire. Aki akar velem beszélni, az keressen meg! ;)

szita szita péntek 2010.09.24. 21:20:29

@[megmondoember]: Annyit még azért hozzátennék, hogy semmi gond nem lenne az ilyen szolgáltatásokkal, ha azokat a felhasználó kérésére lehetne aktiválni, illetve a felhasználó tudna a létükről. Amíg ez nem így van, addig az én fene liberális szememet csípi.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.09.24. 21:30:16

Benne van hogy amerikai T-Mobile, meg hogy New Yorki bíróság.



Szerintem az az érdekes elvi kérdés, van-e joga _szólás_nélkül_ szűrni a szolgáltatónak? Mert ha szól, hogy sorry, ezért meg ezért nem mehet, az azért egész más. Ám ha csendben kummant, te pedig azt hiszed, sikeresen elküldted, az szerintem baj.

Itt van például a vírusirtók esetében a kaszínó, amelyik van akit idegesít, mint kéréstlen reklám, van aki pedig szenvedélyes játékos, és kifejezetten örül minden ilyen új hírek, reklámnak, lehetőségnek, ablaknak. Ehhez van külön korrektül kapcsolódó: "Kéréstlen alkalmazások keresése" és a "Reklámprogramokat, kémprogramokat és biztonsági kockázatokat jelentő programok keresése". Erről így _te_rendelkezel_, magyarul becsekkolod őket vagy sem, és nem rendelkezik senki nélküled, helyetted, tudtodon kívül. Ez itt szerintem a főlényeg.



Kicsit Karcos 2010.09.24. 22:10:00

@[megmondoember]: pedig helytáll szó a cenzúrázás erre. Azt pedig ne gondold, hogy attól, hogy gép végzi a szűrést (nyilván), attól még egy ember sem olvas bele a leveleidbe. Hogyan teszteljük a szolgáltatást, ha nem próbálhatják ki? Nemrég pl. a guglinál volt ebből visszaélés, ki is rúgtak érte valakit. Tudomásul kell venni, hogy a levéltitok az olyan, mint az adótitok, a szolgáltató jól dokumentált, kiválasztott, felkészített emberén és az érintette(ke)n és persze az ÁVH-n kívül senki másnak semmi köze hozzá.

@Csizmazia István [Rambo]:

"Ám ha csendben kummant, te pedig azt hiszed, sikeresen elküldted, az szerintem baj."

Elkummantják a kézbesítési jelentést is? Nyilván, ha egyszer nem kézbesítik az üzenetet:)

Diktatúra Pécssett, új céget foglalt el a Fidesz! 2010.09.24. 22:20:30

Az eredetinel tervezetthez képest 26 millió forinttal több megbízási díjért, 96 millióért vállalta Hódmezővásárhely városmarketingjének menedzselését a Prestige Média Kft. A társaság tulajdonosa az a Várhegyi Attila, aki egykoron a Fidesz pártigazgatója volt és korrupciós ügye miatt volt kénytelen távozni a politikai életből.

Újabb öt évig Várhegyi Attila egykori fideszes pártigazgató cége, a Prestige Média Kft. felel Hódmezővásárhely városmarketingjéért, derül ki a Közbeszerzési Értesítő szeptember elejei számából. A cég egyedüli ajánlattevőként nyerte el a megbízást. A hírről beszámoló Kreatív arra is emlékeztetett, hogy a cég második alkalommal nyeri el ezt a megbízást. Először 2008-ban bízták meg őket ezzel a feladattal, akkor két évre 28,8 millióért vállalták a munkát, 1,8 millióval többért, mint amennyit a város eredetileg szánt a munkára.

Ppix 2010.09.24. 22:39:27

Eccerű, a sunyi Index szerkesztők direkt nem írják ki, hogy USA T-Mobile, különben ki nem szarná le ezt az unalmas post-ot. Semmi különös, csak a szokásos manipuláció.

A blog hasonló színvonaló szerzője meg aszisztál hozzá, a félrevezető első mondattal.

Ezen én nem lepődnék meg, az egész webes nézettségi biznisz a hazugságra épül.

A csótány is ember 2010.09.24. 23:16:31

Ja hogy usa? Pont leszárom. Mi a francért kell félrevezetni az embereket?

eax_ 2010.09.24. 23:22:03

"(...) amihez valamilyen szinten bele kellene néznie a forgalmunkba, ez pedig sérti a felhasználók jogait"

A routinghoz is "valamilyen szinten" bele kell neznie a forgalomba, pont ugyanez a szint (netflow) pedig tokeletesen elegendo a fertozott gepok 99.9%-anak eszlelesehez.

Redneck pornstar 2010.09.24. 23:59:05

Az irgalmas Allah és az ő prófétája Mohamed nevében: Pofátlan T-Mobile, hol az irodád? :-)

[megmondoember] 2010.09.25. 00:48:00

@esmein: Látom a kritika talált. És sebzett. :)

esmein 2010.09.25. 01:50:43

@[megmondoember]: nem az érdekelt amit mondasz, hanem amennyire jellemző. Szaladj írj blogot, ha te jobb vagy mint ő, aztán majd meglátjuk azt ki olvassa.

Felteszek egy jelentéktelen összeget rá, hogy egy gizda kis billentyűszorfos vagy, aki meg a takinenitől is elnevezést kér, és az otthon magányában retteg, hogy a nagy szájaért ne verjék nyakon. Fikázás az megy. (a másodregék meg már 2002-ben is uncsik voltak.)

Shinjuku 2010.09.25. 02:44:52

@esmein: ... értéket??? mivan?

Geos62 2010.09.25. 05:35:30

@movhu: azért nezd meg a citi netbanking oldalt, én náluk vagyok, de netbankolni nem szoktam velük. A legidegesítőbb, hogy ad hoc utalásokat nem tudsz csinálni, hanem először fel kell vened a kedvezményezettet a kedvezményezett listába, ami viszont már egy sms jóváhagyásos procedura.

- Rendi - 2010.09.25. 06:59:06

@Geos62: Az miért baj, ha vigyázni próbálnak a pénzedre?

KaPé 2010.09.25. 08:02:08

@szita szita péntek: Végülis a kőkorszakban is volt élet, úgyhogy hajrá. Javaslom, az utcára se menj ki, tudod, a térfigyelők...

F173 2010.09.25. 08:57:01

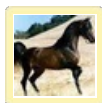
@Ppix: Semmi félrevezető nincs a cikkben! A nemzetközi márkáknak pont az a lényegük, hogy mindenhol egyforma minőséget alkalmazzanak! Ha a T-Mobile Szabolcs, szűri a leveleket, elég valószínű, hogy a T-Mobile Budapest is azt csinálja!

Nincs semmilyen hitelrontás a cikkben, mert az egységes márkán és az egységes tulajdon alapján a cégnek is az a célja, hogy egy egésként kezeljék őket!

Én speciálisan nagyon gőrény dolognak tartom, hogy megsértik a levéltitkot az én megkérdésem nélkül! Nem a postás dolga, hogy eldöntse mi nekem való és mi nem nekem való, kivéve, ha én kifejezetten nem kértem meg rá, hogy csinálja ezt a tevékenységet!

Blossom 2010.09.25. 09:47:48

Hat én csak lestem, hogy miért a new yorki bíró ságra kell elmenni, mert a t-mobile cenzurazza az sms-einket. Nahát, micsoda félrevezetés!



ColT • <http://kilatasgaleria.blog.hu/> 2010.09.25. 10:26:26

"Éppen tudtunk, beleegyezésünk, és jóváhagyásunk nélkül elolvassa helyettünk, előttünk ilyen indokkal az e-mailjeinket," A mailszolgáltató spamszűrői ezt is teszik, igaz jó szándékkal.

Rainbow_ 2010.09.25. 11:10:01

a t-vel itthon is gondok vannak, nálunk a cégnél ők szolgáltatják a netet, mobilt, vezetékest, egy hat évvel ezelőtti 3 forintos tartozás miatt korlátozták a szolgáltatást, késedelmi kamatot követeltek... stb.

Mivel az is követhetetlen, hogy t-mobile, t-systems vagy t-nemtommi már csak egyszerűen t-kurvaanyjának szoktuk becézni.

tutti 2010.09.25. 12:51:55

Engem már tiltott ki a digi, mert vírusgyanús volt a kimenő forgalmam, egy telefon, korrigáltam én is és ők is visszaadták a netet - szerintem teljesen korrekt. Aki nem figyel oda, megérdemli (mint én) :)



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.09.25. 16:28:12

Ha az internetszolgáltató spamszűrésével hasonlítjuk, akkor azért azt tudjuk, hogy:

- kértük/nem kértük a szűrést
- a szűrőbetanítási folyamatot kivéve automata szűr
- tudunk magáról a szűrésről
- elkallódott leveleket megtaláljuk a spam folderben

Itt viszont:

- nem tudunk róla
- amit blokkoltak, az sohanapján se érkezik meg

Azt persze valóban nem tudjuk, hogy egy automata szűrő az "obama" "terrorist" "marihuana" "al kaida" vagy hasonló szavakra, vagy egy ember/Albert Einstein Főbizottság Jégkrémbalett szekciója döntött úgy, hogy ez mehet, az nem mehet,

Mindenesetre ahogy egyszer egy korábbi vállalati magyar szűrő a klasszikus vicc szerint blokkolta Pornóapátli lakosainak teljes levelezését, ha nem tudsz a szűrés tényéről, és Marihuana nevű kölnidet reklámoznád, vagy te vagy Michael Moore és a Hova tűnt Osama Bin Laden című filmedet promoznád, akkor ez úgy bukta, hogy még az okát sem érted. Bár rafinált küldő magát is felteszi a listára utolsó helyre, és ezzel csekkolja a megjött-e, mikor jött meg dolgokat.

Mert ha előre TUDNÁL a szűrés tényéről, akkor nem invesztálnál az üzleti sms-ekbe.

Ppix 2010.09.26. 17:26:35

@F173:

Jaj, hagyjál már ezzel az álnaív kamuzással. Hogy lehet ilyen orbitális baromságokat leírni?

" @Ppix: Semmi félrevezető nincs a cikkben! A nemzetközi márkáknak pont az a lényegük, hogy mindenhol egyforma minőséget alkalmazzanak! Ha a T-Mobole Szabolcs, szűri a leveleket, elég valószínű, hogy a T-Mobile Budapest is azt csinálja!"

Aha. Elég valószínű. Csak a törvényi környezet, a hálózatban alkalmazott hardver és szoftver és az egyes államok nemzetbiztonsági szerveinek hozzáállása tér el.

Hiába az általat "alkalmazott minőségi" csűrés csavarás, azért döreség az egységes márkára hivatkozva feltételezni, hogy mindent tökgugyanúgy csinálnak. Ott van a cikkben, hogy milyen felügyeleti felhatalmazás alapján szűrnek a marketing üzeneteket. Nálunk ilyen nincs.

Mégis mi valószínű akkor?

"Nincs semmilyen hitelrontás a cikkben, mert az egységes márkán és az egységes tulajdon alapján a cégnek is az a célja, hogy egy egésként kezeljék őket!"

Igen, de hogy jön ide az SMS szűrés?

"Én speciel nagyon görény dolognak tartom, hogy megsértik a levéltitkot az én megkérdésem nélkül! Nem a postás dolga, hogy eldöntse mi nekem való és mi nem nekem való, kivéve, ha én kifejezetten nem kértem meg rá, hogy csinálja ezt a tevékenységet!"

Segítek, a reklámüzenet elsősorban nem a privát üzenetek jogi megítélése alá esik, hanem különféle kereskedelmi és fogyasztóvédelmi törvények tárgykörébe.
Nem a Te kis privát üzenetedet szűrnek.

A lényegre persze nem válaszolsz, hogy milyen kis sunyi megtévesztés ez a poszt és a linkelése a címlapon.



nehiddel 2010.09.27. 08:17:16

☐gy vagyok vele, hogy ha nem érdekel egy reklámüzi azt tudom törölni. De, ha a barátnőm épp azt üzeni, hogy seggbe szeretné és ezt cenzúrázzák, mondván, hogy zavaró erotika, akkor mérges leszek.

Jim Tonic 2010.09.28. 17:45:45

[@ergerberger](#): Hát, szerintem neked vannak súlyos értelmezési problémáid, és még támadsz is.

Jim Tonic 2010.09.28. 17:47:30

Megjegyezném, a spam-szűrés és a cenzúrázás tökéletesen ellentétes dolgok. Előbbi értékelendő szolgáltatás, utóbbi viszont szerződésbontásra adhat okot.

Úgy 15-21 hónap

2010.09.28. 21:15 | [Csizmazia István \[Rambo\]](#) | [4 komment](#)

Címkék: [yahoo ítélet 2008 david feltörés palin sarah kernell](#)

A cím nem arra utal, mennyi idő alatt lehet megtanulni elfogadható szinten siklóernyőzni, vagy akár emeltszintű nyelvvizsgát tenni potonghua (mandarin kínai) nyelvből, hanem **annak a valószínű börtönbüntetésnek a mértéke**, amely Sarah Palin Yahoos postafiókjának feltörőjére várhat hamarosan.



Mint emlékeztet, nagyban a választási kampány alatt, 2008 szeptemberében a neten fellelhető publikus információk segítségével törték fel a republikánus Sarah Palin postafiókját, **jelszó emlékeztető segítségével**. Ne menjünk most abba bele, normális dolog-e egy politikustól yahoos címen üzemelni, de **a publikus adatok óvatlan közzétételéről, felelőtlen megosztásáról már mi is értekeztünk egy korábbi posztban**, és **a feltörésnek is számos saját Wikileaks** cikke lett.



A malmok szemlátomást Amerikában sem örölnék sokkal gyorsabban. **David Kernellt bűnösnek találták a 2008-as illetéktelen számítógépes behatolásban**, emellett az igazságszolgáltatás akadályozásában is, mert tette után megkísérelte törölni a gépéről a feltörés bizonyítékait is. A 2010. október 29-ére várható ítélethirdetés előtt a védőknek még formailag van lehetőségük fellebbezést benyújtani, ám **ha nem történik jelentős fordulat az ügyben, és mégsem sikerül próbaidőt kiharcolni, úgy a címben jelzett 15-21 hónap leltöltendő börtönbüntetés látszik valószínűnek**.



Vagyis **most kiegészíthetjük a "Mit tanulhatunk a Sarah Palin esetből" című kérdésre adható válaszok körét a "mit ne adjunk meg jelszóemlékeztető kérdésnek" mellett** azzal is, nagyjából **milyen súlyú ítélet várható** egy ilyen cselekmény után a bíróságon.

 Tetszik  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](#)
- [Akiknek a Captcha kényszerűvé](#)
- [Mi a közös bennük? Trójai, Chrome, kormányzat](#)
- [Elégedetlenség vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2330532>

Kommentek:

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

vrtx 2010.09.29. 08:28:37

Az azért egy kérdés, hogy csak Sarah Palin esetében szabnak ki milyen büntetést, vagy más esetben is lehet erre számítani?! :)

bolhabetu 2010.09.29. 16:47:14

Egyes rosszindulatú pletykák szerint a hölgyből még akár elnök is lehet . Olyan 15-21 hónap múlva kiderül.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.09.30. 17:04:09

@vrtx:

Arra tippelek, jól látod a kérdést, és nem mindig van ez így ;-)



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.09.30. 17:09:59

@bolhabetu:

Meglátjuk. Ha arra gondolok, hogy Schwarci is kormányzó lett a Stallone Pusztító című film után, a 24 óra 3-as évad után meg lett a színesbőrű amerikai elnök, most már csak a későbbi évadok női elnöke hiányzik a jóslatokból. Reméljük, akkor már kevesebbet yahoo mailezik majd, mert a kezére ütnek ;-)

Extra metaadatokkal a még szebb jövőért

2010.10.01. 10:40 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [virustotal](#) [exiftool](#)

Újabb segédprogram eszközzel bővült a VirusTotal repertoárja, ezúttal a [multiplatformos ExifTool](#) ad részletesebb információkat multimédiás állományok vizsgálata esetén.



Az [előző nagy átalakításról](#) már korábban adtunk hírt, ám később sajnos a magyar fordítás is áldozatul esett ennek. Most újabb apró lépéssel egészült ki az oldal fejlesztése. Aki érdeklődik a fotózás után, az már biztos tudja, minden eredeti digitális fénykép megőrzi az eszköz - kamera vagy akár okostelefon - **beállításainak, típusának és a kép körülményeinek idejét az EXIF fejlécében**. Például ha a [Rambo 4 filmnél régebben körülnéztünk, az IMDB oldalán](#) lévő 2007-es fotók a forgatáson készült képek **eredeti, de kicsinyített változatai, amik a későbbi editálás ellenére megőrizték ezeket az EXIF információkat**.



*A képet Karen Ballard készítette egy Canon EOS 5D-vel 2007. július 16-án 11 óra 15-kor, kézi üzemmódban, 1/500-as záridővel és 5.6-os blendenyílással, de az is látszik, hogy a képet MacIntosh-on Adobe Photoshop segítségével kicsinyítették le a weboldalhoz. **Azóta szemlátomást az összes képből kivágták ezeket metaadatokat.***



[Korábban a PDFID fejlécelemző program](#) épült be, amely a PDF-ben levő javascriptekről tud hasznos kiegészítő információt szolgáltatni. Ugyanígy szerepelnek érdekes fejlécdatok az irodai dokumentumainkban is. Mostantól [minden kép- és dokumentum \(DOC, DOCX, XLS, PDF, stb.\) valamint video \(WMV, AVI, ASF, stb.\) állomány EXIF adata megjelenik a vizsgálatkor](#), segítve az esetleges rendellenességek észlelését. Ehhez csak az **Additional information -> Show all** gombra kell rákattintani.



Eddig még nem volt szó róla, de keletkezett a fentiekén túl egy **közösségi kommentelési lehetőség is**, így az eredmény mellett láthatjuk a többi, ugyanazt a fájlt vizsgáló felhasználó megjegyzését is, ami aztán vagy segít rajtunk, vagy sem: időnként azért adhat ez is plusz információt.

Tetszik 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](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Nyári tanácsok utazáshoz](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2335124

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Érdemesebb online bűnözni, mint bankot rabolni

2010.10.04. 18:10 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [usa](#) [uk](#) [letartóztatás](#) [botnet](#) [zeus](#)

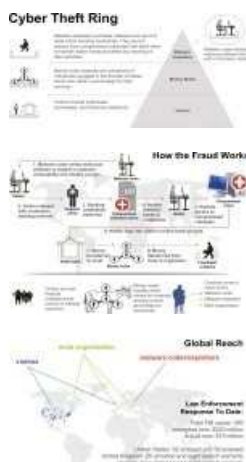
Ha valaki még emlékszik, már 2007-ben megállapítást nyert, hogy az USA-ban a számítógépes bűncselekmények [több pénzt hoztak a szervezett bűnözők konyhájára, mint a drogkereskedelem](#).



A [mostani nagyszabású letartóztatások után](#) a rendőri erők is úgy értékelik, teljes mértékben átalakult hagyományos bűnözés. A **banki azonsítók lopására szakosodott nemzetközi banda tagjait összehangolt akció keretében részben az Egyesült Államokban, részben Nagy-Britanniában** sikerült letartóztatni, sőt még Ukrajában is volt öt letartóztatás, illetve számos házkutatás.



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.



A **Brit rendőrség is elkezdett aggódni**, hiszen [a Zeus botnetes történethez kapcsolódóan 19 letartóztatás](#) éppen az Egyesült Királyságban történt. Érzik, hogy **tudásban, technikában hátrányban vannak és lenne mit fejleszteniük**, hogy jobban lépést tudjanak tartani a fejlettebb kiberbűnözőkkel. Egy kisebb különleges csapat, a London's Police Central e-Crime Unit (PCeU) végzi ezeket a feladatokat egy külön irodában, az ottani viszonyokhoz képest egyáltalán nem horribilis éves keretből dolgozó egység **költségvetése azonban a megszorítások miatt a jövőben még csökkenhet is, ezért valószínűleg szíven üthette őket, amikor a letartóztatott gyanúsítottak állítólag felajánlották speciális szaktudásukat oktatóként**. Általános állampolgári vélekedés egyébként, hogy **a rendőrök inkább az utcákon és a valós életben védjék meg az állampolgárokat, míg a pénzek, online számlák védelme legyen a bankok meg a kereskedők gondja**.



[Lehet böngészni az FBI kapcsolódó közérzési weblapját](#), hátha feltűnik egy ismerős férfi vagy női arc. Ha pedig az ismertett módszerek összevetjük az idei ITBN egyik előadójának felvetésével, hogy egy olyan országban, ahol volt szeretők meztelen képeit jogsértően és következmények nélkül lehet tárolni, ha mindez amerikai szerveren van, [egy lakásban büntetlenül lehet](#) több tucat fantom céget is bejegyezni, ha valakit [eltiltanak a cégvezetéstől, ennek ellenére](#) bátran továbbcsinálhatja, akkor várhatóan lesz jövőkép hasonlóra itt is pár éven belül.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

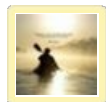
- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2343866>

Kommentek:

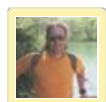
A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói tartalomnak minősülnek, értük a [szolgáltatás technikai](#) üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a [Felhasználási feltételekben](#).



[Christa011 2010.10.15. 10:27:05](#)

Nekem már nagyon elegendő van ezekből a cyber bűnözőkből.

Lehetőleg 220-al agyon csapnám őket.



[Csizmazia István \[Rambo\] • <http://antivirus.blog.hu> 2010.10.15. 10:39:56](#)

Szia Christa011!

Sajnos semmi jóval nem tudlak kecsegtetni. És a helyzet valószínűleg idővel folyamatosan egyre bonyolultabb lesz:

Ismerni fog minket a jövő vírusa:

nonstopuzlet.hu/az-aldozatokhoz-igazodhatnak-a-virusok-20101015.html
viszonyokhoz

Patrick Chan for President

2010.10.07. 13:40 | [Csizmazia István \[Rambo\]](#) | [2 komment](#)

Címkék: [spam](#) [kína](#) [bank](#) [hollandia](#) [üzleti ajánlat](#) [kéretlen](#)

Győztes csapaton ne változtass! - mondta magának félhangosan Patrick Chan ügyvezető igazgató és vezető pénzügyi tisztviselő, majd diktálni kezdett titkárnőjének: Micike, írja kérem: "**Miután az alapokat már sikeresen át a fiók, akkor a részesedése az arány jóvá kell hagynia mind a ketten. Én inkább el nem éri meg az én privát e-mail címét**".



Főnök, van ennek egyáltalán valami értelme? Micike, ne szóljon bele abba, amihez nem ért! Inkább tessék, vegyen még egy málnalekvárral töltött mézbonbont porcukorral meghintve.

Az ember azt gondolta volna, tanul a korábbi elkövetett hibákból, folyamatosan apró lépésekkel javít a technikáján a siker érdekében, cizellál és nüansznyikat csiszolgat a stílusán [ezek után](#), vagy [ezek után](#), esetleg [ezek után](#). **De nem, nem adja fel,** a jó Chan ezek szerint nem tanul holtig. Így marad nekünk a sírva röhögős fogalmazás, emberünk újra meg újra ugyanabba a folyóba lép bele mit sem törődve Herakleitosz alapműveinek esetleges elolvasásával. Mint egy Nyuszi ajtájában ragadt Micimackó, valószínűleg **ő is folyamatosan azt gondolja, nem ragadtam ám be, csak pihenek egy kicsit,** közben meg tűnődök és dudolászok, meg fogalmazok itten kissé.



"A jó válaszra van szükség

Érthető, hogy lehet, hogy egy kicsit nyugtalan, mert nem ismersz, de van egy jövedelmező üzlet javaslatot kölcsönös érdeklődésre számot tartó megosztani veletek. Megvan a hivatkozást én keres valakit, aki megfelel a tervezett üzleti kapcsolatot.

Én vagyok Mr. Chan Patrick ügyvezető igazgató és vezérigazgató-helyettes Hang Seng Bank Ltd. Van egy elsötétített üzleti javaslatot az Ön számára. Azt kell, hogy segítse nekem végrehajtó egy üzleti projekt Hong Kong az Ön országában. Ez magában foglalja az átadás egy nagy halom pénzt. Minden erre vonatkozó ügylet jogilag tenni rántás nélkül. Kérjük, törekednek arra, hogy figyelembe legteljesebb diszkréció érintő valamennyi ügyben ezt a kérdést.

Miután az alapokat már sikeresen át a fiók, akkor a részesedése az arány jóvá kell hagynia mind a ketten. Én inkább el nem éri meg az én privát e-mail címét (e-mail: patrickchan5578@yahoo.com.hk), és végül azt követően, hogy én átadják az Ön további információt a művelet.

Kérjük, ha nem érdekel törölni az e-mailt, és nem vadásznak rám, mert én vagyok én üzembe karrierjét és az életét az én családom a tét ebben a vállalkozásban. Bár semmi sem merte semmi szerzett.

Ön legkorábban választ erre a levélre fogják értékelni."



Ám a hálátlan utókor, a lelketlen közönség nem értékeli az ő fogalmazó zsenijét. Nem is az az igazán szánalmas, hogy spam szemé jön. És nem is az, hogy vannak, akik különféle trükkökkel rendre próbálkoznak. Az igazi szánalom party az, hogy még **egy tisztességes kísérlethez is lusták, nem teszik bele még azt a minimális munkát sem az egyik serpenyőbe, csak bambán várják az ölükbe hulló eredményt.**





Mindenesetre ismét fellélegezhetünk, a magyar internetezők ezúttal is viszonylagos biztonságban maradtak. Vajon gondoltak már arra, hogy esetleg fel kellene venniük egy állástalan magyar tanárt, vagy valami hasonló? Mert hogy így biztosan nem fog menni a csaló biznics.

Ahogy a költő mondja: "Bár semmi sem merte semmi szerzett". Hát ja, egyetértünk művészkém.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

• [1 trackback](#)

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2351559>

Trackbackek, pingbackek:

[Trackback: Megint nyertem ...](#) 2010.10.07. 18:08:30

... mert hihetetlenül szerencsés vagyok, de nem hiszem el...

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 \(törölt\) 2010.10.08. 12:20:02](#)

Rég röhögtem ilyen jól:D



[gothmog 2010.10.17. 18:13:38](#)

Lehet ám, hogy ez ilyen duplacsavar-dolog, hogy aki ennek a béna levélnek bedől, az aztán tényleg oltári nagy balek, és azzal már bármit el lehet hitetni. Akár azt is, hogy ekkora mákja van.

Viszont a levél utolsó előtti sora, amit idéztél, az tényleg olyan szép. :)

Smsben törölhetőek az adatok a mobilokról

2010.10.08. 16:33 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [windows symbian mobile security védelem okostelefon eset](#)

Okostelefonokra tervezett biztonsági csomagot jelentett be a NOD32 vírusirtót gyártó ESET. A Windows Mobile és Symbian operációs rendszereken futó ESET Mobile Security **nem csupán a vírusok, de az adatlopás ellen is** védelmet nyújt: az elvesztett okostelefonokról egy sms segítségével, távolról törölhetőek az adatok.



A Gartner adatai szerint **2010 első negyedévében 54 millió okostelefont adtak el világszerte**, melyeknek több mint felén **Symbian vagy Windows Mobile operációs rendszer** fut. Ezeken a felhasználók jellemzően már nem csupán ismerőseik telefonszámát tárolják, de naptárbejegyzéseiket, feljegyzéseiket is szinkronizálják a készülékekkel, melyek alapértelmezett beállításai szerint még a meglátogatott weboldalak - így például a facebook - belépő adatait is megjegyzik.

A telefon elvesztéséhez kapcsolódó kockázatok mellett folyamatosan növekszik a veszélye annak is, hogy a készüléket vírustámadás éri. Az elmúlt hónapokban számos olyan csaló alkalmazás jelent meg, mely megtévesztéssel veszi rá a felhasználókat arra, hogy hozzáférést biztosítsanak az okostelefonjukhoz. Amennyiben ez sikeres, az alkalmazás **a felhasználó tudtán kívül emelt díjas számokat hív fel, vagy sms üzeneteket küld ezekre**. Emellett szaporodnak az okostelefonokra írt kémprogramok is.



Az ESET Mobile Security segítségével kezelhetővé válnak ezek a biztonsági kockázatok. A most megjelent mobil biztonsági programcsomag az ESET más védelmi termékeihez hasonlóan tartalmaz vírusdefiníciós adatbázison alapú vírusvédelmet és heurisztikus keresést is. **A vírus- és kémprogramvédelem egyaránt kiterjed a készülék beépített memóriájára, valamint a cserélhető memóriakártyák beolvasására és megtisztítására.** Lehetséges a memóriában futó folyamatok ellenőrzése, és az ESET Mobile Security **ellenőriz minden vezeték nélküli kapcsolatot, beleértve a wifi és a bluetooth kapcsolatokon keresztül érkező fájlokat is.** A biztonsági csomag tűzfala arra is képes, hogy **blokkolja az összes mms és adatforgalmat, amikor roamingolunk.**



A vírusvédelem mellett az ESET Mobile Security **legérdekesebb tulajdonsága a távoli törlés (remote wipe) funkció.** Ennek segítségével a jogosult felhasználó elvesztett vagy elloptott telefonjáról távolról tudja törölni az összes adatot egy speciális sms üzenet segítségével. A szoftvercsomag **ezenkívül tájékoztat a biztonsági résekről, kiszűri a kénytelen sms üzeneteket**, és beépített tűzfal segítségével monitorozza a kimenő és a bejövő kommunikációs kísérleteket.



Az ESET Mobile Security funkciói:

Távoli törlés: Vészhelyzet esetén egy speciális sms paranccsal törölni lehet az összes adatot (névjegyzék, üzenetek és a cserélhető memóriakártya adatai) a készülékről.

SIM ellenőrzés: Lehetővé teszi, hogy meghatározott SIM kártyák értesítést kapjanak abban az esetben, ha illetéktelen SIM kártya kerül beillesztésre, beleértve a kártya telefonszámát, valamint IMSI és IMEI számát.



Jelszavas önvédelem: Megakadályozza az ESET Mobile Security eltávolítását a készülékről.

Biztonsági audit: Kényelmes és egyszerű módon jelzi a felhasználóknak az eszköz aktuális biztonsági állapotát, és tájékoztat az esetleges biztonsági résekről.

Sms és mms szűrés: Lehetővé teszi a felhasználók számára, hogy testre szabható fekete- és fehérlisták segítségével meghatározzák, hogy milyen feladóktól fogadnak sms és mms üzeneteket.



Vírus- és kémprogramvédelem: Az ESET keresőmotorjának optimalizált heurisztikai biztosítják a már ismert és a még ismeretlen fenyegetések elleni védelmet. A kártevőket a szoftver törli, vagy karanténba helyezi, ahonnan a későbbiekben visszaállíthatóak. Lehetséges a memóriában futó folyamatok ellenőrzése, és a vírusadatbázis frissítések ütemezésének beállítása (napi, heti vagy havi rendszerességre).

Tűzfal: Előre definiált, vagy a felhasználó által létrehozott szabályok alapján ellenőrzi az összes bejövő és kimenő kommunikációt. A tűzfal ezenkívül képes arra, hogy blokkolja az összes mms és adatforgalmat, amikor a készülék roaming üzemmódban van.



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



Ajánlott bejegyzések:

- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [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/2355825>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Tíz kártevőből hét trójai

2010.10.12. 15:20 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

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

A megtévesztett felhasználók közreműködésével tudnak a legkönnyebben terjedni az internetes kártevők, így a trójai programok vannak többségben az élbolyban. A szeptemberi toplista első helyét ugyan még mindig a Conficker főreg tartja, előnye azonban a második helyezetthez képest ebben a hónapban 8%-ról 5%-ra csökkent.



Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik a hazai felhasználók számítógépeit. A vezető Confickert az INF/Autorun csoport követi, mely a Windows automatikus programfuttatási funkcióját kihasználó kártevőkből tevődik össze. Ezek akár MP3 lejátszókon vagy USB kulcsokon is terjedhetnek, fertőzésük egyik jele, hogy a számítógép működése drasztikusan lelassul.

A toplista többi helyén egy kivétellel trójai programok állnak. A Conficker és az INF/Autorun csoport után harmadik az előző hónapokban feltűnt HTML/ScriptInject trójai, amely egy RAR segédprogrammal tömörített fájlban terjed, és települése során egy üres (c:\windows\blank.html) állományt jelenít meg fertőzött számítógép böngészőjében. A kártevő ezután hátsó ajtót nyit a megtámadott rendszeren, majd további kártékony javascript állományokat kísérel meg letölteni és lefuttatni a háttérben.



A toplista két új tagja közül az első a hetedik helyen megjelenő JS/Redirector trójai. A kártevő az ál-antivírusokhoz hasonlóan hamis riasztásokat jelenít meg a megfertőzött számítógép böngészőjében. A riasztásoknak bedőlt felhasználókat ezután hamis weboldalakra csalja, és megpróbálja megszerezni az adataikat. Mindeközben hátsó ajtót nyit a megtámadott gépen, majd különféle weboldalhoz kísérel meg csatlakozni, és azokról további kártékony kódokat tölt le.

A másik újonc a kilencedik helyezést elérő Win32/KillProc trójai, mely a fertőzött számítógépen különféle kártékony állományokat hoz létre a Documents and Settings mappában, emellett a rendszerleíró-adatbázisban elhelyezett kulcsokkal gondoskodik arról, hogy a számítógép újraindítása után is lefuthasson. Fő célja, hogy a megtámadott gépről adatokat szerezzen, és naplózza a billentyűleütéseket.

Újra felbukkant nyolcadikként a Win32/Shutdowner trójai is. Fertőzés esetén módosítja a Registryben 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 legszembeütőbb hatása azonban, hogy büntetőrutinja lekapcsolja az éppen futó Windows rendszert, és ezzel zavarja meg a munkát, de akár adatvesztést is okozhat.



És végül tizedik lett az első ízben 2009 júliusában listára kerülő Win32/Mebrook trójai, ami egy igen kellemetlen kártevő, hiszen törölheti a merevlemez partíciós tábláját, és így könnyen adatvesztést okozhat.

Vírustoplista - 2010 szeptember

Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2010 szeptemberében a következő 10 károkozó terjedt a legnagyobb számban, és volt felelős együttesen az összes fertőzés 20.90%-ért.



1. Win32/Conficker főreg

Elterjedtsége a szeptemberi fertőzések között: 5.01%

Működés: A Win32/Conficker egy olyan hálózati főreg, 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 eljárásan keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a fűreg 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 szeptemberi fertőzések között: 3.45%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájl 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. HTML/ScrInject trójai

Elterjedtsége a szeptemberi fertőzések között: 2.71%

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. Win32/PSW.OnLineGames trójai

Elterjedtsége a szeptemberi fertőzések között: 1.96%

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. Win32/Tifaut trójai

Elterjedtsége a szeptemberi fertőzések között: 1.69%

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 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/VB féreg

Elterjedtsége a szeptemberi fertőzések között: 1.35%

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. JS/Redirector trójai

Elterjedtsége a szeptemberi fertőzések között: 1.33%

Működés: A JS/Redirector trójai az ál-antivírusokhoz hasonlóan hamis riasztásokat jelenít meg a megfertőzött számítógép böngészőjében. Célja, hogy hamisított (például hamis banki) oldalakra csaljon bennünket, közben pedig hátsó ajtót nyit a megtámadott gépen, 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!/redirector>



8. Win32/Shutdowner trójai

Elterjedtsége a szeptemberi fertőzések között: 1.28%

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/KillProc trójai

Elterjedtsége a szeptemberi fertőzések között: 1.07%

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>



10. Win32/Mebrook trójai

Elterjedtsége a szeptemberi fertőzések között: 1.12%

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 webcímet 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>



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2365036>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Kétmillió zombigép tábor az USA-ban

2010.10.14. 14:20 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [microsoft jelentés zombi botnet](#)

Az Egyesült Államok vezet a botnet fertőzött gépek számának versenyében, becslések szerint **körülbelül két millió akaratát veszített, távirányítható zombigép található az országban**. A Microsoft kimutatása szerint Brazília volt a második helyezett 550 ezer fertőzött géppel.

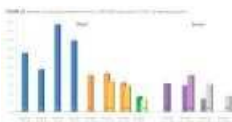


A [240 oldalas jelentés](#) szerint a Lethic nevű botnet volt a felelős a kiküldött spamok 56 százalékáért. A 2010 április és június közötti időszakban a Microsoftnál 6.5 millió fertőzést detektáltak és végezték el a mentesítést. **Ez a szám éppen a duplája az egy évvel korábbi, 2009-es hasonló időszakban mért értéknek**, így ez is jól demonstrálja, mennyire súlyos ez a probléma.

A screenshot of a Microsoft security report showing a table of infected systems. The table has columns for 'Country', 'Number of infected systems', and 'Percentage of total infected systems'. The data is as follows:

Country	Number of infected systems	Percentage of total infected systems
USA	1,100,000	16.8%
Brazil	550,000	8.4%
France	300,000	4.6%
Spain	250,000	3.8%
Germany	200,000	3.1%
Italy	150,000	2.3%
UK	100,000	1.5%
China	50,000	0.8%
India	20,000	0.3%
Japan	10,000	0.2%

A teljes [jelentés 600 millió olyan számítógép vizsgálatára épül](#), melyet valamilyen Microsoftos szolgáltatást, például Essentials vagy Defender csomagot használ. Valamint az is kiderül, hogy **a fertőzött XP operációs rendszerű gépekkel van a legtöbb gond**, ott kell a legtöbbet munkát végezni.



Ebben a hónapban mintha csak be akarnának kerülni a Guinness Rekordok Évkönyvébe a legnagyobb javítófolt kategóriában, **a legtöbb javítást bocstották ki** a tegnapi Patch Tuesday keretében: összesen **49 különféle sebezhetőségre került javítás**, amelyek közül 23 fontos minősítésű volt. Az MSRT (Malicious Software Removal Tool) eszközt pedig igyekeztek tovább okosítani a Zeus botnet kártevői ellen.

A screenshot of a Microsoft security report showing a table of security updates. The table has columns for 'Security update', 'KB number', 'Release date', 'Supported operating systems', and 'Supported products'. The data is as follows:

Security update	KB number	Release date	Supported operating systems	Supported products
Windows 7	KB2616671	10/12/2010	Windows 7	Windows 7
Windows 8	KB2616671	10/12/2010	Windows 8	Windows 8
Windows 8.1	KB2616671	10/12/2010	Windows 8.1	Windows 8.1
Windows 10	KB2616671	10/12/2010	Windows 10	Windows 10
Windows 11	KB2616671	10/12/2010	Windows 11	Windows 11
Windows 12	KB2616671	10/12/2010	Windows 12	Windows 12
Windows 13	KB2616671	10/12/2010	Windows 13	Windows 13
Windows 14	KB2616671	10/12/2010	Windows 14	Windows 14
Windows 15	KB2616671	10/12/2010	Windows 15	Windows 15
Windows 16	KB2616671	10/12/2010	Windows 16	Windows 16
Windows 17	KB2616671	10/12/2010	Windows 17	Windows 17
Windows 18	KB2616671	10/12/2010	Windows 18	Windows 18
Windows 19	KB2616671	10/12/2010	Windows 19	Windows 19
Windows 20	KB2616671	10/12/2010	Windows 20	Windows 20
Windows 21	KB2616671	10/12/2010	Windows 21	Windows 21
Windows 22	KB2616671	10/12/2010	Windows 22	Windows 22
Windows 23	KB2616671	10/12/2010	Windows 23	Windows 23
Windows 24	KB2616671	10/12/2010	Windows 24	Windows 24
Windows 25	KB2616671	10/12/2010	Windows 25	Windows 25
Windows 26	KB2616671	10/12/2010	Windows 26	Windows 26
Windows 27	KB2616671	10/12/2010	Windows 27	Windows 27
Windows 28	KB2616671	10/12/2010	Windows 28	Windows 28
Windows 29	KB2616671	10/12/2010	Windows 29	Windows 29
Windows 30	KB2616671	10/12/2010	Windows 30	Windows 30

A sérülékenység javítások közül az egyik pedig [azzal a Stuxnet féreggel volt kapcsolatos](#), amelyiket az első közismert iráni erőműveket, ipari létesítményeket célzó állítólagos támadásként emlegetnek. Hogy ez aztán **mennyire felel meg a valóságnak, és mennyi benne a szenzációhajhászás**, arról lehet és érdemes is beszélni. Mindenesetre jószívvá ajánljuk [ezt a jó kis összefoglalót](#) hozzá elolvasni.

[Tetszik](#) [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztás](#) [+1](#) [0](#) [Tweet](#)

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Nyári tanácsok utazáshoz](#)
- [Mai szavunk pedig: keyjacking](#)

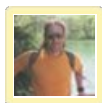
A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2370664>

Kommentek:

gusthy1 • **<http://kolyokjoga.blogspot.com>** **2010.10.15.**
20:28:53

A két milliós zombitábor az 2 db., darabonként egymilliós zombitábor.



Csizmazia István [Rambo] • **<http://antivirus.blog.hu>**
2010.11.22. 10:49:43

Szia Gusthy1!

Csak most vettem észre a kommentedet, és köszi, tökéletesen igazad van.

Dél-Korea is kínai behatolást gyanít

2010.10.18. 10:20 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [kína](#) [korea](#) [támadás](#) [kémkedés](#) [botnet](#)

Többször is adtunk már hírt hasonló angliai, amerikai és németországi esetekről, [az egyik éppen Angela Merkel kínai utazása alatt](#) történt. Most Dél-Korea ismételt rádöbbenhetett, **potenciális és vonzó célpontja a kínai hackereknek.**



A hamis, látszólag saját minisztériumoktól érkező emailek mellékleteiben lapuló kártevőkkel, kémprogramokkal állítólag [stratégiai fontosságú hivatalos dokumentumokat, gazdasági prognózisokat](#) sikerült az ismeretlen támadóknak eltulajdonítaniuk például a dél-koreai Külügyminisztériumból.



Korábban **2008-ban és idén augusztusban is felmerült már** a gyanú, hogy az ellenséges viszonyban lévő Észak-Korea esetlegesen **katonai titkokat szerzett meg** szintén hasonló módszerekkel. Akkor különféle nukleáris rakéták tervei, és más stratégiai haditechnikai eszközökkel kapcsolatos információk kerülhettek rossz kezekbe. Azonban sem akkor, sem most **nem lehetett a támadások forrását kétséget kizáróan beazonosítani**, még ha sokszor el is jutnak például kínai IP címekig.



Bár biztonsági szakértők okkal **feltételezik, hogy mind Kína, mind pedig Észak-Korea több ezer főnyi** hivatalos katonai hacker egységet tart fent erre a célra, a támadások mindig olyan földrajzilag vegyes elhelyezkedésű fertőzött zombigépekről történnek, ahol a támadások konkrét irányítóit **nehéz, vagy éppenséggel lehetetlen** egyértelműen beazonosítani.



Lassan már valóban **nem is az lesz a kérdés**, hogy az egyes országokban az Egyesült-Államokhoz hasonlóan szintén szükséges-e kiberhadereg létrehozása vagy sem, **hanem inkább az**, hogy [mikor és mekkora létszámmal álljon fel](#) az minél hamarabb.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  0  Tweet

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Ez történik a weben egy perc alatt](#)
- [Utaljunk pénzt a S.O.C.A.-nak](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2379000>

Kommentek:

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

zoldbeka55 2010.10.18. 13:23:58

Ez most komoly, hogy hackerakcióval nukleáris titkokhoz lehet jutni? Hogy őrzik ezeket? Eleve mi értelme, hogy ezeket internetre kötött számítógépeken tárolják? (Gondolom különben nehéz lenne hozzáférni, majdhogy nem lehetetlen, mert ki az, aki telepátiaival le tud csenni bármit, egy hálózathoz nem csatlakozó gépről?) Jó, hogy nem egyenesen a Facebook-ra töltik fel a cuccot... Nem értem ezt a dolgot...

Laci Today Magazin • <http://www.lacitoday.blog.hu> **2010.10.19. 09:14:40**

[@zoldbeka55](#): sőt egyszerűbb bombák elkészítéséhez Te Magad is találhatsz instrukciókat a neten, még hackelned sem kell. Én egy bio-bomba leírását tudom: kell hozzá egy nagyméretű, félgömb alakú öntöttvas tárgy (pl. bogrács tökéletes), kell hozzá hagyma, paprika, bab, só, víz, marhahús, zöldségek. A félgömb alakú öntöttvas tárgy alatt tüzet gyújtva, benne vizet forralunk, az összetevőket beledobáljuk, és várunk 3-4 órát. Ezután az elkészült bombalét jóízzel elfogyasztjuk, alszunk rá két órát, majd buszra szállunk és a tömegben nincs más dolgunk, mint hogy ellazulunk. A bomba hatása néhány percen belül észrevehető lesz.

Üdv!

Laci Today

-egy hétköznapi lacilap, a humor hevében-

Oszd meg, keress csilliókat, és uralkodj

2010.10.19. 17:05 | [Csizmazia István \[Rambol\]](#) | [35 komment](#)

Címkék: [adatvédelem facebook vs](#)

Ezer epizódos Telebubbies maraton egyhuzamban való megnézésével leamortizált agyvelő kellene ahhoz, hogy egy sokadik "jaj, hiszen ez csak technikai hiba miatti véletlen, hogy egyenest a reklámcéghez kerültek a személyes adatok" **kijelentést valaki komolyan és őszintén el is higgyen.**



Aki sokszor és sokat vétkezik személyes adataink ellen így, az lassan, de biztosan elfogyasztja a rá vonatkozó lapokat a bizalmi csekkfüzetünkéből. **A bevezetéshez érdemes elolvasni az igen gondolatébresztő bejegyzést: [A Facebook megosztja egyedi azonosítónkat harmadik cégekkel](#).** A lényeg: Emily Steel és Geoffrey A. Fowler, a Wall Street Journal két újságírója **felfedezte, hogy a Facebook alkalmazások több millió felhasználójának adatai még akkor is átkerülnek a hirdetőkhöz, ha a felhasználók a legszigorúbb biztonsági beállításokat alkalmazták a profiljukban. A legszomorúbb ebben az, hogy ez még csak nem is újdonság:**



2010.05.21. [Újabb Facebook-botrány: felhasználói adatlapokat küldenek a hirdetőkhöz](#)

"Egészen pontosan arról van szó, hogy a Facebook **megküldte a hirdetőkhöz azon felhasználók adatlap id-ját, akik az adott hirdető hirdetésére kattintottak a szájton.**"

2010.05.26. [Facebook miatt hisztizni = NEM MENŐ](#)

"Természetesen mindenkinek joga van kényelmetlenül érezni magát, hiszen **a Facebook modelljében a felhasználó nem fogyasztó, hanem maga az áru, amit a cég valódi fogyasztóinak, a hirdetőkhöz ad el.** Legalábbis az adatait mindenképpen."

2010.08.04. [Minden, amit a privacy-ról tudni akartál... I. rész](#)

"Minden egyes alkalommal, ha például a 83 millió virtuális farmer valamelyike a FarmVille mezőgazdasági szimulációs játékkal, vagy a MaffiaWars-szal játszik, **megengedi, hogy letöltsék a profilját és továbbadják az adatait egy harmadik félnek. Az ismeretlen harmadik fél pedig semmilyen szerződéses viszonyban nem vagyunk.**"



Az Egyesült Államok két képviselője, Edward Markey és Joe Barton máris levelet írt Mark Zuckerbergnek, a Facebook alapítójának. **A képviselők szeretnék megtudni, hogy milyen lépéseket tesz a közösségi oldal a biztonsági rés megszüntetésére.** A levélre a Facebooknak október 27-ig kell válaszolnia. A korábbi események fényében félok, hogy [ennek sem nem lesz](#) semmilyen komoly következménye.

Végül is milyen erkölcsi alapon várnánk mást attól, aki [az első millióját is vitathatóan, egyetemi adattolvajként](#) szerezte. Azt, hogy aztán a koncepciót végül is ki lopta el kitől, és hogy a kezdő csapat tagjainak kigolyózása mennyire volt korrekt vagy etikus, **az már ezek után szinte mellékes, ezt teljes egészében az olvasó fantáziájára és megítélésére bízhatjuk.** Az újabb eset fényében azonban látni kell, hogy aki Malymváry Armandóként regisztrálva Zombáról minden mezőbe valami egetverő válogatott baromságot gépel be, **vagy csak mindössze egy szimpla álnevet választva aztán mindent üresen hagy** - hiszen a barátokkal való kapcsolattartáshoz ez is bőven elég - **az közelít jól a saját adatainak védelméhez.**



Sajnos az átlag felhasználók többsége továbbra sem fogja érteni, mi is ez az egész, miért is lenne baj, hogy odaadják az adatait, vagy az is lehet, hogy egyáltalán nem is érdekli - ez a legnagyobb baj. Nem lehet mindenki adatvédelmi szakértő. Viszont azt joggal várhatnánk el, hogy ha például nem értünk az autószereléshez, a szervízes ezt akkor se használja ki a kárunkra, és sarcoljon ki csillagászati összegeket a számlán. Ugyanígy amikor az adatainkat rábizzuk egy vállalkozásra, az akkor is védje ezeket, ha mi ennek minden részletét esetleg nem is értjük pontosan, vagy nem vagyunk képesek ezt ellenőrizni, viszont bizalmunkat odaadtuk a regisztráláskor.

Sixx! Anyádat is nyuggernek hívod? • **<http://orbanfan.blog.hu> 2010.10.19. 22:37:18**

Valahogy tudatosítani kellene az emberekben, hogy a fészbuk ártalmasabb, mint a windows és az atombomba együttvéve...

☐Te is Fido-ztál valaha☐Csak a linkdobozban lévő vízlepcső-s link miatt kérdezem :☐☐



nemecsek ernő áruló • <http://nem.valodi.email.hu/ezt-jelentsd-fel-papcsak> 2010.10.19. 22:43:07

Tudom, hogy rá fogok fázni erre a kérdésre, de: na és?

Meg van adva 3 adatom facebookon. A nevem, a város, ahol élek, meg egy-két klub azonosítója. A hirdetések baromira nem ezen adatok alapján jönnek velem szembe, hanem a böngészési előzményeim alapján, ergo olyan hirdetéseket kapok, amik feltehetőleg nagy valószínűséggel relevánsak számomra. Nem ez minden hirdető célja? Hogy minimalizálja a fals találatokat? Akkor hol van a gond?

Az alkalmazásoknál meg mindig rákérdez, hogy engedélyezed-e a dolgot, aki nem olvassa el a szöveget, csak vakon klikkel, azt úgy hívjuk, hogy az így járás tipikus esete. Tényleg többször elolvastam a bejegyzést, de egyszerűen nem értem, hol itt a gond?

Te adod meg az adatokat, amit használhatnak. Te adod meg az e-mail címed. Te adod meg a neved, a lakcímedet, a születési dátumodat. Nem kötelező. Aki paranoiás, az NE LEGYEN facebook tag könyörgöm. Olyan unalmas már mindenhol ezzel találkozni, hogy "így a gonosz fészbuk, kiadja az adatokat, amiket ÉN megadtam neki, hát még ilyet..." Persze, hogy minden közösségi oldal a felhasználói adatokkal kereskedik. Ez a lényege. Ezért találták ki!

Az ég egy adta világon SOHA SEMMI más célja nem volt!!!

Sixx! Anyádat is nyuggernek hívod? • **<http://orbanfan.blog.hu> 2010.10.19. 22:43:28**

Azé' ez se semmi itt a hozzászólás ablak alatt:

Warning: file_put_contents() [function.file-put-contents]: Only 0 of 165 bytes written, possibly out of free disk space in /var/local/www.blog.hu/bloghu2/Lib/Bloghu/Slog.php on line 138

Sixx! Anyádat is nyuggernek hívod? • **<http://orbanfan.blog.hu> 2010.10.19. 22:45:50**

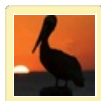
@Gerzsonka: ott a gond, hogy te csak x adatot adtál meg, de vannak akik $n \cdot x$ -et, ahol $n > 1$. És a felhasználók úgy hiszik, hogy az adataik biztonságban vannak. Épp arról szól a dolog, hogy fészbukék visszaélnék a tudatlanok, paranoia-mentesek bizalmával.

Én nem adtam meg semmit (amit megadtam, az hamis volt és töröltem is), mégis felháborít a dolog.

1rem1 Art • <http://1rem1.com> 2010.10.19. 22:52:03

out of disk space wazze...

elfogyott az internet?!



pelikán* • <http://mandiner.blog.hu> 2010.10.19. 23:06:51

A lényeg, hogy kulturáltan használjuk a fácsét, akkor nagy baj nem lehet:

mandiner.blog.hu/2010/08/18/a_kulturalt_facebook_felhasznalo_18_pontja

teddyde • <http://ezmegigyhoggy.tumblr.com/> 2010.10.19. 23:11:51

[☐ pelikán ☐](#): ☐hfényezés = nem menő

ráadásul szar saját cikket ajánlani epic fail...

aDoayen@HWSW 2010.10.19. 23:26:54

szerintem fussunk ennek neki újra...

a psprovokatív szerzője valószínűleg nem tud angolul, vagy egyszerűen figyelmetlen volt

a WSJ anyaga ugyanis arról szól, hogy a Facebookon az ALKALMAZÁSOK osztják tovább az ID-ket. az adataid privacyja olyan, mint amilyennek beállítottad, illetve sajnos, amilyennek a barátaid beállították. (bár azt is tudod szabályozni h a barátaidon keresztül mi kerülhet ki rólad)

a bibi azzal van, hogy mondjuk a farmville tud profilozni a szokásaid alapján, az ID-det kiadja 25 cégnek, akik már konkrét marketingalanyként kezelnek és szépen kapod a direkt megkereséseket, mivel az ID-d és az alkalmazás használati szokások alapján eleve megvagy, a többi adatodat meg magad osztottad meg.

ha valakit érdekel részletesebben, nem blog.hu-san, akkor:

www.hws.wu/hirek/45483/facebook-kozossegi-web-alkalmazas-szemelyes-adat-zynga-farmville.html

1rem1 Art • <http://1rem1.com> 2010.10.19. 23:41:59

[@aDoayen@HWSW](#): végre egy tiszta hang

mokas_gizi 2010.10.20. 01:02:20

Szánalom ez a Facebook, én sosem voltam rajta és sosem kerültem velük kapcsolatba mégis hotmail-os email címeimre kapom a hülyeségeiket, hogy ez meg az szeretné hogy csatlakozzam és életbe sem láttam még azt az embert...

thatwasnice 2010.10.20. 03:40:01

szerintem kicsit túldramatizáld a dolgokat

én leszarom, hogy mit tudnak meg rólam, legyenek vele boldogok, ha tudják milyen márkájú fogkrémet használok vagy akármi, elmondom bárkinek szívesen, de szerintem senkit nem érdekel. meg azt hiszed majd pont a te dolgaidra kíváncsik? ki vagy te? fontos ember???



Dr.Traktor 2010.10.20. 06:55:57

a fészbuk egy szar, aki használja egy majom.

ez egy olyan alkalmazás aminek a világon semmi értelme.

viszont remekül fel lehet használni adathalászatra.

aki ért hozzá az meg kihasználja az olyan ártatlan dolgoktól, hogy megnézem nincs-e bent az új szomszéd jócsaj/kolléganő hogy kis infót megtudjak róla, odáig, hogy kinézem mikor mentek idén nyaralni hogy a haverokkal felnyomjuk a kéglit. (ha már a lányod volt olyan hülye hogy kirakott erről egy beivott topless képet a felirattal: " 2 hét múlva Ibizaaaaaaaaaa!!!!") ja bocs lehet nem is a lányod volt hanem a lányod liba bnője aki szintén veletek utazik! úúúúú. bocs.

egyébként ezen kívül még azt lehet elmondani, hogy az emberek egy jó része hülye (nem csak ahhoz, hogy felismerje miért fontos az adatvédelem) és mivel sokan vagyunk ezen a rohadt bolygón a hülyék száma is egyre magasabb.

másrészt az a véleményem hogy legjobban igenis a saját kárán tanul az ember. már aki nem hülye. annyira.

KolompárRómeó 2010.10.20. 07:13:34

"higyen" Eddig olvastam.

adatvédelem • <http://www.ppos.hu> 2010.10.20. 07:21:48

[a](#) [oayen](#) [WSW](#): Egyetértek. A fő probléma az átadott adatok alapján felépített profil, ami olyan következtetést is tartalmazhat, amiről még a felhasználónak sem volt tudomása. A kialakított profil aztán a direktmarketingtől kezdve, bármire használható. www.adatvedelmiszakerto.hu/2010/09/kozossegi-oldalon-kialakitott-profil-felhasznalasa-allasinterjun/
Hiába szigorodik az adatvédelmi szabályozás, ha mi magunk felelőtlenek vagyunk.

rekszem 2010.10.20. 07:52:58

thatwasnice

Azért az ismerőseidet lehet mire használni, sőt, van lány ismerősöm, akinek az új kolléganője egyből szúrta a szemét, mert az ismerősei között az ő barátjának az exe is fent volt :D

Illetve valahok jól leírták, hogy pl. felteszel egy képet a kecórol, ott a címed, majd bejelented, hogy elutazol, vagy megosztod a gps koordinátáidat, és máris lehet menni fosztogatni.

Vagy valaki kommentálja a képedet, és máris a napszaron találod magadat :DDD

Én iwiw-is mondogrammra váltottam, faszbukra meg sosem regisztráltam be.

bierkamp 2010.10.20. 07:56:01

a Facebook hazudik???? -akkor a NEMZETI Orbán mit csinál?----ja, Lop ás Hazudik...) A Facebook legalább nem lop!

kvadrillio 2010.10.20. 07:59:41

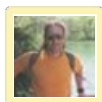
Húúúúú, most akko mindenki meztelenül áll a NAGY MANITÚÚÚ ELŐTT !!!

Na bumm ! Reptéren is átvilágítanak mindenkit csontig !
Neten is tudnak mindent, még ha ki is törlik ! :)

Egyet viszont nem tudnak pl rólam: Interpóóóál által körözött sorozatgyilkos vagyok, jelenleg a siralomházból netezek és várom a méreginjekciót !
Hobbim a vámpírkodás, , üres óráimban a Móríckát olvasom és az internetet csakis azért használom, mert szeretek zongorázni a klaviatúúúúúrán.....
Most, hogy így kiegészítettem digitális lábnyomokkal a profilomat nyugodtan hajtom álomra a nethírektől terhelt fejemet !

...és igyekszem visszavonulni rejtélyes inkognitómba !!! :O)

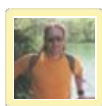
Azért kérem, hogy titkaimat ne adják tovább ! :D



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.10.20. 08:04:16

Szia Sixx! Anyádat is nyuggernek hívod?

Van egy cimborám a Vízlépcsőn, ennyi. Én még Virnet BBS-eztem 300 bauddal :-)



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.10.20. 08:08:53

Szia Pelikán!

Nem ismertem ezt a posztot, de egyrészt szerintem semmi baj azzal, ha valaki a saját posztját kommenteli be, ha az ontopic.

Másrészt van az írászeszedett pontokban számos igazság. ☐. "Ne csatlakozzunk olyan csoportokhoz, klubokhoz, melyek ☐Aki ík☐ felütésre kezdődnek..." ☐ ízi a kommentet.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.10.20. 08:15:15

Szia thatwasnice☐

Szerintem nem kell fontos embernek lenni, hogy mégis vigyázzon az ember a személyes adataira. A célzott reklámokra is szerintem kevesen vágnak.

☐e itt van két gyakorlati példa is.

1. ☐a pornót néztél a neten, most megszívtad
itcafe.hu/hir/porno_internet_trojai_kenzero.html

"...mely a fertőzött számítógépek használoinak webes böngészési előzményeit hozza nyilvánosságra..."

2. Információalapú vírusterjesztés: nehéz küzdelmek várnak ránk
biztonsagportal.hu/szembe-kell-nezni-az-informacioalapu-virusterjesztessel.html

"...sok olyan kártékony program terjed, amelyek nem tesznek mást, mint figyelik a felhasználók tevékenységét, böngészési szokásait, és rendszeresen jelentést küldenek a készítőiknek..."

Végül pedig ha valaki nagyon akar, 10-20 év múlva is eszébe juthat, hogy mégis fontos ember szeretne lenni,



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.10.20. 08:16:28

[@Dr.Traktor](#):

"a fészbuk egy szar, aki használja egy majom."

Szerintem ez így azért nem igaz.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.10.20. 08:17:46

[@KolompárRómeó](#):

Jogos a két pont, ezt benéztem. Kijavítottam, és remélem, most már továbbolvasol :-)



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.10.20. 08:22:11

[@adatvédelem](#): Szia!

A folyamatosan változó FB felhasználói szerződés hatása a megosztott adatokra 2005-2010:
m.blog.hu/an/antivirus/image/201008/faca.jpg



Dr.Traktor 2010.10.20. 08:23:25

[@Csizmazia István \[Rambo\]](#):

azért remélem a többit is olvastad, nem csak az első sommás véleményemet :P



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.10.20. 08:23:29

[@rekszem](#):

Igen, és is erre gondoltam, sok ilyen eset volt már terítéken itt a blogban is.



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.10.20. 08:26:52](#)

[bierkamp](#): Szia

Mentségemre nem én adom a zinde cimlapos címet meg a leadet, azt ők készítik a legjobb belátásuk szerint olyanra, amilyenre ők akarják.

n igazából kételkedni merészeltem abban, hogy már sokadszor merő véletlenül kerül ki tőlük személyes adat a hirdetőkhöz. Szerintem ami egyszer történik, az véletlen. Ami kétszer, az egybeesés. Ami háromszor, az már összeesküvés.



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.10.20. 08:29:29](#)

[@Dr.Traktor](#):

Igen, igen, mindent :-D

[G1 2010.10.20. 08:33:56](#)

Első jótanács: bármilyen vonzónak is tűnhet, kezd azzal, hogy minden alkalmazást letiltasz a faszbukban. Főképpen, hogy indítás előtt ezzel kezdi: az alkalmazás hozzá fog férni az ön és ismerősei adataihoz bla-bla.. Na aki ezt engedélyezi, az ép ember nem lehet...

Második jótanács: ha már mindenképpen közösségi száj, akkor addig juss el legalább, hogy bármi, ami nem a te gépeden van (néha sajnos ez sem igaz), hanem egy ki tudja milyen oldalon, azt beállítás ide vagy oda, bárki a világon láthatja. Olyanok is, akiknek az az életcéljuk, hogy visszaéljenek vele. Ennek szellemében tegyél fel magadról bármit, adj meg bármilyen adatot. És ahogy Rambo megjegyezte: "10-20 év múlva is eszedbe juthat, hogy mégis fontos ember szeretnél lenni"



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.10.20. 08:33:57](#)

[@aDoayen@HWSW](#): Szia!

Köszí a hozzászólást. Sajnos én csak ilyen blog.hu-sat tudtam;-)

Szerintem az elég gáz, hogy csak akkor van probléma, ha egy WSJ újságíró kipattintja azt, és nem akkor, amikor ezeknek az alkalmazásoknak teret adó cég erre magától üzemszerűen odafigyelne, mert mondhatjuk lett volna erre elég idejük. Ha véletlenül nem írnak az újságírók, akkor mi lenne?

[Bougheau Tschichka 2010.10.20. 10:00:39](#)

Nincs ebben semmi meglepő, ha arra gondolok, hogy ki is az alapítója, tulajdonosa. Valami Zuckermann ?



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu)
[2010.10.20. 10:48:19](#)

www.itbusiness.hu/hirlevel/itsecurity_today/2010-10-19_it_security_today_4717.html

Csak idézek:

www.itbusiness.hu/hirlevel/itsecurity_today/2010-10-19_it_security_today_4717.html

"...rendszeresen kiadja a játékosok azonosítóit külső cégeknek. A FarmVille a játékosok barátainak adatait is kiadja..."

"A „vádolt” nem tagadja a vádakat. Reakciójából úgy tűnik, hogy a WSJ összefoglalója előtt már ismerte az eseteket – de nem sietett a megakadályozásukkal."

adatvédelem • <http://www.ppos.hu> 2010.10.20. 17:58:18

☐ [Csizmazia István](#) ☐☐[Rambo](#)☐: Szia☐

Megdöbbentő az ábra, ennyire kézzelfoghatóan még nem is láttam. Sajnos nem állhat minden felhasználó mellett egy adatvédelmi szakértő

adatvédelem • <http://www.ppos.hu> 2010.10.20. 20:22:02

[@Csizmazia István](#) [[Rambo](#)]: Az adatvédelem és a privát szféra ilyen szintű semmibe vétele pedig elkésérítő, ugyanakkor remélhetőleg ttovább erősíti a felhasználók "öntudatát"

Haladócsoporthoz átverés

2010.10.21. 12:45 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [weboldal hamis attack támadó page webhely bejelentett reported](#)

A [korábbi pitiáner ősmagyar nyelvezetű banki adathalásznak csúfolt](#) próbálkozások mellett azért van időnként egy-két olyan jó ötlet is, amire joggal mondhatjuk: hmm, ez ügyes.



Ugye már mindenkinek, vagy legalábbis a netező többségnek [megvolt az ismerős pavlovi reflexeket megmozgató Bejelentett Támadó Webhely](#) szindróma. Ezt láthattuk [egyszerű juzerként](#), amikor böngészünk, de elszenvedhettük úgy is, mint aggodó weboldal tulajdonos.



Hagyományos mosópor, szokásos üzenet

Ekkor ugye Javascript puceralás az összes HTM, HTML, PHP állományunkban, azonnali FTP jelszó csere, és irány a Google Webmaster Tools, ahol is úttörő becsületszavunkra lejelentjük, már tiszta az oldal, meg különben is.



És pontosan itt jön a képbe a jó érzékű csaló, mikor már mindenkinek a retinájába égett a fenti felirat, oda a kezdeti újdonság varázsa, nincs kétségbeesés, csak fásultság, megint egy, meg megint egy és megint egy, uncsi. Ilyenkor már lazul a figyelem, csökken a koncentráció, és ez a legmegfelelőbb idő a trükközésre. Meg is érkezett a hamis "Reported Attack Page!" feliratú oldal és azonnal fel is tehetjük az ezer forintos kérdést: Vajon miben különbözik az eredeti és a preparált oldal?



Azok nyerték a hangszórót, akik a letölthető frissítés (Download Updates) gombra tippeltek. Pavlov kutyaíhoz hasonlóan, ahol eredetileg a csengő szó kiváltotta a nyáleválasztást, nálunk pedig a már sokadszorra látott Bejelentett Támadó Webhely váltja ki a "jólvanmárahaggyatokbékében-katt-menjünkmártovább" eseményt.



Vagy éppen DDoS-olják a VirusTotalt, vagy karbantás van, ezért most kínunkban Jottizunk egyet

Nyilván a [naprakész víruskeresővel van némi esély](#) ezt elkerülni, de a klasszikus jön farkas, jön farkas sztori beválik: a sokadik jön a farkas után már nincs izgalom, adrenalin bomba, csak a beletörődő fásult bamba kattingatás, esetleg halk szentségelés. Időközben [az F-Secure blog](#) már arról is beszámolt, megérkezett egy újabb változat, amely "Chrome_secure_upd.exe" nevet kapta a keresztségben.



Azért azt le kell szögezni, kell egy bizonyos fokú hamvas ártatlan naívság ahhoz, hogy valaki higgyen a mesékben, a Mikulásban és

abban, hogy éppen egy támadó webhelyen kattintva kell letölteni azt az EXE frissítést, ami majd elhárítja a bajt, és mindent megold. De ettől függetlenül, jár a pont a vidéki versenyzőnek, van a tervben ráció, nice try. Bár nem igényeltük, de ezúttal is megkaptuk: itt egy újabb bizonyíték, hogy a kártevőterjesztők nem kímélik a fantáziájukat, **így az odafigyelésünkön mi sem lazíthatunk**.

 Tetszik  Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [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/2387959>

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.

Két kongresszusi képviselő levelét megírta

2010.10.25. 16:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [adatvédelem](#) [facebook](#) [levél](#) [hirdetők](#) [vs](#) [kongresszusi](#)

Egy korábbi posztunkban már írtunk arról, hogy a Facebook alkalmazások harmadik fél számára [titokban továbbítják a programokat telepítő felhasználók azonosító ID-jét](#). A reklám cégek nem gyűjthetnek ilyeneket és nem kezelhetnek, tárolhatnak személyes adatokat - _ELVILEG_. A [Wall Street Journal](#) újságírói viszont október 18-án bemutatták, hogy **mégis ez történik - _GYAKORLATILAG_**.



A riport megmutatta, hogy **a tíz legnépszerűbb alkalmazás mindegyike továbbított ilyen személyes adatokat a fejlesztőknek, illetve harmadik félnek, és gyakorlatilag a felhasználók ezt semmilyen módon, semmilyen beállítási lehetőséggel nincs módjuk letiltani, megakadályozni**. Előző cikkünkben azt is megírtuk, hogy az Egyesült Államok két képviselője, Edward Markey és Joe Barton levelet írt Mark Zuckerbergnek, a Facebook alapítójának.



A képviselők azt szeretnék megtudni, hogy milyen lépéseket tesz a közösségi oldal a biztonsági rés megszüntetésére. Most a [Daily Caller jóvoltából elolvashatjuk a levelüket](#), ami **kellemesen határozott hangvételű** (pl. 3. When did Facebook become aware of this security breaches? 11. Please provide copies of any agreements between Facebook and its third party application developers.), szóval érik a botrány.



Reménykedjünk, hogy egy ilyen jellegű fellépésnek talán mégis lesz valamilyen előremutató, a személyes adatvédelem szempontjából jótékony hatása, kényszerítő ereje.



Azoknak pedig, akik már [a nagy Facebook öngyilkosság alkalmából](#) is elgondolkoztak a leiratkozáson, bemutatunk egy összefoglalót a Facebookon túl is van élet :-)) címmel, melyből kiderül, **milyen előnyök származhatnak abból, ha valaki kilép a Facebookról**. Például **felszabadul egy csomó időnk**, ami alatt korábban elágazó itálkeverékek kortyolgatása közben a biztonsági beállításainkat módosítottunk napi-heti rendszerességgel.



Filozófiai értelemben valószínűleg **egy ilyen szimpla kilépés kevés a boldogsághoz**. A klasszikus mondás szerint: "Ha boldog akarsz lenni egy napig, rúgj be! Ha boldog akarsz lenni egy hónapig, házasodj meg! Ha egész életedben boldog akarsz lenni, kertészkedj!" De az szinte tuti biztos, hogy a mondás egyáltalán nem a Farmville-re gondolt :-))

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)

- [Kártékony vírusok - villám őrjárat 8.](#)
- [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/2397332>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Néha még kémprogram sem kell

2010.10.27. 15:35 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [személyes elveszett adatok abszurdisztán orvosi adathordozó](#)

Elég, ha szabályozatlan, vagy csak ellenőrizetlen az adatkezelés, és ráadásul következmények nélkül marad minden elkövetett hiba: akkor [az emberi tényező rendre megmutatja](#), mire is képes.



Újra, ismét, megint "elvesződött" egy rakat bizalmas, személyes adat. [280 ezer ember neve, pontos címe, részletes egészségügyi adata tűnt el egy hordozható adathordozó elvesztése kapcsán](#). A felelős cég természetesen mélyen megdöbben, erősen sajnálja a "szerencsétlen esetet" és természetesen mindent megerősít, mindent megtesz, hogy a jövőben ne fordulhasson elő ismét ilyen. Miért nem kell inkább hetvenháromezer-nyolcszáznegyvenöt-ször leírnia egy 8H-s ceruzával, hogy "bizalmas adatok kezelésére titkosítatlan adathordozót nem használok, különben törjön le a kezem", vagy valami hasonló? Vajon örök időkre kigolyózzák majd őket abból a körből, akik jogosultak egészségügyi adatok kezelésére, vagy csak azt mondják: pardon, és ezzel részükről minden rendben?



Ha figyelembe vesszük, hogy egy számítógép kártevővel való támadásának mostanában jobbára két fő célja lehet: vagy egy botnet részévé akarnak tenni minket, vagy csendben személyes adatainkat, jelszavainkat akarják ellopni róla. Ez ellen mindenki odafigyelése, pénztárcája, szakmai tudása, lehetőségei szerint igyekszik valamit tenni, és jól-rosszul, megoldja saját gépe védelmét. **Am amikor az egészségügyi, adóhivatali rendszerben szereplő adatainkról van szó**, azt gondolnánk, ők profik és [ebből élnek, ezért mindenkinél jobban tudatában vannak annak, mi a feladatuk](#), és azt hogyan tegyék.



Itt a blogban már [számtalan elveszett laptop, adathordozó](#), nem ritkán kormányzervek tulajdonában lévő eszközök rajta **kényes adatokkal való elvesztéséről számoltunk be**. Persze Murphy-vel szólva "ami elveszhet, az el is veszik" - na jó, ez azért persze barokkos túlzás, meg nincs is így jól. De ha viszont azt a logikát követjük, hogy egy gyanúsított azért kap börtönbüntetést, mert [megtagadja a nyomozás során a saját számítógépén található titkosított fájlrendszerhez tartozó személyes jelszó megadását](#) a hatóságoknak, akkor a hivatásos adatkezelő esetében a kötelező titkosítás elmulasztása miért nem jár hasonlóan súlyos következményekkel a felelősökre nézve?



Persze annyit azért mindenképpen hozzá kell tenni, amit Jakab Péter említett az ITBN-en: **már az is pozitív, ha valahol legalább beszámolnak a bekövetkezett biztonsági incidensekről**. Mert eközben ugye [a mi országunkban egész pontosan nulla ilyen](#) történik ;-)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Ez történik a weben egy perc alatt](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2402484>

Kommentek:

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

Sixx! Anyádat is nyuggernek hívod? • **<http://orbanfan.blog.hu> 2010.10.30. 17:40:56**

Jakab Péter... Miközben az új bankkártyát úgy küldik az ügyfélnek, hogy berakják a szabványos banki borítékba, a postás meg egyszerűen behajítja a postaládába. És amikor ezt szóváteszem neki (miután személyesen is van szerencsém ismerni), még csak nem is válaszol.

Sixx! Anyádat is nyuggernek hívod? • **<http://orbanfan.blog.hu> 2010.10.30. 17:44:34**

Egyébként ehhez már lehet, hogy gyenge az angolom, de... miből derült ki, hogy az elveszett drive nem volt titkosítva? A hivatkozott cikkben nem láttam semmi erre utaló szöveget.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> **2010.10.30. 19:11:20**

Buona sera!

A hivatkozott cikkben ilyen nem szerepel, de van az a klasszikus vicc, miszerint ha egy úrinő azt mondja: nem, az azt jelenti hogy talán. Ha azt mondja talán, az az jelenti hogy igen. Ha pedig azt mondja igen, akkor nem is úrinő. Van ez egyébként politikussal.

Szóval ha lett volna erős titkosítás, akkor az szerepelne a nyilatkozatokban, dicekednének vele, hogy szerencsére semmilyen veszély nem fenyeget. Ha viszont nagy kuss van, meg az hogy mindent megtesznek, hogy a jövőben hasonló eset ne fordulhasson elő, akkor 99%, hogy nem volt titkosítás. A tolvaj clear textben olvassa a cuccot, és éppen alkuszik rá, mennyi pénzt kérjen érte.

Még régen volt hasonló szleng, mikor az úrhajósok mentek a Holdra, és ha a rádióban azt mondták, kitűnően vannak, az azt jelentette, hogy jól vannak. Ha azt mondták, az úrhajósok állapota kielégítő, akkor még éppen nem haltak meg, volt pulzusuk ;-)

Most jön a Java

2010.10.29. 18:18 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [linux java macintosh trójai botnet koobface](#)

Nem volt egy eseménytelen hét. Először jött a nyitott Wifi hálózatokban [Facebook és egyéb accountokat arató Firesheep Firefox kiegészítő](#), most pedig egy **Java** cucc borzolja az idegeket: tudja ez lovon és trapézon is, Macen meg Linuxon.



[A Koobface Boonana a Java egy hibáját kihasználva terjed már nem csak Windows, hanem Macintosh és Linux platformon is.](#) Persze kattintani kell, elfogadni, engedélyezni a futtatást az állítólagos Photo Albumnak. Aki nem szokott nyakra-főre trójaikat simán benyelni, például az, [aki az állítólagos hiányzó Mac videokodeknél is észnél volt](#), annak kevésbé ijesztő. [Macintosh és Linux alatt is engedélyt kér a Javas dolog](#), vagyis konkrétan **benézni, appletet bambán engedélyezve kattintani kell a lefuttatásához**.



Egy Translate Google segítségével olvasható spanyol blogbejegyzés még egy [Ubuntu alatti Koobfacet is megmutat](#) Wiresharkban. Bár állítólag a Windows verzióval szemben a Mac és Linux kártevők még nem nevezhetők teljesen kész változatnak, a [Securemac cikke szerint botnet veszély fenyegeti a Macs gépeket és egy ingyenes eltávolító eszközt is közreadtak](#).



Ha valaki Facebookozik, és mondjuk **jó esetben még van is neki NoScriptje**, akkor is az a valószerű, hogy arra az URL helyre stabilan engedélyezte a scriptek futását, vagyis még így is veszélyben lehet. Minden jel arra mutat egyébként, hogy [a Java a rengeteg sérülékenysége miatt egyre vonzóbb kártevő célponttá](#) válik.



Elképzelhető, hogy [most adódott egy olyan alkalom](#), ami miatt lassan elkezdik jobban zaklatni az alternatív platformok az eddig nyugodalomban lévő felhasználóit is, bár **önmagától automatikusan lefutó kódot még szerencsére nem láttunk**, kíváncsian várjuk a fejleményeket. Addig is [egy kis tudatmódosító olvasnivaló](#), [Kell-e antivírus Macre?](#) munkacímmel.

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

 Megosztás  +1  Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Kártékony vírusok - villám őrző 8.](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [A kiknek a Captcha kényszerűsége](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2408295>

Kommentek:

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

Nincsenek hozzászólások.

Az év legkreténebb ötlete

2010.11.02. 14:05 | [Csizmazia István \[Rambo\]](#) | [4 komment](#)

Címkék: [usb kulcs](#) [new york](#) [dead drops](#) [falban](#)

Mint az közismert, (Cincinatus több száz éve halott, történelmi alak, akit miután visszavonult a közéletből, az eke mellől hívtak vissza a szenátusba, továbbá) **közös lónak túros a háta**. Nem is beszélve a közösen használt óvszerről, vagy a többszörhasználatos közös fecskendőről. Valami hasonlót álmodott meg most a korszakalkotó "művész": a Markos-Nádas duó "[Kőbe zárt lélek](#)" nyomán íme itt a **kőbe zárt USB kulcs**.



Az ötlet eredetileg talán a [geocaching](#) egyfajta utánérzésének két sör utáni művészi házasítása valamiféle Dropbox lehetőséggel lenne. **Urbánus Ubul metroszexuális városlakó hordozható gépével ugyebár "kényelmesen" felcsatlakozik** a házfalba bebetonott USB kulcsra, majd egy laza csuklómozdulattal **begyűjti az eddig számára ismeretlen és hónáhított fertőzéseket, kártevőket**, majd a magasból szól vala az Úr hangja: "Szaporodjatok, sokasodjatok!"



Ez a kártevő és kémprogramterjesztőknek kimondottan jó lehetőség lenne, igaz szerencsére egyelőre kis volumenben működik. Bár ki tudja, ha a Mester mer nagyot álmodni, a [blogja szerint ez még csak a kezdet](#).



Ha csak a közelmúltban lezajlott Stuxnet főrege gondolunk, **ott a még azok a Windows-os gépek is megfertőződtek a külső USB eszközön keresztül egy biztonsági rés miatt, amelyeknél le volt tiltva az automatikus futtatást biztosító Autorun funkció**. Ahhoz hogy ezt a Dead Dropsot egy épeszü ember igénybevegye, [ahhoz nem konspiráltan üzengető Abigélnek kell lennie](#), hanem sokkal inkább shanghai táncosnő legyen az öreganyánk, és baltával pucolja az ablakot. **Még egy évet se kell visszamenni az időben, hogy a [fotókidolgozásra kihelyezett automaták által terjesztett](#) vírusokra kegyelettel emlékezzünk**.



Kár, hogy már kiment a divatból a [vigyünk operát az őserdőbe vagy a húzzassunk át egy gőzhajót a hegyen](#) a benszülöttekkel performance, így nekünk most be kell érünk helyette ezzel az USB-s dologgal. Ha figyelembe vesszük, hogy vannak emberek, [akik képesek heti 3000 forintot fizetni SMS-ben "ingyenes MSN"](#) használatért (meg olyanok is vannak, akik ezt a pénzt pofátlanul elkérik), **biztosan lesz erre is megfelelően divatos és trendi érdeklődés**.



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



Tweet

Ajánlott bejegyzések:



- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2415397>

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](#).

[vrtx 2010.11.02. 14:07:37](#)

Tudtommal nem "közös lónak túros a háta", hanem túros a háta a mondás szerint. (Nem kötekedésből írom...! :))



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.11.02. 15:07:44](#)

Szia Vrtx!

Köszí szépen, javítottam :-)

[44 2010.11.05. 00:45:18](#)

Komolyan mondom, gyűlölöm ezt a blogot, mert érdekes címeket adsz, rákattintok, azt hiszem, hogy valami értelmes tartalom jön be, és nem. (Viszont a képek jók.)

Az egy dolog, hogy a közösen használt eszközökön több a vírus, de az meg egy másik, hogy ezzel ki törődik. Ilyen alapon fel se keljünk az ágyból, tudod. Minden USB-használat, minden internethasználat, minden nem tiszta forrásból származó program vírusveszélyt jelent, ezzel megtanultunk együttélni. Az, hogy valami művész most pendrive-ot épít be a falakba, ettől tökéletesen független dolog. A kettőt egybemosni az év legkreténebb ötlete, valóban.

Amíg egy tetszőleges internetes oldalon én vírusveszélynek teszem ki magam, és amíg rengeteg pénzt fizetek a vírusirtóért, addig nekem eszembe sem fog jutni egy ilyen kezdeményezésről rögtön a vírusokra gondolni. Ez már neked is csk munkahelyi ártalom, mert a veszély itt sem nagyobb, mint bármilyen más közösségi helyen. Sőt, ha nem használják őket, ami voltaképpen várható, akkor még kisebb is, mint máshol. Ez inkább a digitális és a valódi világ megkülönböztetésére való rámutatás. Vagy bármi más.



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.11.05. 09:12:59](#)

Szia 44!

Isten hozott a blogon :-)

"a közösen használt eszközökön több a vírus, de az meg egy másik, hogy ezzel ki törődik"

Az óvatosság szerintem napi szükséglet. Aki az adatait nem szeretné közpredává tenni, azoknak azért kellene törödni.

"Amíg egy tetszőleges internetes oldalon én vírusveszélynek teszem ki magam, és amíg rengeteg pénzt fizetek a vírusirtóért, addig nekem eszembe sem fog jutni egy ilyen kezdeményezésről rögtön a vírusokra gondolni."

Egyetlen korrekt vírusirtó sem ígér 100%-os védelmet, mert ilyen nem is létezik. Megóv sokmindentől, de ha például zárat vesz a lakásod ajtajára, az sem garantálja 100%-ban, hogy bár fizetted a zárért, sosem törhetnek be. De persze jobb, ha van egy jó zár, mintha minden tárva-nyitva lenne.

"Ilyen alapon fel se keljünk az ágyból"

Lehetnek egyébként jók látszó ötletek, például nézem az Animal Planetet, nagyon szeretem az állatokat, de vannak dolgok, amik mégis rosszul sülnének el, és hasznos lehet, ha előtte képben vagyunk, valamit olvastunk róla, pl.

mek.niif.hu/01000/01028/01028.htm - Rejtő: Elveszett cirkáló című etológiai szakmunka:

"Ezek után úgy jártunk volna, mint az a bizonyos félhülye úr aki viperát talált a hóban, és mert nem foglalkozott soha állattannal, keblén melengette az illető csúszómászót."

De gondolhatom úgy is, a sok öltönyös politikus sosem csinál semmi jót, csak dumálnak, majd én megoldom, elmegyek Afrikába, és ételt osztok sajátkezűleg. Amikor azonban elindul a kiosztás, és a szerencsétlen éhezők valósággal megrohanják a teherautót (tegyük fel, hogy élve, megcsónkítás és elrablás nélkül megérkeztünk), akár a testi épségünk, vagy az életünk is veszélybe kerülhet (az úgy gondoltam, azt hittem sokszor egész más, mint a valóság). Ha előtte egy a térséget jól ismerő biztonsági tanácsadót, aki már sok ilyenben részt vett, megkérdeztünk volna, biztos adott volna olyan instrukciókat, amelyekkel minimalizálhattuk volna a kockázatokat.

Szerintünk azért hasznos ez a blog, mert ilyen infokra hitünk szerint minden számítógéphasználónak szüksége lehet, nem csak az érdeklődőknek. Felhívja a figyelmet a gyenge pontokra, a lehetséges kockázatokra, és sokszor jönnek elő olyan dolgok, hogy "Jé, hát nem is gondoltam volna, hogy a jelszóemlékeztető kérdéssel ilyen lehet.", vagy "Jé, nem is gondoltam volna, hogy egy routerben lévő memóriába is lehet kártékony kódot feltölteni.", vagy "Jé, nem is tudtam, hogy minden eszköz alapértelmezett jelszava egy nagy nyilvános adatbázisban szerepel a neten, és azt bárki olvashatja". Abban persze tökéletesen igazad van, hogy mi sokmindent ezen a speciális "szemüvegen" keresztül nézünk, és "mindenről ez jut az eszünkbe", de hát ezért írják az ilyen cikkeket IT biztonsági szakemberek, és nem balett táncosok vagy kőfaragók.

Mindazonáltal folyamatosan igyekszünk nem szakbarbárnak lenni, és reméljük, sosem leszünk ilyenek :-)

"Tengerészek barkochbáznak. Szörös? Nem. Akkor rum."

Ahol a Vistát még tényezőnek gondolják

2010.11.04. 14:45 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [vista](#) [hamis](#) [2010](#) [antivirus](#)

Ha megnézzük akár a [saját blogos szavazásunkat](#), vagy éppen a [w3schools logjaiból nyert](#) aktuális információkat, a Vista inkább csak a futottak még kategóriára predestinált.



Egyszer már jól megvitattuk azt a jó kis felismerést, hogy milyen **tuti ötlet volt a Windows Antivirus XP-nek nevezni egy hamis vírusirtót** azon a piacon, ahol az XP toronymagasan vezette az oprendszerek versenyét. Ám azt is számításba kell venni, hogy az új fenyegetettségek soha nem a régiek helyett, hanem velük együtt, mellettük párhuzamosan jelennek meg. Ezért aztán [jelennek meg rendre egyre újabbak és újabbak](#).



Ha mostanság nézzük az adatokat, jól látszik, hogy nyár végén-ősz elején nálunk már szépen átvette a vezetést a Win7 az XP-től. Ezért a kiberbűnözők ha már kattintásra vágytak, inkább lehetett volna a neve Antivirus Windows7 2010 is, de az majd biztos csak a jövő héten lesz aktuális ;-)



Mindenesetre se realitás-, se üzleti érzéke, se pedig mentsége nincs annak, aki az Antivirus Vista 2010-et és a Vista Antispyware 2010-et elkövette, így remélhetjük, a szokásos 5% bedőlő palimadarat ezzel a névvel már nem biztos, hogy ki lehet fogni :-)



Az ilyen, és hasonló nevű bekapott fertőzéseket egyébként szokás szerint [nem egyszerű levakarni](#), ezért ehhez általában [különböző részletes egyedi útmutatók](#), valamint [eltávolítási segédesszközök](#) állnak rendelkezésre.



Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Utaltunk pénzt a S.O.C.A.-nak](#)

- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2422905>

Kommentek:

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

Nincsenek hozzászólások.

Nem adja a trónját a Conficker

2010.11.05. 12:31 | [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. **Az októberi magyar lista első helyét már 2009 októbere óta - azaz éppen egy esztendeje - az a Conficker féreg tartja**, amely az operációs rendszer frissítéseinek hiányát, a gyenge jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed.



A nagy számú fertőzésnek az is az oka lehet, hogy folyamatosan számtalan új variáns, módosított változat jelenik meg belőle, melyeknél a készítőik rendre igyekeznek tesztelni és kizárni a felismerést, valamint sok Windows alapú számítógépen nem fordítanak elég figyelmet a naprakész vírusvédelem mellett az operációs rendszer frissítéseire is.



A trójaik döntő fölénye továbbra is igen látványos, tízből hét. Mint ismeretes, a trójai faló – melynek történetét a görög regékből ismerhetjük – egy olyan program, ami valami mást csinál, mint amit magáról eredetileg állít. Ez a más nem minden esetben okvetlenül romboló vagy káros, de sok esetben igen: fájlokat törölnek, felülírják a merevlemez, vagy távoli hozzáférést biztosítanak a rendszerhez a támadónak. **A klasszikus trójai általában tartalmaz egy billentyűleütés naplózót (keylogger) is**, amelyet készítői játéknak vagy valamilyen hasznos segédprogramnak álcáznak. Az ilyen trójakat sokféle céllal alkalmazhatják: rejtett távoli (backdoor) elérést szeretnének biztosítani egy adott számítógéphez, ellenőrizni kívánják a billentyűleütéseket, valamint jelszavak lopására specializálódnak (a legtöbb kémprogram ez utóbbi kategóriába esik).



Helyet cserélt októberben a korábbi harmadik és negyedik helyezett, így ezúttal az előkelő **harmadik helyen találjuk a Win32/PSW.OnLineGames trójait**. 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.

Negyedik lett a HTML/ScrInject trójai, amely egy RAR segédprogrammal tömörített fájl, és települése során egy üres (c:\windows\blank.html) állományt jelenít meg a böngészőben a fertőzött számítógépen. Hátsó ajtót is nyit a megtámadott rendszeren, és ezen keresztül **további kártékony JavaScript állományokat kísérel meg letölteni és lefuttatni a háttérben**. A nyolcadik helyre lépett előre a **Win32/Mebroot trójai**, ami egy igen kellemetlen kártevő, hiszen törölheti a merevlemez partíciós tábláját, és így könnyen adatvesztést okozhat.



Egyetlen újoncnak sikerült csak felkerülni a lista tizedik helyére, így is egy trójai helyébe lépett egy másik trójai. **A JS/TrojanDownloader.HackLoad trójai saját kódjának telepítése során HTML állományokba írja bele rövid, mindössze 76 bájtos kódját**. A HTML állomány megnyitásakor a megtámadott számítógépről különféle weboldalakhoz kísérel meg csatlakozni, azokról pedig további kártékony kódokat tölt le.

Vírustoplista - 2010 október

Az ESET **több százezer magyarországi felhasználó visszajelzése**in alapuló statisztikai rendszere szerint 2010 októberében a következő

10 károkozó terjedt a legnagyobb számban, és volt felelős együttesen az összes fertőzés 20.75%-ért.



1. Win32/Conficker féreg

Elterjedtsége az októberi fertőzések között: 5.68%

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 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 az októberi fertőzések között: 3.44%

Működés: Az INF/Autorun egyfajta 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>



3. Win32/PSW.OnLineGames trójai

Elterjedtsége az októberi fertőzések között: 2.23%

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 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. HTML/ScrInject trójai

Elterjedtsége az októberi fertőzések között: 2.22%

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/scriinject-b-gen>



5. Win32/Tifaut trójai

Elterjedtsége az októberi fertőzések között: 1.79%

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>



6. Win32/VB féreg

Elterjedtsége az októberi fertőzések között: 1.46%

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 októberi fertőzések között: 1.35%

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/Mebrook trójai

Elterjedtsége az októberi fertőzések között: 1.06%

Működés: A Win32/Mebroot.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 particiók tábláját.



A számítógépre kerülés módja: A felhasználó maga telepíti.

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



9. Win32/KillProc trójai

Elterjedtsége az októberi fertőzések között: 0.84%

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>



10. JS/TrojanDownloader.HackLoad trójai

Elterjedtsége az októberi fertőzések között: 0.68%

Működés: A JS/TrojanDownloader.HackLoad trójai saját kódjának telepítése során HTML állományokba írja bele rövid, mindössze 76 bájtos kódját. A HTML állomány megnyitásakor a megtámadott számítógépről különféle weboldalakhoz kísérel meg csatlakozni, azokról pedig további kártékony kódokat tölt le.



A számítógépre kerülés módja: A felhasználó fertőzött weboldalt nyit meg vagy maga telepíti.

Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/trojandownloader-hackload-ad>



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés traceback címe:

<http://antivirus.blog.hu/api/trackback/id/2423706>

Kommentek:

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

[Vakonlátó](#) • <http://baloghrobert.tk> 2010.11.06. 17:33:44

Elképeztő, hogy mennyire felelőtlenek az userek.

Kiss Ádám és vírusok

2010.11.08. 18:40 | [Csizmazia István \[Rambol\]](#) | [7 komment](#)

Címkék: [játék](#) [tánc](#) [kiss](#) [security](#) [smart](#) [ádám](#) [eset](#) [vírusvideó](#)

Ádámnak megfertőződött a számítógépe - pedig mikor megvette, nem is kért hozzá külön vírusokat ;-). Aztán keresett valakit, aki meg tudja tisztítani. Hozzánk fordult, **mi pedig megkértük, mondja el, mit gondol a vírusirtókról.**



A négy és fél perces film alacsony költségvetéssel készült házi videó, mely a komikus új laptopjának történetét meséli el, majd a végén táncra is perdül.



Az alkotás Kiss Ádám és a vírusok címmel került fel a YouTube-ra, és a www.youtube.com/esetmagyarország címen megtekinthető. Ha azt gondolod, [te is tudsz úgy táncolni, mint Kiss Ádám](#), próbáld ki magad! Töltsd le a NOD32 dalok egyikét, és vedd fel, ahogyan táncolsz rá.

- [The NOD Song](#)
- [Winning The World Over](#)
- [Infected](#)

Az eredményt töltsd fel a YouTube-ra, és a linket küldd el nekünk a tanc@eset.hu e-mail címre!



Szavazni a www.facebook.com/kikapcsolodas oldalon lehet, a legtöbb szavazatot kapott 5 táncos pedig mostantól minden hónapban 3 éves ESET Smart Security licencet kap - egészen a játék végéig.



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



Ajánlott bejegyzések:

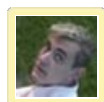
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- ["Szösölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2434063>

Kommentek:

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



[mrlujoak 2010.11.08. 20:09:57](#)

Hopika, Sony Ericsson C902-vel nyomja Ádi? Szuper.

[indust • http://indust.hu 2010.11.09. 07:50:52](#)

Ha még pólót vagy csokoládét is adnának, oké, de egy ilyen licensz olyan kevésbé kézfogható..



[prof. Perselus Piton 2010.11.10. 07:16:10](#)

Szia Rambo és többiek :-))

Nem a témához tartozik, de nem jutott jobb hely az eszembe...hármán is írták, hogy működik ez a link és látják, hogy ki járt náluk:

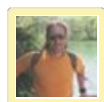
iwiwapp.blogger.hu/tag/iwiw_who_view_ki_nezett_meg

én nem merem megnézni, mert vírusfóbiám van :-)) de kíváncsi lennék a véleményedre, pláne, hogy mindhárman letoltak, mikor a linkre betettem nekik válaszul ezt a cikket:

hiszedmi.blog.hu/2010/10/29/iwiw_ki_nezi_a_profilomat

én a nem működikre tippelek (szerintem csak a hozzászólásomat jelezte a linkre és nem emlékszem, hogy jártam-e náluk ténylegesen) és ha igazam van, szeretném tudni, mi benne az átverés (ingenyreklám, stb.)

Köszönöm előre is, ha utánanézel :-))



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu 2010.11.10. 09:48:35](#)

Szia prof. Perselus Piton!

Nem ismerem konkrétan ezt az alkalmazást, de most megnéztem. Képernyőképek itt:

kepfeltoltes.hu/101110/iwi1_www.kepfeltoltes.hu_.png

kepfeltoltes.hu/101110/iwi2_www.kepfeltoltes.hu_.png

kepfeltoltes.hu/101110/iwi3_www.kepfeltoltes.hu_.png

Elvileg a javascriptek világában sok minden lehetséges, anno például az Iwiw szigorúan örködött, nehogy le tud menteni a kapcsolataidat, de volt azért rá okosság:

benjamin.hu/2007/11/15/export-tool-iwiwhu/

Visszatérve az eredeti kérdésre, én nem hiszem, hogy ezt csinálná a program, talán a reklámok miatt csinálhatják, és az ajánlatott keress munkanélkül pénzt kattintással Buxta ajánlat sem volt túl bizalomgerjesztő. Ha már egy leírásához odairják: "EZ NEM ÁTVERÉS!", akkor biztos az :-). Az újságírósdiban van egy hasonló okosság: "Ha a cikk főcíme kérdőjelre végződik, akkor az biztosan nem igaz"

Szerintem a biztonság egy bizalmi kérdés, és ebben fontos helye van a "Mit telepítek" és "Honnan, kitől telepítek" kérdéseknek. Mivel vírust felismerni könnyű, trójait felismerni nehéz, és ez utóbbiak hihetetlen mértékben elszaporodtak, jó hozzáállás, ha csak megbízható, ellenőrzött forrásból telepítünk bármit. Még ennek ellenére is lehetnek balesetek (fertőző vagy tolvaj applikációk a Facebookban vagy App Storeban), de ott legalább látványos következménye van, és idővel orvosolják. Ha mondjuk lenne egy komoly antivírus cég, és a honlapjukon email lottót is látnál, meg egy felhívást, hogy emellett kulcsmásolást és teniszütőhegy másikúrozást is vállalnak, az ugye komolytalan :-)

Még az ingyen kattintással való pénzkeresethez egy kis adalék, itt egy fórum, ahol kergetik az emberkék az elveszett könnyűs pénzkeresetes pénzüket egy másik bombabiztos lehetőség és befizetett pénz után, érdemes beleolvasni, és tanulni belőle:

www.hoxa.hu/?p1=forum_tema&p2=45523



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu) **[2010.11.10. 09:50:07](#)**

Másfelől a bizalmi kérdés nálam úgy is jelentkezik, ha előbb kell elfogadnom a licencszerződést, előbb kell látatlanban lájkoljak valamit, amikor még nem is tudom mi az, és majd csak utána tölthetem le, akkor kenjék a hajukra. Nálam ez úgy logikus, előbb pontosan megnézem mi az, és ha akarom, lájkolom, ha akarom megadom elérhetőséget, ha akarom, beírom hogy Malyomváry Armandó, Malyomfalva, lo@lo.lo, stb szemetet. Ha pedig hosszútávon tényleg meg van a bizalom, akkor adom csak meg a valódi személyes adataimat és nem akárkinek.

Most divat ez az előre lájkolom, előre megbízom benne, előre elfogadom és megosztom az összes ismerősömmel, majd utána láthatom meg pontosan, hogy mi is a játék, lásd "Az emberek 98%-a nem tudja 17 másodpercnél továbbnézni ezt a videót" esetet:

antivirus.blog.hu/2010/08/16/dr_gany_es_fusher_professzor_modszere

Szóval én a helyedben kihagynám, persze csak a fentiek nem csináltak neked kedvet hozzá :-)



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](http://antivirus.blog.hu) **[2010.11.10. 09:52:22](#)**

Sorry, kopipészt error:

teniszütőhegy másikúrozást = teniszütőhúrozást



[prof. Perselus Piton 2010.11.10. 19:00:13](#)

Köszönöm a részletes választ...és a szokásos, székéből kiesős nevetést, ami minden írásodnál előtör belőlem (valaki fakutya lehetett a felmenőim közt)...

De hiába, nem jött meg a kedvem a kipróbáláshoz :-)) továbbra is maradok a megérzésnél, ha pedig az nem elég, akkor majd megint fárasztalak téged :-))

Viszont csinálhatnál ebből egy gyors cikket, amit belinkelhetnék (és gondolom, mások is) az ismerősöknek...

A teniszütőhegy másikúrozás pedig igenis egy nagyon jó témaa :-PP

Köszönöm még egyszer a választ, további szép estét!

Luke Skypewalker

2010.11.10. 14:25 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [apple](#) [skype](#) [iphone](#) [engedély](#) [telefonhívás](#)

Nitesh Dhanjani észrevételeire **mindig érdemes odafigyelni**. Ő volt az, aki annak idején az emlékezetes [Safari Carbet Bomb](#) [sebebevezetőségéről is beszámolt](#). Most az Apple IOS kapcsán tett **érdekes felfedezést a weboldalakba ágyazott Skypehívásokkal** kapcsolatban.



Elvileg ha találkozunk egy akármilyen indulatú weboldalon egy olyan kóddal, amiben szerepel egy hívás, pl. "<iframe src='tel:1-408-555-5555'></iframe>", akkor az a normális működés, hogy **feljön egy ablak, ami nagyon helyesen engedélyt kér**. És akkor választhatunk a hívás vagy a mégse között, ami pedig **a leglényegesebb, kattintás nélkül nem történik semmi**.



Innentől kezd érdekes lenni a történet, ugyanis **ha a telefonra már telepítve van a Skype alkalmazás**, és a megintcsak ki tudja milyen indulatú weboldalon pedig az alábbi kód található: "<iframe src='skype://14085555555?call'></iframe>". [Ekkor ugyanis a Safari rákérdezés nélkül, azonnal elindítja a hívást](#).



A biztonsági szakértő **már kapcsolatba lépett az Apple fejlesztőivel, valamint a Skype csapatával is**, és jelezte nekik a problémát. A hibát nagyvalószínűséggel az Apple-nél kell majd valahogy orvosolni, [a történetben szereplő Skype ugyanis csak egy példa](#) arra, hogy **bármilyen harmadik fejlesztő fél által készített alkalmazás felülbírálhatja a Safari alapértelmezett engedélykérős beállításait**.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [Az XP élt, az XP élt, az XP élni fog](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szösölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [Mai szavunk pedig: keyjacking](#)



A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2437951

Kommentek:

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

Nincsenek hozzászólások.

Az asszony a világ négere

2010.11.12. 14:05 | [Csizmazia István \[Rambol\]](#) | [12 komment](#)

Címkék: [oktatás](#) [csalás](#) [képzés](#) [védekezés](#) [számítógépes](#)

Énekelte egykor [John Lennon egy dalukban](#), egy egészen [más kontextusban](#). Egy nemrég lezárult kutatás eredménye azt mutatja, hogy a nők látszólag jóval nagyobb eséllyel esnek áldozatául a különféle nigeriai és egyéb számítógépes csalásoknak, mint férfitársaik.



A mintegy kétezer résztvevőt felölelő felmérés, amelyben a számítógépes csalások minden formáját vizsgálták - spam, hamis árúk, közösségi oldalakon való hamis profilok és egyéb social networking megtévesztések - azt mutatta, hogy [a 25-34 év közötti hölgyek bizonyultak a legnaivabbnak](#).



Nos kutatás ide, eredmény oda, a konklúzió talán kissé elszórttá tűnik, a dolog valószínűleg nem ilyen egyszerű. Azt viszont biztosan kijelenthetjük, hogy **nemtől függetlenül mindenkire ráfér az alaposság, biztonság tudatos óvatosság és a gyanakvás**, és a felkészítés, rendszeres oktatás adja ehhez a kulcsot az emberek kezébe, hogy megértsék, mire és miért kell vigyázni. Például a nyitott wifik száma is mintha az utóbbi időben csökkenne a magánemberek esetében, akik [mintha kezdenék megérteni a problémát](#). Ellenben néhány céges helyen - például ügyvédi irodákban, autókereskedésekben - mintha még mindig nem fordítanak megfelelő figyelmet ennek fontosságára.



Szoktuk mondani, hogy **fusson a gépeken a naprakész biztonsági program, frissítsük rendszeresen az alkalmazásokat és az operációs rendszert**. És persze egyre jobban igaz az ["Az vagy, amit telepítesz"](#) is, magyarul nagyon érdemes megválogatni és odafigyelni arra, hogy **csak megbízható forrásból származó, megbízható programokat telepítsünk**. [Ez néhol viszonylag egyszerű](#): például ha Macintosh esetén csak az Apple Store-ból, Linux esetén pedig csak a hivatalos tárolóból származókat választunk.



Ugyanez viszont már **nem ilyen egyszerű a Windowsnál és mondjuk olyan applikációknál sem, mint az Androidos okostelefonra vagy Facebookon választható alkalmazások esetében**. Ekkor az alapos utánajárás, Google keresés, a gyártók háttérének vizsgálata, a licencszerződés alapos átolvasása adhat némi támpontot. Ám a gyanakvásnak nem kell, sőt nem is szabad itt megállnia, **ahogy egy megfelelő biztonsági szoftver kiválasztása is bizalmi kérdés, az igénybevett számítógépes szervíz kiválasztásánál sem szabad kizárólag a fizikai közelséget és az olcsóságot preferálni a megbízhatósággal szemben**. Ellenkező esetben könnyen [horrorisztikus családi végkifejletek alakulhatnak ki](#).



Hogy a felmérésben vázolt helyzet nemektől függetlenül is megváltozzon, ahhoz nyilván sok minden kell. Mindenesetre **első helyen a**

megfelelő szintű és rendszeres képzés áll, de a már [gyerekkortól kezdődő biztonsági oktatás](#) is felülmúlhatatlanul [fontos - lenne](#).

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

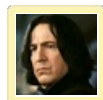
- [A PRISM szeme mindent lát](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2443838>

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 [Felhasználási feltételekben](#).



[prof. Perselus Piton 2010.11.12. 19:57:14](#)

A gyerekkorban kezdett biztonsági oktatás nálam esélytelen volt, mert akkoriban még szobaméretűek voltak a számítógépek :-)) vagy tán háznyiak?

De a nigériai cuccnak bedőlőknél talán nem a biztonsági oktatás, hanem az IQ hiányos, nem? :-PP



[Emmet Ray 2010.11.12. 23:16:40](#)

prof. Perselus, mielőtt valaki lecsapja a labdát, jelentkeznek: a végkövetkeztetés, hogy a nők IQ hiányosak. Mit nyertem?

[medvetoka 2010.11.13. 00:25:08](#)

Az összes antivírus program szar, lassítja a gépet. Ha meg negyedévente a biztonság kedvéért lefuttatok egy 30 napos próbaverziót, az nem talál semmit.

Most akkor miért is kellene nekem biztonsági program? Miért ekkora a veszély?

Egyszerűen nem kell rákattintani a your_wife_naked.zip-re, meg az "Ön a 999.999-ik látogató"-ra, valamint használni kell a router tűzfalát.

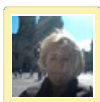


[flugi_ • http://fundi.blog.hu/ 2010.11.13. 02:57:59](#)

csak én nem értem a szabad wifi "kockázatát"? Azt odáig értem, hogy az államnak jól jönne egy biztosabb számonkérhetőség, de nekem miért lenne buli? Főleg, ha nem olyan ótvar szolgáltatónál vagyok, amelyik gyanúsításra dobja az ügyfelet?

[Frengi • http://frengi.blog.hu/ 2010.11.13. 06:38:22](#)





Gyanítom, hogy ezeket a vírusokat a vírusirtó cégek gyártják, különben ki adna 40€ a McAffyért 60 napra?

Réka • <http://rekafoto.com/blog> 2010.11.13. 10:03:10

@Frengi: akkor a McAffy helyett használj McAfee-t, az egy évre és 3 gépre kb 30 font. :)



prof. Perselus Piton 2010.11.15. 16:40:42

@Emmet Ray: ez így, ebben a formában nem igaz (ezt valami kabarében mondták, de nem emlékszem, melyikben)...

Szóval a nők nem buták, csak mindenhez érzelmi alapon közelítenek, ezért gyakran összetűzésbe kerülnek a logika szabályaival :-))) (ezt meg én mondom, nőként, 150-es IQ-val)

Tehát nyertél...ha a név ellenére te is nő vagy,akkor egy kritikát, ha mégis férfi, akkor a tudatot, hogy ezen nők bármelyikének áldozatául eshetsz :-)))



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.11.17. 10:22:47

Szia Flugi !

Csak egy apró érdekes adalék nyitott wifihez. Ha például tehetséges programozó vagy, minden évben megnyered a Hack the Vendort, naponta töröd a Nasa weblapját, a MiTM a kisujjadban van, aztán ha valami eseménnyel gyanúsítanak az otthoni nyitott wifis otthoni géped kapcsán, hiába védekezel, nem fogják életszerűnek ítélni, ha azt állítod, biztos más, valamilyen rossz csúnya idegen bácsi csinálta :-)

Egyetértek veled abban, hogy a feltételezett számonkérhetőséget hozod fel, vannak országok, például a németek, akik már büntetik:

index.hu/tech/biztonsag/2010/05/14/nemtorszagban_megbuntetik_azt_aki_nem_vedi_jelszoval_a_wifijet/



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.11.17. 10:27:11

Szia Medvetoka!

Ha pluszban fut még egy program a gépen, akkor gyorsítani nem tud rajta. Abban mélységesen igazad van, hogy sokan tudnak, vagy tudnának óvakodni a "naked pamel anderson.zip" és hasonló csalafintaságoktól. De trójai meg social engineering trükk sok van, ha például szabálytalan parkolásról, kézbesítetlen futásomagról van szó, azonnali adóvisszatérítésről, sokan kattintanak. És van ugye még a testreszabott dolog, amikor elolvasság a Facebookon, hogy Lego és WoW fan vagy, akkor már lehet neked ilyec témában küldözgetni, és arra lehet, hogy mégis ráharapsz.



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.11.17. 10:29:45

@prof Perselus Piton!

Én R20 és R40 operátorként kezdtem, padló alatt futó kábeldzsungellel, bolgár mosógépméretű lemezegységekkel, lyukszalaggal, lyukkártyával :-)



prof. Perselus Piton 2010.11.17. 17:51:25

@Csizmazia István [Rambo]:

Ó, a lyukkártya...egy gyakorló általános iskolába játam, ami ráadásul a főiskola épületének egyik hatalmas szárnyában volt...és hazafelé elvitt az utunk a matematika tanszék épülete és természetesen a szeméttárolójuk mellett is :-))

Nézegettük a lyukkártyákat és próbáltuk megfejteni a titkot...és meg voltunk győződve róla, hogy bent a "bácsik" úgy olvassák a kártyákat és néha szerpentinként dobált szalagokat, mint mi a könyvet :-)

prof. Perselus Piton 2010.11.17. 17:53:05



☐ a mellet végére, elvégre nem cicirovat ez :-))

Megjött az új 2011-es évad

2010.11.15. 17:05 | [Csizmazia István \[Rambo\]](#) | [5 komment](#)

Címkék: [internet win security 7 hamis 2011 antivirus](#)

Bár a címnek lehetne kellemes és pozitív üzenete is, ezúttal erről szó sincs. Bő egy hete [szóltuk le az ódivatú Antivírus Vista 2010-et](#), és tessék, meg is érkeztek az új versenyzők a hamis vírus kategóriában, **élükön a friss és ropogós Win7 Internet Security 2011-gyel.**



Közeledik az év vége, és ezúttal nem késedelmeskedtek sokat a nevek aktualizálással a kártevő terjesztők, **gyorsan rákönyököltek hát a randomnév generáló gombra - [le van itt fedve minden létező Microsoft platform](#):** Vista Antimalware 2011, Vista Antispyware 2011, Win7 Antispyware 2011, XP Security Tool 2011, XP Security 2011, XP Antispyware 2011, Vista Security 2011 **valamint a már emlegetett Win 7 Internet Security 2011.**



A Win7-es megjelenések mellett mindenesetre láthatóan **a még mindig tömegesen használt XP használókról sem feledkeztek meg.** A hamis riasztást adó kamu képernyőn a mi kedvencünk a Microsoft Visual Studios .CAB telepítőállományban állítólag szereplő EICAR teszt fájl volt :-)



Szerencsére [a valódi vírusirtók jó része már detektálja](#) ezeknek az ál vírusirtóknak a komponenseit, valamint folyamatosan [elérhetőek a különféle lépésről lépésre útmutatók is](#) a **kézi mentéshez.**

  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0 

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Informatikai biztonság az egészségügyben](#)
- [Akiknek a Captcha kinszenvedés](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szösölmédia" és nyaralás](#)

A bejegyzés trackback címe:

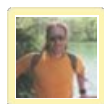
<http://antivirus.blog.hu/api/trackback/id/2450230>

Kommentek:

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

indust • <http://indust.hu> 2010.11.1. 08:02

A sorozatjunkie-n volt kérdés, hogy melyiket kaszálnád, hát ez az új évad felidézte bennem egyből. :)



Csizmazia István [Rambo] • <http://antivirus.blog.hu> 2010.11.17. 10:15:

Szia Indust!

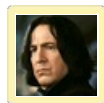
A melyiket kaszálnád itt még mindig jobban hangzik, mint a melyiket sunáznád ;-)



prof. Perselus Piton 2010.11.17. 18:01:15

Írom az előző poszthoz, hogy nem cicirovat, ti meg itt sunáztok :-)))

Nálam a játékaim "törését" szokta felismerni a vírusírtó, halálra idegelve engem (és mivel analfaBéka vagyok hozzá, nem tudom betenni a kivételek közé, hogy legközelebb ne találja meg őket)...tudom, menjek a boltba és vegyem meg :-)



prof. Perselus Piton 2010.11.17. 18:50:24

+t a mellet végére, elvégre nem ciciblog ez :-))



prof. Perselus Piton 2010.11.17. 18:55:18

kissé szétszórt lennék? ez meg hogy került ide?

Megjelent az ESET Cybersecurity for Mac

2010.11.17. 09:55 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [macintosh védelem](#) [trójai eset](#) [cybersecurity](#)

Több más gyártó után az **ESET is bemutatta** a Macintoshok védelmére szánt programcsomagját, egy olyan terméket, ami [még biztonságosabbá teszi az egyébként kevésbé támadott](#) alternatív operációs rendszereket.



Az ESET Cybersecurity teljes körű **védelmet kínál a Mac felhasználók számára az internetes kártevőkkel szemben**. A szoftver nem csupán a Macintoshokra írt vírusokat állítja meg, de a **Windows és Linux platformra készült kártevőket is**, így megakadályozza, hogy a Mac felhasználók tudtukon kívül továbbítsák ezeket.



A **biztonsági programcsomag ugyanazt a heurisztikus ThreatSense technológiát kínálja**, mint a windowsos ESET NOD32 Antivirus, így intelligens algoritmusok segítségével felismeri a legújabb kártevőket is, és alacsony erőforrásigényének köszönhetően nem lassítja le a számítógépeket. „*A Mac-es operációs rendszereket töredék annyi kártevő támadja, mint a windowsos gépeket, ez tény. Az adatok védelme azonban minden platformon fontos, hiszen a gépeken rajta vannak személyes dokumentumaink, fotóink és üzleti levelezésünk*” - emelte ki Kiss Zoltán Gergő, az ESET magyarországi képviselőjét ellátó Sicontact Kft. szakértője. Az ESET Cybersecurity **blokkolja az internetről érkező kártevőket és a fertőzött cserélhető adathordozókat**. A felhasználók személyre szabhatják a kézzel indított víruskeresés mélységét, beállíthatják a víruskeresés idejét, valamint az átvizsgálni kívánt archívum méretét.



Az otthoni felhasználóknak szánt **programcsomag 32 vagy 64 bites Intel® processzort igényel**, és a Mac OS X 10.5.x (Leopard), valamint a Mac OS X 10.6.x (Snow Leopard) rendszereket támogatja. **Az üzleti felhasználásra szánt változat ESET NOD32 Antivirus Business Editon for Mac OS X néven kerül forgalomba, és tartalmazza a központi menedzsment funkciókat is**, melyek segítségével egyetlen konzolon keresztül, távolról konfigurálható az OS X és a Windows alapú gépek védelme a **vállalati hálózaton belül**.



Bővebb információ az otthoni felhasználóknak szánt termékről az alábbi linken érhető el: <https://www.eset.hu/otthoni/cybersecurity>. A vállalati felhasználóknak szánt termékekkel kapcsolatban az info@sicontact.hu e-mail címen lehet érdeklődni, a **szoftverek próbaváltozata** pedig [letölthető az ESET magyarországi honlapjáról](#).

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1  0  Tweet

Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2454192

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Harry Potter és a Voccs Onlány Friei

2010.11.18. 14:50 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [google potter seo film csalás harry](#)

A rendre megjelenő új [Harry Potter filmek mindig jó aktualitást és táptalajt adnak](#) a kártevő terjesztőknek, csalóknak; a felhasználók szemszögéből viszont mindez úgy látszik, soha nem tanulnak semmiből. Pedig a [vadonatúj mozikat sosem a Google találatok](#) fogják tálcán kínálni ingyér.



A Websense vizsgálatai alapján [a Google találatok egyenesen egynegyede visz](#) kártevővel fertőzött weboldalra. És nincs ez másként a Harry Potter és a Halál Ereklýei I. esetében sem. Most éppen nem kodek trükközés van, hanem van helyette egy **minőségi IQ teszt** nyeremény, sügér-e vagy - [kérdezik az ukrán IP címről](#).



Az angol nyelven az a tétje, hogy megnyerjük-e az iPadet: **vajon meg tudjuk-e válaszolni azt a fogós, ravasz keresztkérdést, hogy ki az Apple társalapítója: A. Steve Jobs vagy B. Bill Gates.** Uhh, hát ezt azért nehéz így kapásból fejből rávágni, az Árpádházi királyok, Duna hidak nevei folyásirányban, az aranycsapat tagjai - az még hagyján, de hogy **még ezt az ismeretlen Apple-s tagot is hogy lehet séróból megjegyezni, az egy kész rejtély.** Nem vagyunk polihisztorok, így muszáj lesz valahogy kinyomozni, felhívni a telefonos Tudakozót vagy egyenesen a Google és Wikipedia oldalakon utánanézni ennek a furmányos válasznak ;-)



Az angolhoz hasonlóan a magyar oldalon is **nyereményjáték fogad bennünket survey helyett.** Úgy látszik angol óra helyett elmentek nekik otthonról, vagy meglazult egy deszkájuk.



Itt vajon mi óv meg bennünket attól, hogy ellenségeink begépeljék mobilszámunkat?



A magyar módi a "felmérésre", "ellenőrzésre", sőt szabatosan fogalmazva **a gaz spambotok és spammerek a mozi stream ellopását megakadályozandó biztonsági lépésként mi balkáni gyökerek fizessünk elő egy emeltdíjas hollandiai szolgáltatásra: 500Ft/SMS, 6 SMS/hét.** Jó hír, hogy az egész lezajlik röpké 2011. január 31-ig, így a watch online free nem is kerül többbe, mint lássuk csak, az annyi mint, köbgyök per anyád a négyzetten, **3000 HUF hetente, az összesen tíz hét, hehe: barátilag mindösszesen alig 30 ezer HUF.**



Ennyiért pedig igenis megéri megnézni egy igazi jó filmet, pláne ingyen és online, ezt nem vitathatja senki :-)





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



0



Ajánlott bejegyzések:

- [Gyerek-barát netezés](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2456690>

Kommentek:

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

[Evil Dick 2010.11.29. 23:32:19](#)

Vérgáz.

Itt a Zeus trójai lehetséges utódja

2010.11.22. 12:30 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [trójai botnet ares kártevő készlet zeus terjesztő](#)

A szakemberek szerint az Ares trójai program tekinthető a korábbi [botnet építő Zeus kártevő](#) utódjának. A **supporttal támogatott jelszólopó kártevőket terjesztő teljes készlet ára 6000 dollár**, de csökkentett tudású kezdőcsomag már olcsóbban is kapható, 850 USD összegért.



A fejlesztők folyamatosan mindent megtesznek, hogy [a kártékony kódokat terjeszteni szándékozók igényeit megfelelően kielégítsék](#). A későbbiekben is **könnyen módosítható, moduláris elemekből álló készletet szinte mindenféle típusú támadáshoz** - spamküldés, kártevőterjesztés, DDoS, stb. - könnyen használhatóvá tették, és kívánságra, illetve külön pénzért egyéb extrák, sőt folyamatos terméktámogatás is jár hozzá. Aki akarja, annak [időlegesen bérelhető is](#).



Az anonim fizetést is megoldották a WebMoney segítségével, ahol sem a vevő, sem pedig az eladó nem tudja meg végül, igazából kivel is üzletelt.



A fejlesztők állítása szerint [a megvásárolható Ares készlet minden egyes darabja teljesen egyedi](#), külön kívánságra például tetszés szerint banki azonosítók elleni támadásokhoz is tuningolható. A **hatékony védekezési megoldáson** mindenesetre [mind a biztonsági programok fejlesztőinek és szakembereknek](#), mind pedig [az egyszerű felhasználóknak](#) folyamatosan dolgozniuk, illetve figyelniük kell.



Az én csak egy hétköznapi juser vagyok szemléletnek vége, mindenkinek lehet olyan félténivalója a számítógépén - legyen az végrendelet, orvosi vizsgálatok eredménye, önéletrajz, üzleti elszámolás, jelszólista vagy privát fotók - amelyek [rossz kezekbe jutva sok kellemetlenséget](#) okozhatnak.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Kártékony antivirusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kinszenvedés](#)

A bejegyzés traceback címe:

<http://antivirus.blog.hu/api/trackback/id/2464977>

Kommentek:

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



[prof. Perselus Piton 2010.11.23. 12:13:44](#)

Szokták mondani, hogy nem haladok a korral, mert csekken fizetek, besétálok a bankba, ha kell valami, stb. És sosem szoktam tudni megvédeni magam az ilyen megjegyzésekkel szemben...de majd most :-)) csak bedobom, hogy Ares már les az adataitokra...

Komolyra fordítva a szót, azért ez tényleg elég ijesztő...

[cworm \(törölt\) 2010.11.23. 13:42:42](#)

És ez tényleg működik is, vagy olyanok ezek is, mint a fake av-k? :)

Pandúrból lesz a legjobb rabló

2010.11.24. 11:01 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [ítélet](#) [matthew anderson](#) [kémprogram](#) [kártévőterjesztés](#)

Egy 33 éves skót hackert ítélték el spam levelek küldéséért, valamint kémprogramok terjesztéséért, és 18 hónap börtönbüntetést kapott.



Egy eredetileg még 2005-ben indult vizsgálat zárult most le ezzel az ítélettel. A vizsgálat szerint **a férfi egy moop nevű nemzetközi bűnbanda tagjaként** 2005-ben és 2006-ban tízmilliónyi kértelen elektronikus levelet küldött ki kártévőt tartalmazó melléklettel.



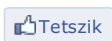
A kémprogram képest volt magánszemélyek, kisvállalkozások számítógépein hátsóajtót nyitni, és azon keresztül bizalmas információkat, jelszavakat tudtak ellopni, de kémkedtek a beépített webkamerát távolról bekapcsolva is. Összesen három személyt tartóztattak le az akkori cselekmények kapcsán. A rendőrség a házkutatások és számítógép átvizsgálások során **megtalálta az eltulajdonított személyes adatokat, bizonyítékul szolgáló távolról készített képernyőképeket, jelszólistákat.**



Szokatlanul **enyhe ítéletnek tűnik ez botnet üzemeltetésért**, valószínűleg Amerikában nem úszta volna meg ennyivel. A [védő érvelése szerint fiatalos kalandvágy vezérelte](#), de azóta már megkomolyodott, bűnösnek vallotta magát és megbánta tettét.



Az eset megítélését azonban erősen súlyosbítja, hogy a "Warpigs" és "aobuluz" nickneveken is szereplő [Matthew Anderson eredetileg számítógépes biztonsági szakértőként dolgozott](#), és egy Optom Security nevű biztonsági céget vezetett.



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



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)
- [Ez történik a weben egy perc alatt](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- ["Szósölmédia" és nyaralás](#)

A bejegyzés **trackback** címe:

http://antivirus.blog.hu/api/trackback/id/2469711

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Zeus toborzó

2010.11.26. 12:50 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [java](#) [facebook](#) [csalás](#) [trójai](#) [botnet](#) [zeus](#)

Hogyan lehet önkénteseket toborozni a botnet hadseregbe hatékonyan, könnyen, gyorsan, csak most, csak önöknek? Mi sem egyszerűbb! Meríteni kell egy óriási 500 milliós edénybe, és legyen mondjuk a horgon valami ilyesmi: Keress sok pénzt egyszerűen. Kész is, lehet húzni felfelé a damilt, a siker biztos.



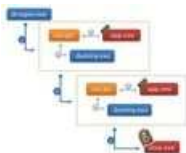
Természetesen [a Facebookon zavarosban halászókról szól a poszt](#), most éppen a "Learn How To Earn £20/Hour With PTC" nevű felhasználó a téma, tényleg **szép név, csak a személyiben kicsit hosszú lenne**. Még csak 11 embernek tetszik, de a szám nyilván nőni fog, illetve a lájkolók száma **nem egyenlő a rákattintott és úgy járt emberek** számával. Ha az elkövetők kombinálták volna a módszert **"Az emberek 98%-a nem tudja 17 másodpercnél tovább nézni ezt a videót" trükkkel**, 48 óra alatt **óriásit tarolhattak volna, szinte érthetetlen, miért nem tették mégsem**.



Mindenesetre **a linkre kattintva sosem tudjuk már meg a nagy titkot** - hasonlóan Gorcsev Ivánhoz, akinek a kapuőr elkezdte ugyan magyarázni: "Az én mesterségem három fő kelléke az ész, a pszichológia és a jól ápolt szakáll. De kell még ezenfelül...". Hogy mi kell ezenfelül, az itt sem derül ki, még ha nem is egy 14 karátos autó tehet róla. Nos minket is elsodornak itt az események, ugyanis a pénzkereső varázsreceptre kattintva először egy facebookon kívüli weboldalon találjuk magunkat, aztán **nyomban egy .JAR kiterjesztésű állomány emelkedik szólásra és szeretne letöltődni** nagy tisztelettel. Vajon a 6500 forintos órabér fantasztikus titka rejtőzik benne?



Kérdezzük meg erről orvosunkat, gyógyszerészünket és **Virustotalunkat**. Minő fájdalom, siker receptnek se híre, se hamva, [hanem helyette egy Java nyelvű TrojanDropper](#) öltögeti ránk a nyelvét.



Bár az is lehet, eredetileg mégis van értelme van ennek a pénzkeresési módszernek. Réges régen, mikor a hülyét még pontos j-vel írták, a C64-et sem találták még fel, volt olyan újsághirdetésben terjedő csalási módszer, ami úgy szólt: "Akar ön munka nélkül egyszerűen pénzt keresni? Küldjön egy ezrest egy borítékban és elküldöm a receptet!" Ha az akkori csalóknak volt egy kis humorérzékük, akkor az volt a válaszban: "Hehe, így lehet, add fel te is ezt a hirdetést!".



Ha viszont híján volt a humorérzéknek, akkor simán csak eltette a pénzt, és nem válaszolt. Magyarul itt is **lehet, hogy igaz a történet**

magya, csak éppen a hirdetés feladója keresi meg ezzel a 20 fontos óradíjat, a fejpénzt, nem pedig a naív kattintó.



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



Ajánlott bejegyzések:



- [Kártékony vírusok - 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/2474195>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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 kapható a Stuxnet kódja a feketepiacon

2010.11.29. 12:55 | [Csizmazia István \[Rambol\]](#) | [3 komment](#)

Címkék: [trójai feketepiac stuxnet skynews](#)

A SkyNews egy riportban számolt be arról, hogy az iráni Bushehr atomerőművek ellen bevetett [Stuxnet kártevő](#) kódját már árulják a bűnözők az interneten.



[Mivel egy igen kifinomult, és bonyolult kódról van szó](#), ezt módosítani ha nem is könnyű, de természetesen lehetséges.



Arról nincsenek pontos információk, hogy generáló készlet formájában vagy maga a forrás lett az árucikk, de szakértők szerint mindenképpen félő, hogy megfelelő változtatások után más erőművi, közművi, kórházi, közlekedési, akár célzottan rendőrségi hálózatok vagy egyéb célpontok ellen is készíthetnek majd további variánsokat, vagyis a [terroristák remekül fel tudnák azt használni](#).

Operációs rendszer	Stuxnet 1	Stuxnet 2	Stuxnet 3	Stuxnet 4
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3

Operációs rendszer	Stuxnet 1	Stuxnet 2	Stuxnet 3	Stuxnet 4
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3
Operációs rendszer	Windows XP SP3	Windows XP SP3	Windows XP SP3	Windows XP SP3

A korábbi vizsgálatok szerint a kártevőt kifejlesztők rendkívül **alapos tudású szakemberek** lehettek, maga a kártevő elkészítése pedig nagyfokú elkötelezettséget és komoly anyagi háttérrel rendelkező megbízói kört sejtet.



Mindenesetre úgy tűnik, **egyáltalán nem értelmetlen dolog manapság cyberhadssereget verbuválni**, és azokkal [rendszeres hadgyakorlatokat tartani](#). Akit pedig a Stuxnet bővebben és részletesebben is érdekel, annak **hasznos olvasmány lehet az Aleksandr Matrosov, Eugene Rodionov, David Harley és Juraj Malcho víruselemzők által készített 81 oldalas [Stuxnet under the Microscope](#) című összefoglaló**.

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

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [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/2480796>

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](#).



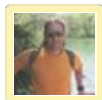
buherator • <http://buhera.blog.hu> 2010.11.29. 14:52:52

Mikko Hypponen (twitter.com/mikkohypponen) twitterét lett volna érdemes figyelni ezügyben:

Nem valószínű, hogy kikerült a forráskód, a bináris pedig eddig is könnyen megszerezhető volt (ugye magától terjed a drága). Másrészt ha valakinek van egy forráskódja, amellé némi túlzással kell még egy atomerőmű/forgalomirányítási rendszer/csofgyár, amire az új variánst el lehet készíteni, illetve ahol lehet tesztelni.

Evil Dick 2010.11.29. 23:22:13

Ebből is csak azért lett médiahír, mert észrevették a "célszemélyek", hogy egyáltalán létezik és fut ez a vírus. Legközelebb detektálhatatlanabbra kéne gyártani a kódot.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.11.30. 21:49:02

Phh, persze nem így akartam. Forráskód vagy generáló készletre gondoltam.

A teszteléshez szükséges csokigyárat vállalom :-)

A legnépszerűbb hobbi

2010.12.01. 11:45 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [kína](#) [kártevők](#) [kibertámadás](#)

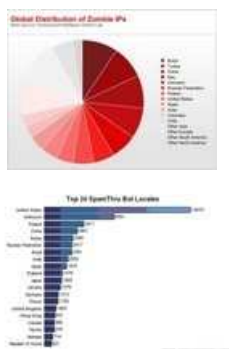
Kínában az év eleje óta összesen 460 számítógépes támadót tartóztattak le (szándékosan nem hackernek nevezzük őket). Ha visszatekintünk az időben, jó két-három éve, hogy egyre gyakrabban olvashatunk [vélt vagy valós kínai eredetű](#) támadásokról.



Mi is megírtuk 2007-ben, hogy [Angela Merkel kínai látogatása alatt](#) fedezték fel, hogy a német kancellária és több más **kulcsfontosságú minisztérium számítógépei kínai eredetű kémprogramokat** tartalmaztak.



Aztán **idén év elején derült fény arra**, hogy [feltörték a Google szervereit](#) és ahhoz illetéktelenül hozzáférést szereztek, majd a kiemelt érdeklődés és nemzetközi figyelem miatt [bezártak egy \(azaz uno, ein, one, ágyin\) igaz a legnagyobb hacker iskolát](#).



Kínában a hackelés, számítógéppel való [különböző színű kalapokban való ténykedés](#) igen csak **népszerű hobbinak számít**, és a népességhez viszonyítva a 460-as érték még a jéghegy csúcsának sem nevezhető. A **nagy számok törvénye** alapján a helyzetet ezzel **biztosan nem oldották meg**. A kérdést persze árnyalja, hogy sok esetben gyanítható, a kínai kormány bátorítására, kérésére, vagy **nem hivatalos támogatásával zajlanak** különféle kiber támadások [a Dalai Láma, vagy éppen a Google ellen](#).



Mindenesetre végezetül a konteo kedvelőknek - mintegy lazításképpen - íme egy kis adalék felvetés arról, hogy a [Wikileaks](#) [kiszivárogtatások vajon mennyire lehetnek pusztán véletlenek](#), vagy esetleg eltűnődhetünk, mennyire időzítettek, sors- és forgatókönyvszerűek.

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

Megosztás +1 Tweet

Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [Informatikai biztonság az egészségügyben](#)
- [Safe mód a Mechagodzilla ellen](#)
- ["Szösölmédia" és nyaralás](#)
- [Dropbox csalival terjedtek a kémprogramok](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2485490>

Kommentek:

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



[exter69](#) • <http://sexopoly.tarhely.biz> 2010.12.01. 21:19:03

Ha egyszer a kis sárgák beindulnak valamire, ez a minimum.

Mobil böngészés mellékhatásokkal

2010.12.03. 13:30 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [apple safari iphone böngészés nitesh dhanjani](#)

Hogy mitől okos az okostelefon, nos [arra többféle válasz](#) is lehetséges. Többek közt az is, hogy [segítségével az interneten](#) levelezhetünk, közösségi oldalakat érhetünk el illetve weboldalakat böngészhetünk vele. Fontos kiemelni, hogy [ha létezik is rá biztonsági alkalmazás](#), a hagyományos számítógépen futó társaihoz képest az lényegesen szerényebb.



[Nitesh Dhanjani mint már annyiszor](#), ismét érdekes felfedezést tett. Úgy találta, mivel a kényelem és a kis kijelző miatti egyszerűsítés jegyében a böngészett URL kiírása rejtésre kerül, és ez komoly veszélyeket hordozhat magában. [Kísérletéhez a valódi](#) Bank of America oldalát használta, és bemutatta, hogy amint [az eredeti oldal már betöltődik, és a link eltűnik, az kicserélhető egy kártevőt tartalmazó hasonló kinézetű linkre](#), amelynek iPhone alatti igazi címe azonban így rejtve marad. A felhasználó csak akkor észlelheti azt, ha és amennyiben a képernyő legtetjére scrollozva újra leellenőrzi a címsort.



Ha ugyanezt megnézzük egy **asztali gépen, akkor jobban el vagyunk kényeztetve információkkal**: böngészőnkben jelezhetnek a biztonsági (a Finjan SecureBrowsing, a Robot Genius Guard, Phishtank Sitechecker vagy a McAfee SiteAdvisor) pluginek, megnézhetjük az IP címet és az URL-re vonatkozó NetCraft rekordot, valamint összehasonlíthatjuk a címsorban és az állapotsávban kijelzett linket.



Nem mellesleg pedig a használt **internet biztonsági csomagunktól is kaphatunk riasztást** a feketelistás linkre, vagy a linkről letöltődni akaró kártevőre, de akár mindkettőre is egyszerre. Amit [azokon a szerencsés mobil eszközökön is megkaphatunk, amire már léteznek security csomagok](#). Egy biztos: mobil böngészőkliensekben már eleve nehezebb a kétséget kizáró ellenőrzése annak, hogy biztosan a hiteles, kívánt oldalon vagyunk-e éppen.



A fentiek fényében azon lehet inkább eltűnődni, hogy **vajon okos dolog-e** az okostelefonon olyan weboldalakat böngészni, amelyek túlmutatva a szokásos tájékozódó, olvasgató, megnézem az időjárást/moziműsort/menetrendet/koncerteket módin felül már **hivatalos ügyek lebonyolítására, bankolásra, pénzügyek intézésére is** használná az asztali gépekhez viszonyítva biztonsági szempontból mindenképpen szűkebb keresztmetszetű platformot.

Ha valakinek van véleménye, kommentekben hozzászólni, egyetérteni, vitatkozni ér :-)

Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 Tweet

Ajánlott bejegyzések:



- [Kártékony böngésző kiegészítők jönnek](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2489937>

Kommentek:

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



[prof. Perselus Piton 2010.12.04. 15:44:32](#)

Anno takarítógépet akartam venni...előadtam, hogy legyen vizes, de nagyon jól porszívózzon is, mert szőrhullató apró állat is lakik velem...erre azt mondta az eladó, hogy vegyek egy szuper porszívót és mikor épp kell, béreljek egy vizes gépet, mert valami vagy vizez vagy poroz, de együtt sosem jó :-)) azóta minden műszaki cuccnál ez jut eszembe...tehát a telefonom csak telefonálásra és sms írásra alkalmas...nem biztonsági megfontolásokból, de ezek szerint ma már az sem utolsó szempont...

Jó hír Mikulásra

2010.12.06. 15:20 | [Csizmazia István \[Rambol\]](#) | [1 komment](#)

Címkék: [mikulás](#) [botnet](#) [spammer](#) [oleg nikolaenko](#) [mega d](#)

Elege van abból, hogy minden nap csak a biztonságunkat fenyegető rossz dolgokról értesül? Unja már a nyomasztó híreket, miszerint megint újabb számítógépes kártevőt fedeztek fel, [amely gonoszságban és pusztításban felülmúlja](#) elődeit? **Jöjjön hát most Mikulás nap alkalmából ezúttal valami szívderítőbb pozitívum.**



Az amerikai hatóságok **sikeresen letartóztatták a 23 esztendőes Oleg Nikolaenkot** (kár hogy a mai Miklós nap miatt nem Nikolai Olegenkonak hívták inkább, de sebj), akit [azzal vádol az FBI, hogy ő üzemeltette a Mega-D botnet](#) néven közismert fertőzött számítógépekből álló zombihálózatot.



Egy FBI ügynök eskü alatt tett [részletes terhelő vallomást](#) ellene, melyben a CAN-SPAM törvény megsértésével, valamint azzal vádolják, hogy [együttműködött a tavaly év végén elítélt spamkirállyal, Thomas Lance Atkinsonnal](#).



A SecureWorks és az M86 Security munkatársai már 2008 óta folyamatosan nyomoztak a Mega-D botnet után. Mint emlékeztetes, a [2008 évvégi McColo hoszting cég kitiltása](#) következtében átmenetileg ugyan csökkent a botnetes aktivitás, de [pár hónap múlva már sajnos nem volt érezhető](#) a rájuk mért csapás áldásos hatása.



Reméljük, Karácsonykor is kapunk valami ajándékot és a piros betűs ünnepre való tekintettel megint letartóztatnak majd valamilyen **jelentősebb botnet pásztort**, hogy ezzel is megédesítsék a mákos bejglinket. Végül, de semmiképpen nem utolsósorban **minden Kedves Olvasónknak teli puttonyt és gazdag Mikulást kívánunk az alábbi kis klippel!**



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.



Ajánlott bejegyzések:

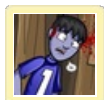
- [Gyerek-barát netezés](#)
- [Kártékony vírusok - villám őrjárat 8.](#)
- [Kártékony böngésző kiegészítők jönnek](#)
- ["Szösölmédia" és nyaralás](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2496378>

Kommentek:

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



[leviske 2010.12.06. 21:17:41](#)

Hát nem tudom, én olyannak nem tudok örülni, hogy valakit letartóztatnak, függetlenül attól, hogy mit tett.

Vírusvédelmek hazai tesztelése

2010.12.08. 14:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [tesztelés](#) [laboratórium](#) [checkvir](#) [vírusvédelmi](#) [veszprog](#)

A Veszprog Kft. által üzemeltetett CheckVir tesztlaborban elindult a vírusvédelmi rendszerek valós idejű tesztelése. A bárki számára elérhető független szolgáltatást az erre a célra fejlesztett automatikus rendszer biztosítja, mely képes a vírusvédelmi rendszerek közel valamennyi verzióját vizsgálni.



A tesztelési feladatot ellátó számítógépek - ez **24 darab négy magos, és 12 darab egymagos gépet** jelent - biztonsági okokból egy speciális tűzfalon keresztül érik el az internetet. Egy Debian Linux alatti rendszer perl szkriptek segítségével gondoskodik arról, hogy Windows operációs rendszer képfájlját (image-ét) – mely tartalmazza a vírusvédelem aktuális verzióját – cserélje és megfelelő időközönként elindítsa. A rendszer arra is **képes, hogy menetközben észlelje, ha egy vírusvédelem frissítése megtörtént**, így a teszteléshez a frissítési feladat során elmentett image-et (képfájlt) tölti be. A tesztelési feladatnak megfelelő Wintask szkriptet, illetve a teszteléshez szükséges fájlokat (pl.: minták, vírusmentes állományok) másol a rendszerbe, majd a bootolását követően a tesztelési feladat végrehajtódik. A tesztelést követően **az eredményeket a debian Linux alatt futó perl szkript a webservertől SQL adatbázisába másolja**. Az automatikus rendszer egy adatbázisban gyűjti vírusvédelmek különböző verzióira vonatkozó tesztelési eredményeket, melyek az interneten folyamatosan elérhetők, egyszerűen és kényelmesen nyomkövethetők.



A CheckVir projektben a tesztelési eljárások a szokványos felhasználói viselkedésre épülő használatot mintázzák. A vírusvédelmi megoldásokat a tesztelés során egy fekete doboznak tekintik, majd az alábbi tesztfeladatokat hajtják végre:

- Kártevők ismeretének a vizsgálata (felismerés)
- Kártevők ismeretének a vizsgálata (eltávolítás - helyreállítás)
- Téves (false positive) riasztások vizsgálata
- Sebesség ellenőrzése kártevőmentes környezetben



Ezenfelül kerül sor még az úgynevezett "Konténer" tesztre. Ez utóbbiban a számítógép használata során keletkező további fájlokat tartalmazó állományokat vizsgálják. Ezeket vagy a felhasználó hozza létre kézzel - **például készít egy tömörített ZIP csomagot vagy egy dokumentumba beleágyaz egy másik állományt**. De létrejöhetnek ilyenek átlagos körülmények között automatikusan is. Ez utóbbira példa, amikor egy felhasználó **egy e-mail üzenetet tölt le és azt az e-mail kliense tárolja el**.



Az ilyen típusú állományok esetén a **védelmi rendszernek ismernie kell ezen speciális állományok szerkezetét**. Az ilyen vizsgálatok elvégzése azért nagyon fontos, mert ha például egy védelem azt az üzenetet adja – miután egy számítógépet teljesen átvizsgált -, hogy az vírusmentes, akkor **érdemes tisztában lenni ezen üzenet korlátaival**. A vizsgálat során olyan állományt használnak, melyet valamennyi, a tesztelésben résztvevő védelem ismer (például az EICAR tesztfájlt: www.eicar.com) és ezt az állományt csomagolják be különböző "konténerekbe". **A vizsgálat során azt tesztelik, hogy képes-e a védelem az adott „konténerben” megtalálni a kártevőt, illetve, hogy ezt a beágyazott konténerek sorában milyen mélységig képes megtenni**. Ezen túlmenően speciális körülmények között is vizsgálják a védelem képességeit: hosszú fájlnevek használata, jelszóval védett konténerek.



A weblapon **jelenleg csak egy szimuláció fut, nem valós termékekkel**. Most történik ugyanis a különböző antivírus gyártókkal a konkrét megállapodás. **A szolgáltatásról és a cégről további részletes információkat** magyar és angol nyelven a www.checkvir.hu weboldalon lehet találni.



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



Ajánlott bejegyzések:

- [A PRISM szeme mindent lát](#)
- [Informatikai biztonság az egészségügyben](#)
- [Android kémprogram persze csak a mi érdekünkben](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2501661>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Tízből nyolc trójai. Mennyiii?

2010.12.10. 11:10 | [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. Ebben a hónapban sem sikerült letaszítani a trónjáról a lassan 13 hónapja a vírustoplista élén álló Conficker férget.



A novemberi magyar lista első helyét már 2009 novembere óta az a Conficker féreg tartja, amely az operációs rendszer frissítéseinek hiányát, a gyenge jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed. Kisebb fajta meglepetés lehet az INF/Auron vírus eltűnése, amely már 2008 szeptembere óta folyamatosan listatag volt, és általában rendre az élmezőnyben vert tanyát.

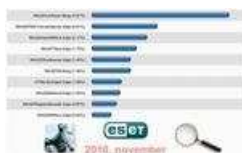


A novemberi lista emellett jól láthatóan **rekorder is egyben**, [hiszen minden korábbinál több](#), a tízből összesen nyolc trójait tartalmaz. A trójai egy olyan program, ami valami mást (is) csinál, mint amit magáról eredetileg állít. Ez a más sok minden lehet: hátsóajtót nyithat a gépén, kémkedhet jelszavak és a bizalmas adatok után, meghamisíthatja a keresési eredményeket, vagy a hálózati beállítások manipulálásával észrevétlenül hamis oldalakra irányíthat bennünket böngészés közben.

A két újonc egyike a Win32/HackMS alkalmazás. Ez eredetileg egy Microsoft programokhoz készített warez kulcsgeneráló eszköz, **amely azonban kártevőt is tartalmaz**. A program telepítésekor olyan rejtett állományokat és olyan Registry bejegyzéseket is létrehoz, amelyek a hálózati beállításokat és a keresési eredményeket titokban módosítják a számítógépen.



A másik újonnan listára került kártevő a Win32/RegistryBooster alkalmazás, amely a hamis antivírus programokhoz hasonlóan a felhasználót hamis riasztásokkal becsapva a **program fizetős változatának megvásárlására igyekszik rábeszél**ni a fertőzött számítógép tulajdonosát. Érdemes nagyon körültekintőnek lenni, amikor állományokat vagy telepítendő programokat töltünk le. **Csak ismert, ellenőrzött, megbízható helyről** installáljunk szoftvereket, illetve minden újdonságnak alaposan nézzünk utána az interneten. Ha már sokan panaszkodnak egy-egy ilyen alkalmazásra, inkább kerüljük el a felesleges kockázatokat.



Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2010 novemberében a következő 10 károkozó terjedt a legnagyobb számban**, és volt felelős együttesen az összes fertőzés 18.72%-ért.



1. Win32/Conficker féreg

Elterjedtsége a novemberi fertőzések között: 5.67%

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 eljárásan keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a főreg 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 novemberi fertőzések között: 2.61%

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>



3. Win32/HackMS trójai

Elterjedtsége a novemberi fertőzések között: 2.17%

Működés: A Win32/HackMS alkalmazás eredetileg egy warez kulcsgeneráló eszköz, amely azonban kártevőt is tartalmaz. A program telepítésekor olyan rejtett állományokat és olyan Registry bejegyzéseket is létrehoz, amelyek a hálózati beállításokat és a keresési eredményeket is 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 novemberi fertőzések között: 1.73%

Működés: A Win32/Tifaut fájlokat hoz létre a C:\Windows\System32 mappában csrs.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 novemberi fertőzések között: 1.46%

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 novemberi fertőzések között: 1.46%

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 novemberi 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/Mebroot trójai

Elterjedtsége a novemberi fertőzések között: 1.03%

Működés: A Win32/Mebroot.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/%21mebroot>



9. Win32/RegistryBooster trójai

Elterjedtsége a novemberi fertőzések között: 0.87%

Működés: A Win32/RegistryBooster alkalmazás a hamis antivírus programokhoz hasonlóan a felhasználót hamis riasztásokkal becsapva a program fizetős változatának megvásárlására igyekszik rábeszélni a fertőzött számítógép tulajdonosát.



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 novemberi fertőzések között: 0.64%

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>



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



Ajánlott bejegyzések:

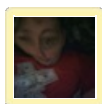
- [Gyerek-barát netezés](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Majdnem mindenki átverhető adathalászzal](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/2503813>

Kommentek:

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



[PokerKevin](http://pokerheaven.blog.hu/) • **<http://pokerheaven.blog.hu/>** **2010.12.10.**
[13:07:54](#)

A legjobb víruskereső!

Fertőzött DoubleClick banner hirdetés

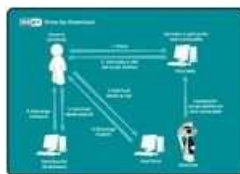
2010.12.13. 14:25 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [google](#) [hirdetés](#) [banner](#) [doubleclick](#) [fertőzött](#) [adshufffle](#)

A Wired magazin számolt be arról, hogy a Google DoubleClick rendszerében rosszindulatú hirdetést találtak. A megjelenő hirdetésre még csak rá sem kellett kattintani, az a [drive-by-download módszernek](#) köszönhetően magának a pusztán megjelenésnek a felhasználó tudta nélkül, észrevétlenül megfertőzte a látogatók számítógépét.



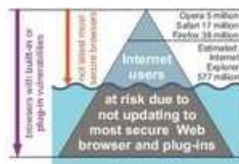
A [kártékony tartalmakról](#) az Armorize vizsgálata szerint az AdShufffle (három f betűvel) nevű csaló reklámszolgáltató tehet, akik a létező és legitim AdShuffle (két f betűvel) cég nevével éltek vissza.



A fertőzött banner hirdetések a Runnersworld.com és az OrganicGardening.com oldalakon jelentek meg, és párhuzamosan többféle sebezhetőséggel is próbálkoztak, [többek közt a háttérben a böngészőben megnyitott PDF állományok útján](#).



Időközben a Google azt a tájékoztatást adta, hogy [a bejelentés után már egy külön szűrővel figyelik és kerülnek el](#) a hasonló incidenseket.



És mit tehetünk mi? Ellene a számítógépünk frissítésekkel való naprakészen tartásával, Windows esetén a [Sandboxie és a DropMyRights programok](#) használatával, illetve a Firefox böngésző alatt a már [sokat emlegetett NoScript kiegészítő](#) alkalmazásával lehet felvenni a kesztyűt.



Egy 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](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés `trackback` címe:

`http://antivirus.blog.hu/api/trackback/id/2512535`

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Karatézzuk le a kártékony linkeket!

2010.12.15. 16:10 | [Csizmazia István \[Rambo\]](#) | [2 komment](#)

Címkék: [alma link kaland url kártékony adathalászat](#)

Az internetes bűnözők egyik kedvelt fogása, hogy [meghamisítanak jól ismert weboldalakat](#), majd ezeken keresztül megszerzik a gyanútlan látogatók személyes adatait és jelszavait. De vajon mennyire vagyunk képesek felismerni a hamis webcímeket? Sün, sün, eksün!



A NOD32 magyarországi képviselte egy jópofa oktatójátékot készített ennek teszteléséhez. "Az adathalászat azért veszélyes, mert megtéveszti a felhasználókat. Egy hamis e-mail nem tartalmaz kártékony kódot, csupán egy linket. Így annak ellenére, hogy adathalászat elleni védelmet már szinte mindegyik biztonsági szoftvercsomag kínál, az ilyen **linkeket még a kiváló vírusirtó szoftverek sem ismerik fel minden esetben.**



Amikor a felhasználó egy ilyen, álcázott linkre kattint, **egy olyan weboldalra kerül, ami megszólalásig hasonlíthat az eredeti oldalhoz, amit utánoz. A bűnözők így hozzájutnak a felhasználók jelszavaihoz, és sok esetben hitelkártya adataikhoz is** - nyilatkozta Csizsér Béla, az ESET magyarországi képviselétét ellátó Sicontact Kft. ügyvezetője.



A bűnözők jól álcázzák az adathalász hivatkozásokat. **Tipikus példa erre, amikor egy weboldalon egy olyan kattintható linkkel találkozunk,** mely látszólag a www.jo-weboldal.hu hivatkozásra mutat. Azonban, amikor rákattintunk, a böngésző címsorában láthatjuk, hogy a link a hxxp://www.jo-weboldal.hu.ru orosz weboldalra vitt bennünket, ami alapos okot adhat a gyanúra.

A játék során **egy sünit kell irányítani, és eldönteni, hogy a lehulló almákban lévő webcímek közül melyik tartozhat egy adathalász weboldalhoz, és melyik a helyes webcím.** A játékot a <http://www.eset.hu/almakaland> weboldalon keresztül ingyenesen használhatják magánszemélyek, iskolák és akár olyan vállalatok is, melyek szeretnék biztosítani, hogy alkalmazottaik [megtanuljanak biztonságosan internetezni.](#)



A sikeres és tempós végigjátszás után lehetőség van a Top listára is felkerülni, illetve mindenképpen kapunk egy jelképes oklevelet is. **Az igazi siker persze maga a gyakorlás és a saját hibáinkból való tanulás.** Futhat bármilyen szoftver a gépeken, a [rendszeres képzés, az óvatos gondolkodás mindig is](#) fontos marad.



A helyes webcímek felismerése egyébként képezhetné akár az általános iskolai tananyag részét is, ami jelentősen hozzájárulna ahhoz, hogy a magyar felhasználók [biztonságosan tudjanak internetezni](#). Mindenesetre az Alma Kaland segítségével most nem csak **a gyerekek, de a felnőttek is játszva megtanulhatják felismerni** az adathalászok tipikus csapdáit.

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

Ajánlott bejegyzések:

- [Android kémprogram persze csak a mi érdekünkben](#)
- [Akiknek a Captcha kínszenvedés](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- [Dropbox csalival terjedtek a kémprogramok](#)
- [Küldj pénzt! - Az elveszett poggyász sztori](#)

A bejegyzés trackback címe:

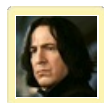
<http://antivirus.blog.hu/api/trackback/id/2517228>

Kommentek:

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

Evil Dick 2010.12.16. 21:11:52

100 százalékos lettem a 8 pályán. Menő vagyok? :)



prof. Perselus Piton 2010.12.23. 18:27:06

Evil Dick: Menő Manó :-))

Nálam bezavart a macska, a billentyűzetre heveredve, így kiderült, hogy nem vagyok százaz :-P

Márkanévét kegyelettel lejáratjuk II.

2010.12.17. 15:20 | [Csizmazia István \[Rambol\]](#) | [Szólj hozzá!](#)

Címkék: [csalás](#) [security](#) [smart](#) [hamis](#) [antivírus](#)

A hamis vírusok és egyéb scareware kategóriába sorolható pénzt zsaroló alkalmazások virágkorukat élik. **Sajnos egyre gyarapodó számuk nem csak a randomizált nevek tobzódása** és a [2011-es évjárat felbukkanása](#) okán érdekes, hanem a sanda névválasztás miatti félrevezetés, és [a márkanevek renoméjának tudatos rombolása is](#) elszomorító.



[A Vírusok Varázslatos Világa 40. része is](#) pontosan ilyen, **létező védelmi programok kinézetéhez és/vagy nevéhez való hasonlóságokról** szólt. Ezúttal az ESET egyik programja is [célkeresztbe került egy hamis Smart Security nevű program](#) kapcsán.



A kamu program, amely hamis riasztással csak a pénzünket akarja

Szerencse a szerencsétlenségben hogy azért **nagyon-nagyon laikusnak, tapasztalatlannak kell lenni ahhoz, hogy a hamis programot valaki összekeverje az igazzal**, és méginkább szembeszökő a két program közti különbség [annak, aki esetleg ismeri korábbról a NOD32 programjait](#).



A valódi ESET Smart Security, amely nem szólít fel fizetésre

A nevek választása itt is **a korábbiakban megismert kaptafára variálódik: sima Smart Security, XP Smart Security, Windows Smart Security**, de [az idők szavára hallgatva van Win7 Smart Security is](#).



És bár [a sötét oldal mindent bevet](#), mindenesetre érdemes a programok pusztá nevéen felül azt is jól megjegyezni, hogy **valódi védelmi program sosem ugrik fel csak úgy véletlenül böngészés közben egy számítógépre**. Így továbbra se igyunk mosatlan gyümölcslevet vagy használjunk kéretlen antivírus programot ;-)



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



0



Ajánlott bejegyzések:

- [Kártékony böngésző kiegészítők jönnek](#)
- [A kiknek a Captcha kinszenvedés](#)
- [Tízből öt kártevő hátsóajtót nyit](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2521150>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.

Mentés másként

2010.12.23. 10:10 | [Csizmazia István \[Rambol\]](#) | [2 komment](#)

Címkék: [blog](#) [xmas](#) [kellemes pdf](#) [mentés](#) [karácsonyt](#)

A [Karácsony nem csak a szeretet ünnepe](#), hanem **optimális esetben az évvégi számvetés, rendszeres jelszócseré és [számítógépes munkáink nagy szabású mentésének ideje is](#)**. Barkács Pajtás ezúttal a [blog.hu](#) posztok kapcsán külön egyéni buherálási célokat tűzött ki maga elé két bejgli között: menteni mindent.



De jó is lenne az összes eddigi - több, mint háromévnnyi - bejegyzést lementeni, mondjuk Portable Document formátumban - mondta Barkács Pajtás. Ezzel Broáfka Ottokár és Kovács Brezsnyevke is egyetértett. Igaz, ezt egyesével könnyedén megtehetjük a [nyomtatás fájlba nevű trükkkel](#), de ki az az önként jelentkező, aki be fogja járni a fát, és minden egyes poszton ezt szöszmötölve elvégzi? Nos, igen, szóval senki.



Akkor hát automatizáljunk! A cél nem egy szofisztikált piaci alkalmazás, hanem csak egy olyan különbejáratú **saját használatra szánt, fatengelyes kis script** **segédeszköz összeütése, amely mondjuk max félóra alatt megvan**, és kényelmesen a már említett PDF formátumba lementené az eddigi összes blogbejegyzésünket az [antivirus.blog.hu](#) oldalról **anélkül, hogy a bemutatott fáradságos rabszolgamunkával napokig méltatlanul lódobogást kellene játszanunk a billentyűzeten**.



Kezdsenek a <http://antivirus.blog.hu/archive> link segít meghatározni, mikor indultak el a bejegyzések, nálunk ez 2007 szeptember volt. Aztán már csak annyi a dolog, hogy inntől kezdődően Krisztustól napjainkig mondjuk wget-ekkel leszedjük minden hónap összesítőjét egy-egy fájlba. Nagy ritkán előfordul, hogy nulla hosszúságú fájl keletkezik, akkor azt az egyet újra meg kell lőni (pont ezért készül külön, hogy látszon, ha esetleg valamelyik hibás).



Ezekből készül majd a **linkbányászás**, és az egyedi blogposztoknak a lementése DATUM_CIM.PDF névformátumban. **Vegyük észre, hogy a lementett havi HTML állományokban maguknál a bejegyzések címeinek kezdeténél szerepel az egyedi 'a class="post_anchor"'** fűzér, így számunkra ezek a sorok lesznek érdekesek.



A PHP (vagy Ruby, Perl, bármi) kódunk semmi mást nem csinál, csak **pillanatok alatt legenerálja az összes év összes hónap HTML fájljából az összes posztra vonatkozó sorokat** egyetlen nagy parancssori SH állományhoz, amelyik [egy ügyes segédprogrammal](#) majd aztán a megadott URL címeiről ténylegesen beolvassa a tartalmat és kiköpi azt PDF formátumban a következő wkhtmltopdf <url> <fájlnév> szintaktikával, pl.:

```
wkhtmltopdf http://antivirus.blog.hu/2007/09/22/hacktivity_2009 20070922_hacktivity_2009.pdf
```

Az összesítő **HTML-ek megdarálása után elindíthatjuk ezt a scriptet** és jöhet a nyolcfogásos ebéd, kávé, dohány, tabak és egyéb gyarmatáru, állatsimogatás, Scooby Doo maraton, etwas.

Kizárólag ez a munkafázis tart sokáig, futásához nálunk mintegy két óra kellett. Mikor aztán végül az összes poszt PDF-je elkészült, úgy éreztük, nehézkes és kényelmetlen, hogy minden bejegyzés egyesével külön fájlban van, és ez a későbbi tematikus keresgélést is megnehezítheti. Ezért úgy döntöttünk, **legyen minden egyes évfolyam összefogva egy nagyobb PDF-ben**, ez a művelet percek alatt abszolválható volt. Ehhez a GhostScriptet használtuk, ami pikk-pakk össze is fűzte a kért fájlokat.



Az ősi mondás szerint minden programban van legalább egy változó, egy elágazózás és egy hiba :-). A fenti módszerünk azokat a blogokat kezelte jól, ahol egy hónap bejegyzései egy oldalra kifertek. Mi direkt nem nehezítettük meg a saját dolgunkat, és ezért 25-re vettük az admin beállításoknál az egy lapon megjeleníthető bejegyzések számát, ennél több nálunk egyik hónapban sem keletkezett. **A lementett bejegyzések egyébként tartalmazzák az esetlegesen keletkezett kommenteket is**. Amit ez a technika nem tud: csak kis méretben szerepelnek benne a képek, lehetne a kód rövidebb, lehetne a kód szebb, biztos másképp is lehetne, meg különben is, továbbá automatikusan felismerhetne minden blog.hu doboz elrendezési sablont, valamint Alt+F1-re masszírozhatná a hátunkat és behozhatná nekünk a sört a hűtőből ;-)



Maga a leszedés és konvertálás hiába tart egy combos 2GHz Intel Core Duo, 4GB RAM gépen 1-2 óráig, mindez nem igényel semmilyen extra felügyeletet vagy plusz beavatkozást, hiszen közben nyugodtan lehet elmélyülten dolgozni (pl. az Angry Birds csúzlival gyakorolni) vagy akár el lehet menni addig is kávézni, ebédelni, aludni, fenyőfát venni, etc.



Szóval bitfaragás közben mi magunk is láttuk a korlátokat, meg hogy lehetne még mit csiszolgatni rajta, de **a befektetett félóra egységnyi energia láthatóan busásan megtérült, szenvedésmentesen hozta a kitűzött célokat**. És emellett egy az egyben, vagy mindössze minimális módosítással aztán bármelyik más blog.hu napló archiválását is elvégezhetjük így, nálunk például a [konteo évfolyamok](#) már itt figyelnek, be vannak spájzolva hideg csillagfényes téli estékre olvasgatnivalónak :-)

Végezetül, de nem utolsósorban minden Kedves Olvasónknak ezúton Kívánunk Kellemes Karácsonyi Ünnepeket!



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



Ajánlott bejegyzések:

- [Kiberzaklatás - mit tehetünk ellene?](#)

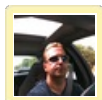
- [Majdnem mindenki átverhető adathalászattal](#)
- [Ez történik a weben egy perc alatt](#)
- [Elégedetlenek vagyunk a Facebook biztonságával](#)
- [Safe mód a Mechagodzilla ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2533330>

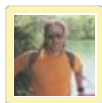
Kommentek:

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



[Benkovics Tomi 2010.12.24. 14:34:01](#)

Nagyon boldog Karácsonyt neked és a családnak is!



[Csizmazia István \[Rambo\] • http://antivirus.blog.hu](#)
[2010.12.28. 19:25:29](#)

Szia Tomi!

Hasonló jókat kívánok én is neked oda a nagy messzeségbe :-)

2010 trendjei

2010.12.28. 12:10 | [Csizmazia István \[Rambo\]](#) | [12 komment](#)

Címkék: [statisztika](#) [os böngésző trend](#) [2011](#) [2010](#) [kártevő](#)

Mik voltak a vezető kártevők, csalás típusok a hamarosan záródó esztendőben? Milyen böngészővel nézték legtöbben az Antivirus.blog-ot? Mik lesznek a jövő heti lottószámok? Összesítésünkben minden kiderül.



Ha a magyarországi adatokra alapozott havi toplista adatok "rémét" keressük, nem kell sokáig kutakodni, [ez egyértelműen a Conficker féreg volt](#). 2010-ben mindegyik hónapban az a Conficker féreg állt az első helyen, amely [az operációs rendszer frissítéseinek hiányát](#), a gyenge jelszavakat és az automatikus futtatás lehetőségét kihasználva terjed. Vezető helyét immáron 2009 novembere óta tartja, és a december havi, még le nem zárt adatok szerint most is az élen fog végezni.



Ha az év legnépszerűbb csalási formáját keressük, úgy a [hamis antivírusok és társaik](#) komoly eséllyel lehetnek dobogósak ebben a versenyszámban. Az ál antivírusok böngészés közben, fertőzött linkek, bannerek, weboldalak segítségével terjednek. Természetesen nem egy hagyományos ismert vírusirtóról, hanem egy kártékony, [az embereket becsapó és gépeinket megfertőző programról van szó](#), amely – nem mellékesen – még a pénztárcánkat is megcsapolhatja. A [nevüket már szinte képtelenség](#) listába foglalni, [havi több száz névvariációval](#) bővül, és [a bűnözőknek igencsak megéri](#) ezt a kétes foglalatosságot űzni. Ezért szinte minden 2011-es kártevő előrejelzés ezek további erősödését jósolja. A [pénzügyi adatok kifürkészése, a kémprogramok alacsony ára, és széles körű felhasználása komoly problémákat](#) fog okozni.



Az ESET 2011-es jóslatai szerint a [Facebookon és más egyéb közösségi oldalakon](#) is erőteljesebb kártevő tevékenység várható, és nagy valószínűséggel emelkedik majd a kereső találatok mérgezése, manipulálása (Blackhat SEO) is, valamint [a social engineering módszerek továbbra is](#) favoritok maradnak.



A blogunkra visszatérve a látogatóink böngészőinek tekintetében a néhány havonta ellenőrzött és most a legutóbbi hónap grafikonját megnézve [egyértelműnek látszik a Firefox letaglózó fölénye](#). Sajnos az OS felmérésünk hamvába holt a poll-r.hu leállásával, így [ezt újra kellett kezdenünk egy másik helyen](#). Ezekből egyértelműen látszik, hogy a **Windows tortaszelete a legnagyobb**.



Kevésbé édesszájúaknak az alternatív operációs rendszerek világából ott a Linux és a Macintosh. És bár az év vége az [OS X-re megjelent biztonsági csomagoktól](#) volt hangos, **2010-ben (még?) nem történt olyan mennyiségi áttörés**, ami jobban ráirányította volna a figyelmét a kártevőterjesztőknek, illetve [számuk még mindig az alatt a küszöb érték alatt lehet, hogy egyelőre nem éri meg rá tömegesen](#) kártevőket

fejleszteni.



Mindenesetre az biztosan látszik, hogy **lesz bőségesen téma a következő Boldog Új Esztendőre is**, így a blog szerzőjének internetes támadások vagy érdemi téma híján 2011-ben sem kell majd posztírás helyett [dizsműárúk és képes levelezőlapok terjesztésével](#) vagy dohány, tabak és gyarmatárú nagykereskedéssel foglalatzkodnia.

 Tetszik  Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

 Megosztás  +1 0  Tweet

Ajánlott bejegyzések:

- [Kártékony vírusok - villám őrjárat 8.](#)
- [Informatikai biztonság az egészségügyben](#)
- [Majdnem mindenki átverhető adathalászattal](#)
- [Ez történik a weben egy perc alatt](#)
- ["Szóölmédia" és nyaralás](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2543519>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.Bisex.hu](http://www.bisex.hu) •

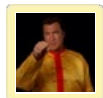
**<http://www.bisex.hu/aff/99e46a59d4f8188eda373d36ecd8cc3a>
2010.12.28. 16:03:27**

avg 2011-es vírusirtóját használom. nekem bevált, ingyenes



[;Viva La Onda! 2010.12.28. 16:57:26](#)

Ezt nem illik, itt az ESET termékeit kell futtatni. :) (Bocs Rambo, nem lehetett kihagyni a szurkapiskát.) Egyébként a 2011-es AVG-ben van rootkit-védelem?



[Cockpuncher • http://bornirt.blog.hu/ 2010.12.28. 17:24:56](#)

Az AVG Internet Security 2011-ben van rootkit-védelem. De úgy látom, a free edition-ben is: www.avg.com/us-en/free-antivirus



[;Viva La Onda! 2010.12.28. 17:25:56](#)

A free-re gondoltam, nem tudok áldozni fizetős cuccokra. Kösz az infot!



[;Viva La Onda! 2010.12.28. 17:27:35](#)

Bár ahogy elnézem az oldalán, szegény free-t eléggé kiherélték, nem tudom, megéri-e lecserélni az Avira-t?



[rotfl • http://kigondoltam.blog.hu 2010.12.28. 18:40:44](#)

Meglepő a szavazás szerinti 15%-os linux használat.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.12.28. 19:30:05

@rotfl

Sziasztok!

Hát igen, ez engem is meglep, mindig a Macet várnám másodiknak a summa windows után.

Gondolom ez valójában azt jelenti, hogy akik sokat olvasgatják ezt a blogot, azok közül sokan linuxoznak, és semmiképpen nem azt reprezentálja, hogy magyar viszonylatban ennyire népszerű lenne. Ott úgy 3-5 százalékra saccolnám az arányt - legalábbis desktopilag.



¡Viva La Onda! 2010.12.28. 22:19:39

Szerintem a linux elérhetőbb a nagy tömegeknek, a Mac-nél azért erős a sznobfaktor, amit az árak is tükröznek.



Csizmazia István [Rambo] • <http://antivirus.blog.hu>
2010.12.29. 08:28:42

Egyetértek Viva La Ondával. Ha nem nézzük most a wares aspektust, és ha az ember nem játékmegszállott, továbbá munkája miatt nem kényszerül olyan pajzanságokra, mint SAP, Macromedia Flash, AutoCAD, hajszál pontos Office kompatibilitás és hasonló, akkor igenis lehet jó választás a Linux.

Ebben a nagy monetáris restrikciónban ;-) szinte nem is lehet olyan megoldandó számítógépes feladatot találni, amire ne lenne ingyenes linuxos megoldás itt, míg a Win és Mac világban igen könnyű beleütközni a "ja ezt már csak fizetős program tudja" dolgokba, ami kétségtávol egy kellemes tiszta, száraz érzés.



Benkovics Tomi 2010.12.29. 14:53:44

@Viva La Onda:

Szerintem a "sznob-faktor" nem olyan döntő tényező, mint sem, hogy mit kapsz a pénzedért... Csak nézd meg a kapott ingyenes szoftvereket, az energia takarékoságot, az Apple által nyújtott terméktámogatást, (ez lehet MO-n nem olyan jó, de azt nem tudom...) és nem utolsósorban a design-t!

A sznobizmus szerintem a Bentley-nél kezdődik, ami kényelmetlen, sokat fogyaszt és még ronda is.



¡Viva La Onda! 2010.12.29. 19:56:04

Sejtettem, hogy megtalál a rajongótábor. :)



rotfl • <http://kigondoltam.blog.hu> 2010.12.30. 10:56:38

@Csizmazia István [Rambo]:

Lehetett több választ is adni? Mert mégis csak furcsa, hogy a linuxosok szeretnek olyasmit olvasgatni ami nem is érinti őket. :) Én inkább arra tippelnék, hogy linuxot is használnak miközben wines rendszereket gyógyítgatnak esetleg vagy ilyesmi. Én is linuxot használok itthon, de nem szoktam vírusokkal kapcsolatos híreket olvasgatni, pedig napi szinten wines rendszerekkel vagyok kapcsolatban.

Egyébként az egy hónapos otthoni NOD-os licenc nem fog esetleg változni? Elég sok home gépet láttam ahol rég lejárt licenc mellett kapták be a sok nyálókát a jüzerek, mert elég körülményes móka a havi csere-bere. Bevallom, az avast módszere szimpatikusabb.

BÚÉK 2011!

2010.12.30. 17:45 | [Csizmazia István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [szilveszter](#) [buék](#) [top5](#) [évvége](#)

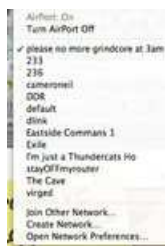
Itt a Szilveszter előtti utolsó nap, megnézzük antivirus **blogunk idei legnézettebb posztjainak Top 5-ös listáját**, és közben emeljük poharunkat húsz forintól huszonötre.



Végigtekintve a statisztikán, **az alábbi cikkek kapták a legnagyobb figyelmet 2010-ben.**

1. [Cenzúrázzák az SMS üzeneteket](#)
2. [Tíz gyanús jel, hogy zombi-e vagy](#)
3. [Mivel nyissunk meg PDF-et?](#)
4. [Minden, amit a privacy-ról tudni akartál... II. rész](#)
5. [Deaktiválták a Facebook hozzáférsünket](#)

Búcsúznak az Óévtől a blog szerkesztői, tanácsadói testülete, a teljes jogkörrel felruházott igazgatótanácsi tagság, valamint a felügyelő bizottság, és a felügyelő bizottságot felügyelő bizottság tagjai: Barkács Pajtás, Broádfa Abgeschtürchen Ottokár és Kovács N. Brezsnyevke. Év végi válogatásunkban első helyen [néhány felejthetetlenül emlékezetes nevű internetes WiFi elérés](#) szerepel, majd **az igényes szórakoztatás jegyében további intellektuális képgaléria** következik alant.





		
	Stone (40,000 B.C.)	iPhone 3G (2006)
SMS	X	X
Video recording	X	X
Video call	X	X
Changeable memory cards	X	X
Touchscreen	X	✓



Zárásként pedig megköszönjük az idei figyelmet, és vírusmentes Boldog Új Évet Kívánunk minden Kedves Olvasónknak az alábbi két viccel és egy videóval!

"Lány és fiú beszélgetnek. Kérdezi a fiú:

- Mi a foglalkozásod?

- Az EDS Hungary EMEA North-Central HUB Központjában az ABN AMRO Team-hez tartozó Workplace Services Service Deskjén vagyok Chat Support Agent. És neked? - kérdez vissza a lány.

- Ács."

"Egy szőke pszichológusnő az iskolában kap állást. Rögtön az első nap meglát egy fiút, aki nem futkározik a többiekkel, csak áll magában. Odamegy hozzá és megkérdezi:

– Jól érzed magad?

– Jól.

– Akkor miért nem futkározol a többi fiúval?

– Mert én vagyok a kapus..."

És a videó:



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



Ajánlott bejegyzések:

- [Kártyakönyv böngésző kiegészítők jönnek](#)
- [Az XP él, az XP élt, az XP élni fog](#)
- [Hogyan szűrjük ki a gyanús Android appokat?](#)
- ["Szósölmédia" és nyaralás](#)
- [25-ször több a mobilos kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/2548361>

Kommentek:

A hozzászólások a [vonatkozó jogszabályok](#) értelmében felhasználói 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.