Amikor a frissítés okozza a bajt

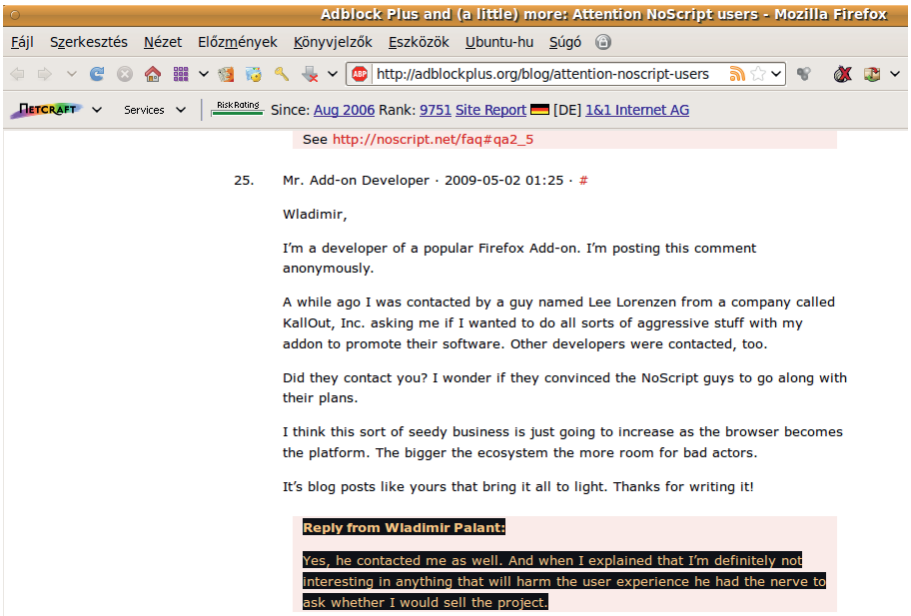
Frissen és fiatalosan

Sorozatunk előző részében arról beszélgettünk, mit kell tennünk annak érdekében, hogy rendszerünk friss, vagyis sebezhetőségmentes maradjon. Most, a 32. epizódban arról lesz majd szó, mikor rejthet magában veszélyeket a frissítés.

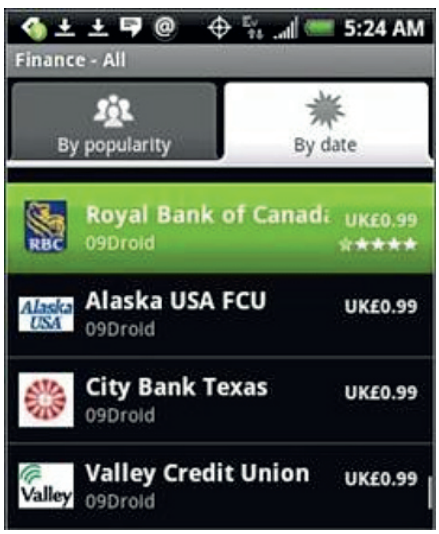
A korrektséghez hozzátartozik, hogy az ilyen frissítési balesetek viszonylag ritkán fordulnak elő, de kétségkívül léteznek, valós veszélyeket jelentenek, ha mégoly ritkán is. Következzenek az ilyen, mind a felhasználó szempontjából, mind pedig a kibocsátó szempontjából kínos esetek.

2007. 08. 16.: Ubuntu ungabunga

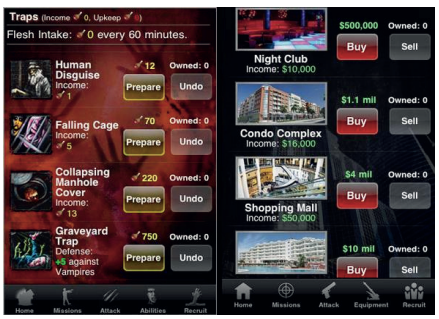
Korábban már láttuk, hogy a trójai programokkal való megfertőződés egyik legfőbb oka a megbízhatatlan helyekről való letöltés. 2007. augusztus 16-án kiderült, hogy a Canonical csoport anyagi támogatásával fenntartott nyolc Ubuntu fejlesztői kiszolgáló közül öt fertőzöttnek bizonyult. A szervereket önkéntes rendszergazdáknak kellett volna karbantartani – erre azonban gyakorlatilag nem került sor. A vizsgálat során a szerveren futó mindegyik olyan szoftvert, amelynek a pontos verziószáma egyáltalán megállapítható volt, biztonsági szempontból elavultnak találtak. A nagy veszély abban állt, hogy ha a támadók esetleg hozzáfértek volna a forráskódokhoz és a hivatalos bináris csomagokhoz (futtatható formára lefordított fájlok), saját kártékony kódjaikkal észrevétlenül megtoldhatták volna azokat, így minden, a fertőzött szervert használó Ubuntut telepítő vagy azt frissítő gép megfertőződhetett volna. Emiatt végül az üzemeltetők kénytelenek voltak a korábbi dátumú, biztosan tiszta mentésből visszaállítani egy fertőzetlen állapotot és ebből töltötték fel végül a szervereken tárolt tartalmakat. (Forrás: hopp.pcworld.hu/6831)



Érdekes levelezés az Adblock Plus fórumán: ez tanúsítja, hogy több Firefox addon-fejlesztőt megkereste már egy *Lee Lorenzen* nevű úriember egy KallOut nevű cégtől, és érdeklődött arról, hogy hajlandók lennének-e bizonyos „agresszív viselkedést" beépíteni a programjukba, amellyel reklámoznák a megbízó szoftverét. Ők állítólag nemet mondtak, ami lehet, hogy így van, lehet, hogy nem, és ki tudja, még kiket kerestek meg, amiről pedig nem is tudunk



Már egy androidos program is lelepleződött. A Droid09 nevű szoftver a felhasználók banki adatait próbálta megszerezni. Az Android Marketplace kínálatából azóta eltávolították az inkriminált alkalmazást



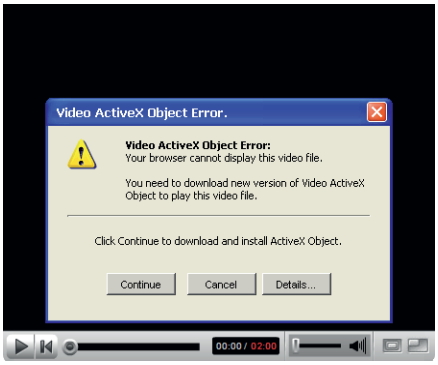
Az Apple iTunes App Store-ban elvileg csak szigorúan ellenőrzött szoftverek lehetnének. Van azonban precedens arra is, hogy egy váratlan frissítéssel trójai funkciók is belekerülnek egy korábban biztonságos alkalmazásba – ilyen volt például az iMobsters vagy a Vampires Live. Amíg az első fecske le nem lepleződik egy blogban vagy egy nyilvános fórumon, addig minden letöltő vagy frissítő áldozatul eshet

2008. 02. 18.: Firefox 2.0 nyelvi pack trójaival

Hogy ki melyik országba születik, és melyik nyelv az anyanyelve, az szerencse kérdése. Aki vietnami illetőségű, és ekkoriban letöltötte a Firefoxhoz való vietnami nyelvi csomagot, az egy trójait is kapott vele. (Forrás: hopp.pcworld.hu/6832)

2008. 05. 22.: a vírusirtó tiszta állományokra riaszt

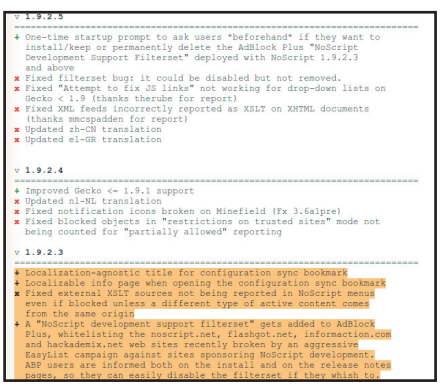
A vírusirtók esetében az adatbázis-frissítés az esetek 99,99 százalékában problémamentesen zajlik. Ezzel együtt minden gyártó esetében előfordult már egy-egy hiba. Sajnos ilyen eset már velünk is megtörtént, az ESET a megszokott alapos ellenőrzés dacára egy olyan NOD32 szignatúrafrissítést bocsátott ki, amely a gépek egy részén furcsa dolgo-



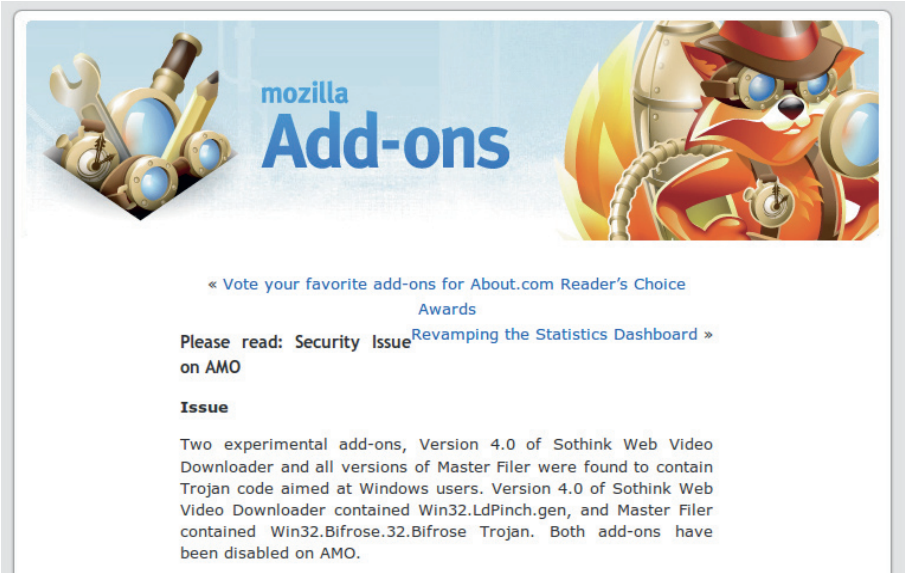
Ez a történet már szinte szakállas. Felugrik egy ablak, hogy frissítsük a kodeket, mert csak akkor tudjuk megnézni az állítólagos videót, amire szükségünk van (van?). Kodek helyett persze kártevő érkezik, de szakáll ide vagy oda, még mindig vannak, akik bedőlnek egy ilyen olcsó trükknek, akár OS X-en is

kat művelt. A 3119-es számú szignatúrafájl, amelyet 2008. május 22-én 10:45-kor adtak ki, néhány gépen tiszta fájlokra is riasztott, egyes esetekben pedig lefagyást eredményezett. A probléma kizárólag a vírusirtó 3.0-s változatát érintette. A laborba hamar eljutottak a visszajelzések, és a 3121-es, 13:40-kor kiadott javított adatbázis korrigálta a hibát. A mintegy három órán keresztül fennálló gond a felhasználók töredékét érintette, mivel ahhoz, hogy adatbázis-problémát okozzon, nem csupán az kellett, hogy a kritikus időszakban kerüljön frissítésre a vírusirtó, de az is, hogy a felhasználó ugyanekkor indítson el bizonyos (például Adobe-os) alkalmazásokat.

A teljes AV-mezőnyt vizsgálva nem egyedi eset, a különféle vírusvédelmi programoknál sajnos többször is történt már hasonló probléma. 2007 decemberében a Kaspersky azonosított tévesen a Windows Explorerben kártevőt, míg 2007. június 27-én a VirusBuster frissítése és az APEH Abev programja ve-



Háború tört ki 2009 májusában az Adblock Plus és a NoScript fejlesztői közt. A NoScript titokban úgy frissítette a programját, hogy az AdBlock Plus ne legyen képes letiltani a NoScript weboldalairól a hirdetéseket



2010. február 25-én röppent fel a hír, miszerint két kísérleti stádiumban lévő Firefox-kiegészítő is fertőzött volt. Bár az utólagos vizsgálatok megállapították, hogy a Sothink Video Downloader 4.0-s verziója esetében ez csak vaklárma volt, ám a másik, Master Filer nevű kiegészítés valóban tartalmazott kártékony kódot

szett össze. Ugyancsak hasonló esetek történtek például a Nortonnál, ahol rendszerfájlok kerültek indokolatlanul karanténba, illetve 2006-ban a McAfee háza táján is volt egy hasonló sajnálatos esemény. Szerencsére az ilyen esetek rendkívül ritkák, mivel a frissítés kibocsátása előtt a gyártók nagyszámú tiszta állomány esetében is ellenőrzik, hogy valóban vakriadómentes-e az új szignatúra. Ilyenkor a versenytársak sem nyilatkoznak kárörvendően – nem ritkán technikai segítséget is nyújtanak egymásnak, ha ez szükséges –, hiszen tudják, ez a veszély Damoklész kardjaként egyformán ott lebeg mindegyikük feje felett. (Forrás: hopp.pcworld.hu/6833)

2009. 01. 13.: Seagate firmware-frissítés katasztrofális következményekkel

2009 januárjában kínos élményben volt része a Seagete 3,5 hüvelykes 7200.11-es és ES.2 sorozatú Barracuda, illetve Maxtor DiamondMax 22 merevlemez-tulajdonosoknak. Megjelent ugyanis egy olyan SD1A verziójú firmware-frissítés, amely azt ígérte, hogy BIOS-kompatibilitási problémákat fog megoldani, valójában azonban ez a szoftverfrissítés teljességgel blokkolta és megakadályozta az adatok további elérését. A cégnek emiatt bocsánatot kellett kérnie, valamint kártérítést kellett fizetnie a bajba került ügyfeleknek, és nemcsak az eszköz értékét, hanem az adat-visszaállítás teljes költségét is állták. (Forrás: hopp.pcworld.hu/6834)

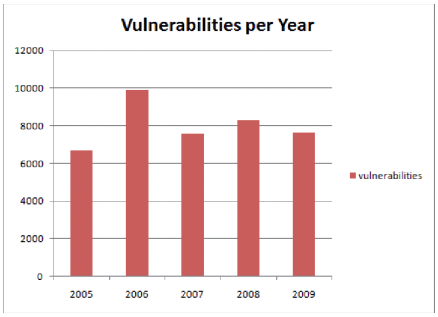
2009. 05. 05.: NoScript vs. AdBlock Plus csörte

A NoScriptet rengetegen használják világszerte, hiszen a weboldalak automatikusan futó JavaScript kódjai ellen igen hatékony eszköz. Az egyik frissítésével azonban érdekes helyzetet idézett elő, és egyúttal meg is sértette vele a Mozilla addon-készítőkre vonatkozó szabályozásait. A botrányt az Adblock Plus és a NoScript fejlesztői közt kitört háborúskodás okozta, ennek hátterében hirdetések és az ezekből befolyó bevételek álltak. A NoScript úgy alakította át programját, hogy az AdBlock Plus ne tudja letiltani a NoScript weboldalairól érkező hirdetéseket, amihez természetesen nem lett volna joga. A probléma leginkább az volt, hogy mindez titokban történt, és a felhasználók soha nem tudtak arról, hogy a NoScript bizonyos JavaScriptek futtatását mégis engedélyezte a gépükön.

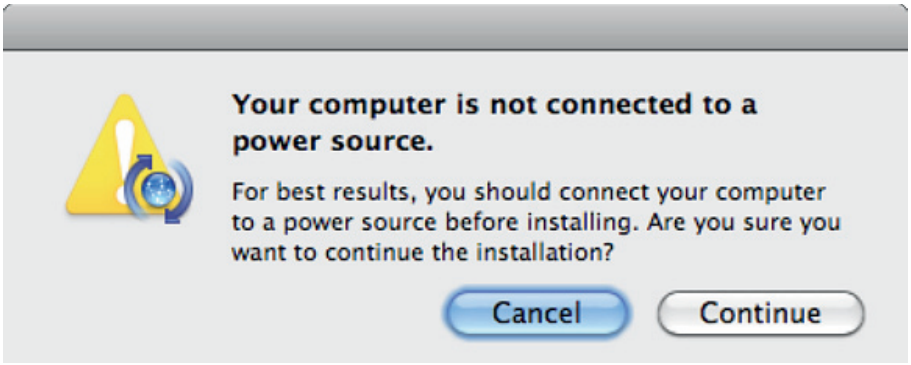
Giorgio Maone, a NoScript szerzője a vádak nyilvánosságra kerülése után aztán egy hosszú blogbejegyzésben kért bocsánatot. „Kérlek titeket, fogadjátok el legőszintébb bocsánatkérésemet és higgyétek el, hogy szégyellem magam és megbántam, amit tettem. Tudom, hogy olyan szörnyűséget tettem, ami még nem fordult elő a Mozilla-közösség történetében, s ezzel sok ember bizalmát veszítettem el. Kérlek titeket, segítsetek abban, hogy helyrehozhassam, amit okoztam a hibáimmal." (Források: hopp.pcworld.hu/6836, hopp.pcworld.hu/6835)

2009. 05. 21.: Firefox-kiegészítők – időzített bomba

Néha érdekes levelezést lehet olvasni az Adblock Plus fórumán. Ennek tanúsága szerint



Megdöbbentő az a grafikon, amelyen az évente megjelenő exploitok, azaz sebezhetőségek száma szerepel. Ha most figyelmen kívül hagyjuk a 2006-os kiugrást, látszik, hogy a számok évről évre folyamatosan növekednek



Még ha semmiféle veszélyes letöltés sincs a láthatáron, akkor is érdemes figyelni arra, hogy hálózatról vagy akkumulátorról járatjuk-e a gépet az operációs rendszer frissítésekor. Erre mindhárom rendszer, a Windows, a Linux és a Macintosh is példásan figyelmeztet

a bűnözök üzemszerűen keresik meg a Firefox addon-fejlesztőket, és rendre „bepróbálkoznak" náluk. Jó esetben a szakértők nemet mondanak nekik, akik között a kéretlen reklámok terjesztői szándékosan keresnek olyasvalakit, akiknek már ismert a neve, és felfuttatta a programját. Ha az ilyen, 180 Solutions-jellegű cégek bevásárolnak, akkor a bizalomra épülő addonhasználatnak könnyen vége lehet. Épp emiatt rizikós a kísérleti (experimental) besorolású kiegészítők letöltése, de a hivatalos oldalról leszedett addonokat is csak saját felelősségre telepítsük.

2009. 11. 11.: az első iTunes-fecske

Miénk a trójai, magunknak telepítjük – akár így is lehetne fogalmazni, ha azt kérdezi tőlünk a medve, hogy mondd csak, te vadász, miért is jársz az iTunes App Store-ba? Ez az a terület, ahol még a leggyanakvóbb ember is csapdába eshet. Nem látunk bele a letöltendő programba, így az open source-szal szemben itt jobb híján kénytelenek vagyunk a bolt üzemeltetőjében, azaz az Apple-ben megbízni. Valamennyire tájékozódhatunk az interneten, de ez is maximum akkor óvhat meg bármitől, ha már egy ideje ismert valamilyen anomália, vagyis jobbára már csak eső után van esélyünk köpönyeget találni.

2009 novemberében az Egyesült Államokban, Észak-Karolinában indult per a Storm8 fejlesztők ellen, mert az ingyenesen letölthető játékaik – mint például az iMobsters vagy a Vampires Live – egy beépített hátsóajtón keresztül, titokban továbbították a fejlesztőknek a felhasználók telefonszámát, illetve telefonkönyvükben szereplő számokat, hogy ösztönözhessék őket a teljes változat megvásárlására.

A piszkos trükk kiderült, és most a fejlesztők azzal védekeznek, hogy ez a frissítés „véletlen programhiba volt". Az alábbi programok keveredtek gyanúba: iMobsters, Kingdoms Live, Racing Live, Rockstars Live, Vampires Live, World War, Zombies Live. Valószínűleg az App Store alkalmassági vizsgálói sokkal jobban odafigyelnek arra, hogy nehogy csorbuljon az Apple érdeke üzletileg, a biztonsági szempontok pedig másodlagosak. (Forrás: hopp.pcworld.hu/6837)

2010. 01. 11.: Androidra is van, naná

Nemrégen az említett, az iPhone programáruházához hasonló helyzet adódott az androidos telefontulajdonosok számára is azzal, hogy a Droid09 nevű alkalmazás lelepleződött. A program a felhasználók banki adatait próbálta megszerezni, azóta persze eltávolították a kínálatból. A történet viszont jó példa arra, hogy nagyon ínyencnek, tájékozottnak és válogatósnak (szerencsésnek?) kell/érdemes lenni, amikor ismeretlen szerzők alkalmazásainak telepítéséről van szó. Azonban sajnos szinte kivédhetetlen az az eset, amikor az alkalmazás új korában még sikeresen levizsgázik, így bekerül a bolt kínálatába – ekkor még korrekt, aztán pedig egy váratlan frissítéssel a bűnözők már bele is helyezik a trójai funkcionalitást. Ez pedig addig gyűjti magának a felhasználók adatait és rosszabb esetben pénzét, amíg észre nem veszik, és le nem leplezik. (Forrás: hopp.pcworld.hu/6838)

2010. 02. 04.: trójai Firefox-pluginok

Felröppent a hír, miszerint két publikusan letölthető Firefox-kiegészítő is fertőzött volt. Ezek kísérleti (experimental) stádiumban voltak ugyan, mégis több ezren letöltötték őket. Az egyik a Sothink Video Downloader 4.0-s verziója volt, a másik pedig a Master Filer nevű kiegészítő. A későbbi vizsgálatok azt jelentették, hogy a kiegészítők csak Windows platform alatt jelentettek veszélyt. A trójai komponensek váratlan felfedezésének okaként azt jelölték meg, hogy a korábbi egyetlen vírusvédelmi alkalmazás helyett most többel is ellenőrizték a kiegészítőket. Egy későbbi elemzés vakriasztásnak minősítette a Sothink programjában történt kártevő-detektálást, viszont megerősítette a másik kiegészítőben található trójai létezését. (Források: hopp.pcworld.hu/6839, hopp.pcworld.hu/6840)

Zárjuk a szót

Mindebből remélhetőleg sikerült felvázolni, hogy rendszerünk naprakészen való tartása nem egy egyszerű feladat; a szoftverek letöltése, illetve frissítése közben akkor is előfordulhatnak különféle biztonsági incidensek, ha a terrorista, pornó-, netán warezhonlapokról az sem tudjuk, hogy eszik-e vagy isszák azokat. A felsorolt példákkal természetesen nem a bajba került alkalmazások használatáról igyekszünk lebeszélni az embereket, inkább a nagyobb figyelem és a látókör tágítása volt a cél.

Remélhetőleg a Secunia Personal Software Inspector (secunia.com/vulnerability_scanning/personal/) hamarosan megjelenő 2.0-s programja segíthet átlendülni a Windows-felhasználóknak ezen a nehéz helyzeten, a fejlesztők ígérete szerint ott már a különféle alkalmazások mintegy 70-80 százalékához tudnak majd valamiféle automatizált frissítési megoldást biztosítani, amelyekkel pedig begyógyítják a támadható sebezhetőségeket. Vigyázni és óvatosnak lenni azonban továbbra is nekünk magunknak kell!

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

velemeny@pcworld.hu

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**)