# Miért jó a Linux a kíváncsi szemek ellen? - Ellenvélemény

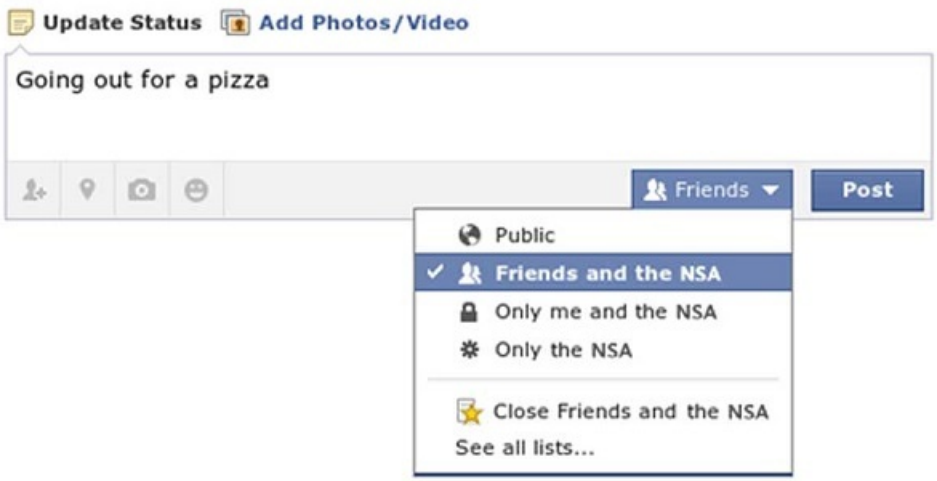
Elemzés – Írta: **Csizmazia István [Rambo]** | 2013-11-09 08:30

**Az Abszolút Biztonság nevű járatra nem vehetünk örök bérletet, pusztán egy operációs rendszerrel nem lehet megoldani minden problémát.**

## Bevezető

Mivel volt szerencsém már az első Chip-mellékletes Linuxok óta ezekkel az operációs rendszerekkel ismerkedni és dolgozni, és valamennyi időt úgy általánosságban a biztonsággal is foglalkozni, árnyalni szeretném azt a túlzottan leegyszerűsítő képet, amit a cikk címe és annak néhány állítása is sugall. A biztonságnak egyébként ez egy alaptétele is lehetne: pusztán azzal, ha valamit használok vagy beszerzek - például Linuxot -, még nem oldom meg minden biztonsággal kapcsolatos problémámat, mert ez nem biztonság, csak annak illúziója. A biztonság állandó figyelmet, folyamatos tanulást, munkát, törődést igényel, nem mellesleg a rendszerünk működésének átlátását, alapos ismeretét, megértését, és még ezzel együtt sem nyújt 100%-os garanciát semmire, csak csökkenti a kockázatokat. A cikk egyébként remek és hiánypótló, köszönet a szerző Egri Imrének, az alábbiakban azonban szeretnék kissé vitatkozni, néhol egyetérteni, másutt kiegészíteni, és tágítani a látómezőt. Összefoglalva: nem árt tudomásul venni, hogy nem vehetünk örök bérletet az Abszolút Biztonság nevű járatra.

Essünk gyorsan át a címmel kapcsolatos felvetésen. A nemzetbiztonságnak (és ez minden országban így van) működnek a törvényes lehallgatásnak, megfigyelésnek olyan formái, melyek a távközlési szolgáltatóknál, internetszolgáltatóknál ellenőrzik az adatforgalmat, és ebből a szempontból azt gondolni, ha valaki Windows helyett Mac OS vagy Linux alól netezik, akkor azt lehallgatásbiztosan tenné, vagy a *"Hárombetűs ügynökségek, trójaik, mindenre kíváncsi keresők"* így nem ellenőriznék, naiv tévhit. Ugyanakkor azt azért lehet vélelmezni, célul kitűzni, hogy a biztonságosnak gondolt, megbízható forrásból származó, például nyílt forráskódú alkalmazásokkal valóban lehet csökkenti a kockázatokat a zárt forráskódba esetlegesen elrejtett hátsó ajtós szoftverekkel, kártevőkkel, rosszindulatú támadókkal szemben. A platformonkénti kártevők mennyiségére később még kitérünk, most lépjünk inkább tovább.




Mit tud rólad a Facebook? Amit beírsz

Mindig minden szoftverben lehet találni sebezhetőségeket, a fejlesztés egy örök folyamat, amely sosincs kész, a felügyelet, a frissítés, a tesztelés mindig a felszínre hoz újabb és újabb foltoznivalókat. Más kérdés az, amikor valami szándékosan gyengít, és a Snowden-ügy bizony hozott fel ilyen információkat: Az NSA annak idején aktívan közreműködött az IPSec szabvány tudatos gyengítésében, de a DES algoritmussal kapcsolatban is történt ilyen beavatkozás a véletlenszám-generáló algoritmusban.

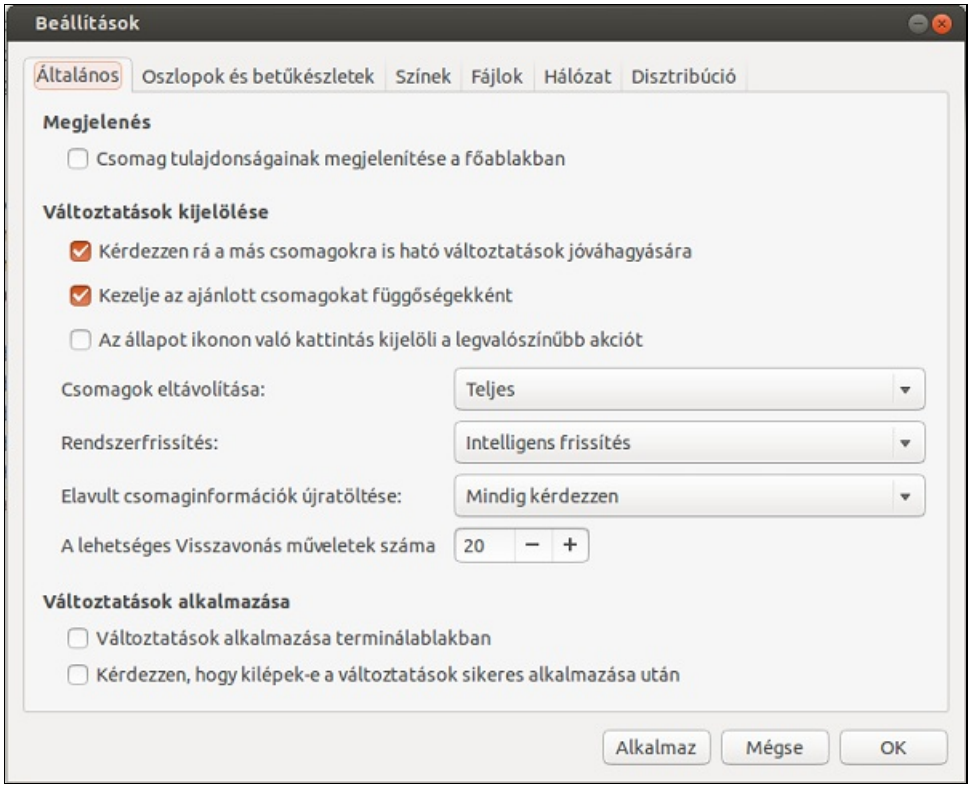
## Piszkos háttéralkuk

### Piszkos háttéralkuk

Innen futunk neki annak a 2008-as történetnek, amely francia földre visz, és idézzük róla a **beszámolót**. *"A szakértő a blogjában arról számolt be, hogy a védett tároló (Protected Storage, PStore) visszafejtésekor arra lett figyelmes, hogy a titkosítás megkezdése előtt ellenőrzésre kerül a Windows területi beállítások, és amennyiben a tartózkodási hely (Locale) Franciaországra van állítva (a GetSystemDefaultLCID() függvény 0x40C értéket ad vissza), akkor a véletlenszerű kulcs választása helyett a titkosítás egy mindig állandó kulccsal történik. Dave leírása szerint a francia kormány meglehetősen izgatott lett ennek hatására, pedig kiderült, hogy az egész eredetileg miattuk lett bevezetve."* Itt egy jellemző példa egyrészt arra, hogy a Microsofttal milyen alkuk köthetők, másrészt az izgalom ugye sosem attól van, hogy ilyenek egyáltalán találhatóak egy szoftverben, hanem mindig az a probléma, hogy ez aztán később kiderül.

Szándékos gyengítésen esett át a Skype is, ahol már a regisztrációkor aláírjuk, hogy a keletkező üzenetek nem a mi, hanem a cég tulajdona. Most azonban az is kiderült, hogy nem csak az alap kommunikáció, hanem a titkosított chatek és hívások is megfigyelhetővé váltak, ugyanis kilenc hónappal azután, hogy a Microsoft megvette a Skype-ot, úgy **alakították át** a programot, hogy még több információt gyűjthessen be az NSA. Itt egyébként néha a biztonsági szakma is meghasonlik önmagával, hiszen például korábbi tanácsaink közé

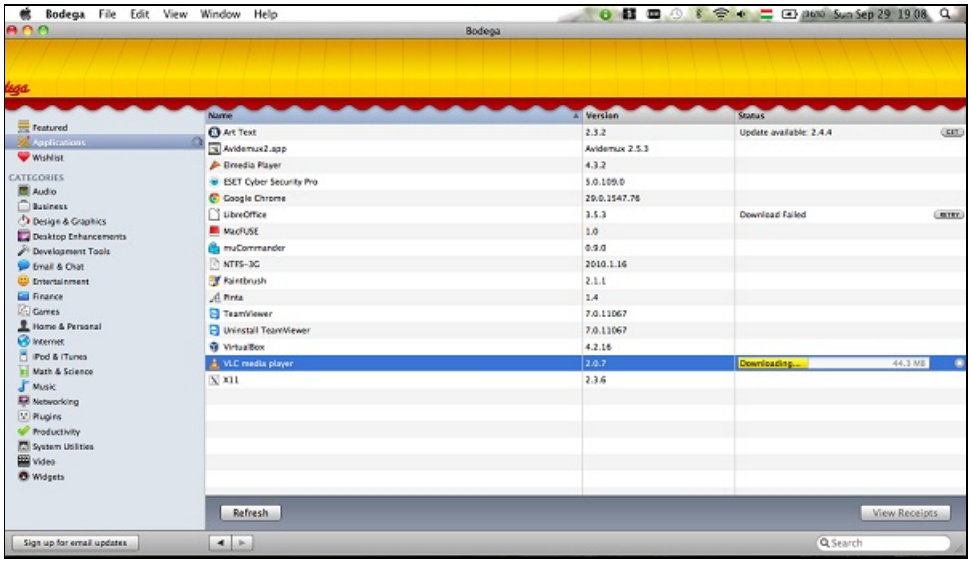
tartozott, hogy alkalmazzuk a titkosított beszélgetést, az teljesen biztonságos, aztán utóbb kiderült róla, hogy annyira azért mégsem az.




A rendszer minden telepített alkalmazás frissítését figyeli, aztán a felugró ablakban egy gombnyomásra el is végezhetjük a frissítést, miközben minden információt részletesen megismerhetünk

**Frissen tartó mechanizmusok**

A Javával kapcsolatosan elhangzott észrevételekkel egyetértek, bár azt hozzá kell tenni, ha valaki csak annyit tesz, hogy a Microsoft Office helyett a LibreOffice irodai csomagját használja, máris a Java használatára van kényszerítve. Az egységes rendszerfrissítést is fontos és kritikus pontnak látjuk, hiszen hiába van naprakész vírusirtónk, ha közben sebezhető, foltozatlan az operációs rendszer. Természetesen itt a Linux felhasználók vannak a legjobb helyzetben, hiszen az ottani frissítés elsőrangú: minden szoftverelemet, alkalmazást figyel, felugrik és figyelmeztet, beállítható, ütemezhető, LTS-re korlátozható és azonnal megkapjuk, naponta, vagy akár naponta többször is. Windows esetében ilyen beépített gyári alkalmazás nincs, az ottani frissítés persze automatizálható, de csak a Microsoft javításokra, ez általában az úgynevezett patch-kedd alkalmával, vagyis minden hónap második keddjén jelenik meg, bár rendkívüli esetekben jelennek meg azonnali javítások is. Az összes alkalmazás frissen tartása harmadik féltől származó programokkal oldható meg, ehhez például a **PSI (Secunia Personal Software Inspector)** az egyik legalkalmasabb segítség. A Mac rendszereknél is hasonló a probléma, bár egy fokkal jobb a helyzet, mert a Mac App Store-ból letöltött és telepített programok mindig jelzik, ha van elérhető frissítés, ha azonban más forrásból is szerzünk be alkalmazásokat, ezen a platformon is segédprogramot kell használni, például az AppBodega nevű programot. Itt a Windowshoz képest nagyot lépett előre az OS X, ugyanis a Mountain Lion óta a felhasználó napi automatikus rendszerfrissítéseket kaphat.




Ez a Bodega nem egy düledező viskó, hanem egy OS X alatti szoftverfrissítő

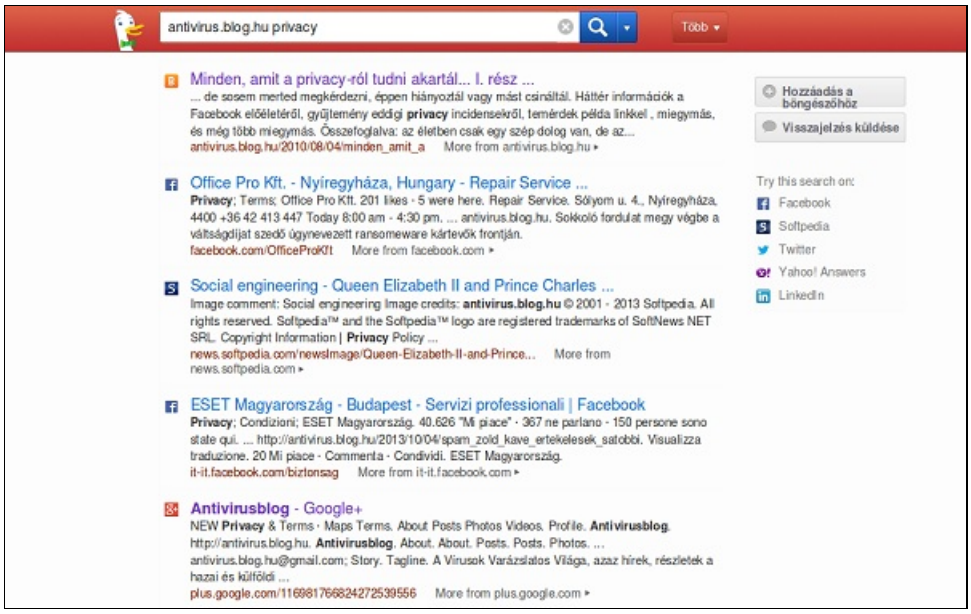
Ismét **idézünk** egyet: *"Kedvenc felhőszolgáltatóink nemigen indulhatnak mostanában a biztonságos chat rendszer versenyen, ezért*

*maradnak az önálló csevegőprogramok, mint a Pidgin és a Crypto.cat."* Anélkül, hogy mélyebben belebonyolódnánk, ismételjük magunkat: pusztán azzal, ha valamit használok, vagy beszerzek, még nem oldom meg minden biztonsággal kapcsolatos problémámat. Ehhez kis kitérőként megemlíteném azt az idén júliusi incidenst, amelynél a Cryptocat véletlengenerálással kapcsolatban merültek fel információk, amelyek miatt egy **meet-in-the-middle** támadással lehetővé vált a sérülékeny változatokkal generált kulcsok feltörése. Akit mélyebben érdekel, érdemes Buherátor erről szóló **cikkét** elolvasni, amiben van még egy, a történethez tartozó kínos baki, ugyanis a neves Veracode korábban már auditálta a Cryptocatet, de nem talált semmilyen problémát.

## Aki keres, az talál

Ismét idéznék a "Miért jó a Linux a kíváncsi szemek ellen?" cikkből: *"legismertebb közülük a DuckDuckGo. Az oldal nem tárolja a kereséseket, nem adja ki harmadik félnek, így – amennyire ez jelenleg tudható – biztonságban érezhetjük rajta magunkat. Persze nem lesznek „gondolatolvasós" találatok, kicsit döcögősebb lesz vele az élet."* A törekvés és a cél tökéletesen világos, de a DuckDuckGo egyelőre nem fogja leváltani a hatékony keresésben sokkal jobb Google-t. Itt nem a "gondolatolvasás" hiánya okoz gondot, hanem az, hogy a találatai messze nem annyira használhatóak. Itt tehetünk is egy próbát, írjuk be például, hogy "buherator ssl" vagy "antivirus.blog.hu privacy". A Google-nál az első három, de sokszor az első tíz is ilyen témájú poszt az adott blogról, míg a duckduckgo esetében csak maximum egy blogposzt van a találatok között, a többi irreleváns. Természetesen még fejlődhet Kacsa úr is, arra viszont nincs garancia, hogy később nem fogják mégis tárolni a kereséseket.

Ha már biztonság és élveboncolás, akkor még egy apró pici észrevétel a "UAC kontra sudo/root" fejezethez. Programfuttatásnál a sudo helyett inkább gksudo-t érdemes használni, mert míg a sudo a felhasználó konfigurációs fájlját használja root jogokkal, a gksudo a root konfigurációs fájlját használja ugyanitt.



Úgy tűnik, nem a DuckDuckGo-val a legérdemesebb keresni a blogarchívumunkban

**A gravitáció nem ismerete nem mentesít a zuhanás alól**

Jöjjenek a vírusügyek. *"Egy józanul használt Linux rendszer a szoftverek valamint kártevő- és vírusbiztonság tekintetében szinte garancia"*. Erről a biztonsági szakembereknek az a véleménye – és erre tucatnyi példát lehet hozni –, hogy biztonság akkor van, ha ezt valamilyen módon ellenőrzöm és az adott pillanatban úgy találom. Ellenőrzés nélkül nem létezik biztonság. Egy Linux rendszeren sem árt egy jó tűzfal, valamint az ismeretlen forrásból származó programok telepítése ott is veszélyforrás lehet, hiszen tudatlanul (**PEBKAC**) trójai kodeket ott is le lehet tölteni. Van egyébként vírusirtó Linuxra is, igaz, többségük nem állandó védelmet ad, hanem lehetőséget a kézzel indított keresésre, ami jól jöhet, ha Windowsos gépekkel vagyunk kapcsolatban. Mivel a hárombetűsök és a kártevőterjesztő bűnözők egyaránt vásárolják a sebezhetőségeket, így az ezek ellen való védekezés nagyon fontos. Mellesleg aki akár Macet, akár Linuxot használ, az heti-havi rendszerességgel nézzen rá az **RKHUnterrel**, meg a chkrootkittel, hiszen a rootkitek először történelmileg éppen Unix környezetben jelentek meg.

Abban volt az Apple óriási tévedése is, hogy sebezhetetlennek gondolta magát, persze 130 millió vírus helyett Linux és OS X alatt csak kb. 10-15 ezer kártevő létezik, ám védekezni mindenhol kell, maga a platform nem ad felmentést, emlékezzünk csak a 2012-es **Flashbackre**, ami 600 ezer OS X-alapú gépet fertőzött meg botnetes kártevővel - felhasználói közbeavatkozás, kattintás nélkül lefutva. El kell fogadni azt, hogy pusztán szemmel nem lehet mindent észrevenni, jó programokkal viszont annál inkább. Mark Russinovich is a SysInternals Toolsszal vette észre a Sony rootkitet, nem szemmel veréssel, miközben a felhasználóknak meg csak az tűnt fel, hogy nem tudnak CD-t másolni, vagy a másolási kísérlet után eltűnik a CD/DVD meghajtó a legördülő eszközök közül.

És ha már mindenkit kritizálunk itt nyakló nélkül, érdemes végiggondolni azt is, mekkora kárt okozott az a hozzáállás, hogy egyedül csak a jogtiszta Windows és Office alkalmazhatja a biztonsági frissítéseket? Vajon az elmúlt évek alatt mennyiben járult hozzá mindez, hogy 130 millió vírusnál is több van erre a rendszerre? A választ az olvasó képzeletére bízom.

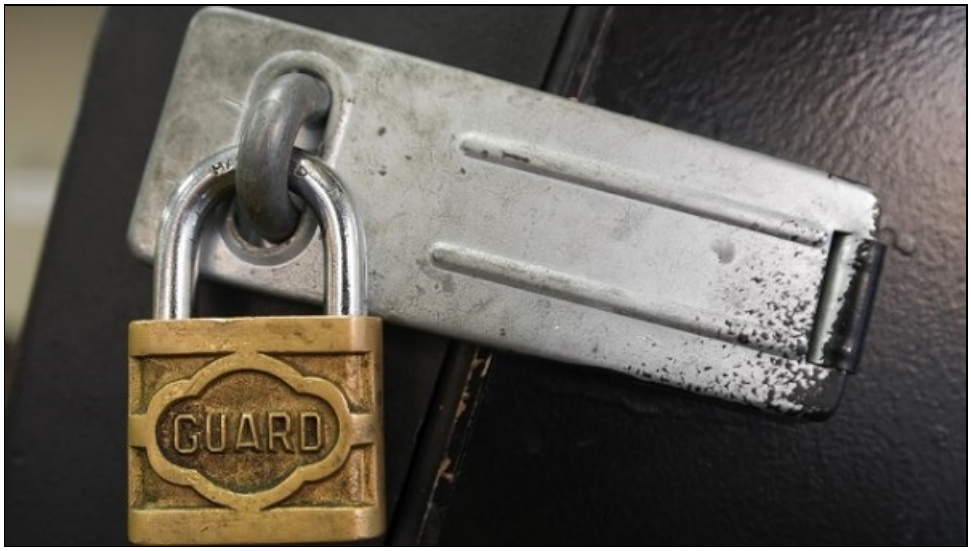
## Híres Linuxos incidensek

**2007. augusztus**

2007. augusztus 16-án **kiderült**, hogy a Canonical csoport anyagi támogatásával fenntartott nyolc Ubuntu fejlesztői kiszolgáló közül öt fertőzött. 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 találták. 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.

**2009. december**

A Gnome-look.org oldalon található képernyővédő "érdekességeiről" két külön topikban is értekeztek, egy UbuntuForumos és egy másik Kubuntus beszélgetés is írt a részletekről. **Az történt**, hogy a képernyővédő mellé titokban érkezett még egy DDoS támadásokhoz is használható extra script az áldozatok számítógépére. A gyanús .DEB csomagot időközben már leszedték a Gnome-look.org weboldalról. A nagy tanulság annyi, hogy hiába van ott a nagyságrendekkel biztonságosabb alternatív platform (vírusok és férgek szempontjából), ha helytelen hozzáállással ellenőrizetlen és megbízhatatlan forrásból való telepítéssel saját magunk ártunk magunknak. GPG-vel alá nem írt, illetve nem hivatalos tárolókból, nem megbízható fejlesztők weboldaláról letöltött tartalom mindig lehet ilyen gyenge láncszem.




**2013. április**

Felbukkant a Linux/Cdorked malware kapcsán egy Apache-kompatibilis károkozó. A telemetriai adatok szerint már 2012 decemberében aktivizálódott, és észrevétlenül hátsó ajtót hozott létre a kiszolgálókon, átirányítás kártékony oldalakra, DNS hijacking, stb. A naplóállományokból nem volt kimutatható, mert csak a memóriában található, ezért szerver oldalon integritásellenőrzéssel lehetett kiszűrni.

A mentések fontosságához tényleg csak egyetlen érdekes adalék, és mindenki döntse el, valóság vagy illúzió a biztonság. Most ne tekintsük az összeesküvés-elméleteket a Word Trade Centerről, egyedül csak a mentési struktúrát nézzük: az egyik toronyban volt az éles szerver, a másik toronyban a mentés szerver. Ember tervez, igyekszik mindenre gondolni, de itt megtörtént a váratlan, a hihetetlen: pontosan 30 perccel élte túl az egyik torony a másikat, és a mentésnek annyi lett.

## Összegzés

A hárombetűsek ellen igen keveset tehetsz, ebben jellemzően nem az operációs rendszered, hanem az eszközeid és a hozzáállásod fog dönteni: GPG, nyílt forráskódú eszközök, SHA512 ellenőrzés telepítés előtt, egyedi és erős jelszavak, lokális titkosítás, stb. Nekik az a dolguk, hogy ott legyenek a forrásnál: az internetszolgáltatónál, a mobilszolgáltatónál, és vagy automatikusan, vagy külön kérésére megkaphassanak bármit. Aki óvni akarja a magánszféráját, mert nyomós oka van rá, vagy, mert nem akarja, hogy átjáróház, nyitott könyv legyen a magánélete, tegyen érte. Egy nyomozás során, törvényszéki szakértői fronton ugyanúgy vissza lehet követni egy lefoglalt Linuxos vagy Mac gép böngészési és minden egyéb előzményét, mint a Windows esetében. Ha viszont valaki **Crypto-FS-t** használ, **GPG-vel** levelezik, **Truecryptes** tárolókban tartja az anyagait, azzal megtett minden tőle telhetőt akár lefoglalják, akár ellopják a gépét. Ami még érdekes, országa is válogatja, hogy például a hatóságok által lefoglalt géphez meg kell-e adni a jelszót. Angliában például, ha nem árulod el, 3 év börtönnel sújthatnak terrorizmus gyanújával. Persze ehhez rögtön hozzá lehet fűzni, hogy egy pedofil, egy drogkereskedő vagy egy terrorista inkább nem árulja el, és ül 3 évet, mint hogy minden kiderüljön róla, és akkor kapna 33-at.

Nincs olyan operációs rendszer, amit nem kell alaposan megismerni ahhoz, hogy megvédhesd. Nincs olyan operációs rendszer, ami automatikusan 100%-os védelmet nyújtana. Egy felhasználó maximum megbízhat ezekben, és abban, hogy ha hosszú távon rosszat akarnak neki, akkor jön egy **Mark Russinovich** és kiborítja a bilit, mint az emlékezetes Sony DRM esetében. Jó kompromisszum létezik csak, és hasznos szokások, megfelelő hozzáállás, hadra fogható alkalmazások. **Miko Hypponen** szerint a nyílt forráskódú rendszerek

jelenthetnek megoldást, és ehhez adalék lehet **Bruce Schneier** amerikai biztonsági szakértő korábbi nyilatkozata is: *"A nem nyílt forráskódú programokat az Amerikai Egyesült Államok Nemzetbiztonsági Hivatala (NSA) könnyebben láthatja el kiskapukkal."*


A felhasználó képzése, biztonságtudatossága, illetve ennek hiánya bármilyen rendszert fejre állít, lásd **ezt a felmérést**. *"A 18-29 évesek 17%-a szokta kikapcsolni a vírusirtóját azért, hogy fertőzött fájlokat tudjon elindítani, 12%-uk pedig azért, hogy fertőzött weboldalakat látogathasson."*

Szokott még érv lenni az “én okosan böngészek”, ebben én nem hiszek, bármelyik weboldal vagy banner tartalmazhat ismeretlen kódot, scriptet. Vagy nézzük meg, a magyarok hogy vizsgáznak biztonságtudatosságból, hányan iratkoztak le két évvel később az előrelájkolós "Mi az indián neved?" alkalmazásról a Facebookon? Szinte senki. A Socialbakers oldalon most is vezeti **a magyar brandek listáját**, az Extreme Silver ékszerbolt olyan jelentéktelen, "futottak még" márkákat előz meg, mint a McDonald’s, Samsung, Túró Rudi, Coca Cola, Disney, Tesco, vagy Vodafone.

Zárás előtt egy kommentet idéznénk: *"Webes exploitok mellett már nagy divat a PDF-be ágyazott Acrobat Reader sebezhetőséget kihasználó kártevő. Igazából AV nélkül amit csinálsz orosz rulett. Ráadásul, a felelőtlenséged másokat is veszélyeztet. A géped fertőzési gócként küldheti a kártevőket bárkinek."*

A biztonság olyan, mint a buddhista tökéletesség, elérni sosem lehet, de törekedni azért ennek ellenére lehetőségeink és tudásunk szerint állandóan kell rá: megbízhatónak vélt eszközök választásával, saját adataink titkosításával és gyakori mentésével, digitális aláírással, egyéb megfelelő magatartással.

**Csizmazia István, IT biztonsági szakértő**

**antivirusblog.hu**