PCWorld FÜZETEK VI.

AZ INTERNET VESZÉLYEI

MODERN FENYEGETÉSEK ÉS ELLENSZEREIK

tartalom

impresszum

SZERKESZTŐSÉG

Főszerkesztő: Molnár József

Főszerkesztő-helyettes: Erdős Márton
Szerkesztő: Kudella Magdolna

Olvasószerkesztő: Cseh Vanda

Munkatársaink: Dávid Imre, Horváth Máté, Jancsó Orsolya, Lukács Richárd, Mészáros Csaba, Wiezner István

Tördelő grafikus: Berényi Teréz

Szerkesztőségi titkár: Cseresznye Anita
Telefon: 577-4301; telefax: 266-4343;
Internet: pcworld.hu;
e-mail: pcworld@pcworld.hu

KIADÓ

Kiadja a Project 029 Media & Communications Kft.
1036 Budapest, Lajos u. 78. IV. em.
Levélcím: 1374 Budapest 5, Pf. 578;
internet: project029.com
Bankszámlaszám:
10300002-20328016-70073285
Felelős kiadó:
Virágh Márton ügyvezető – mviragh@project029.hu
Operatív igazgató:
Babinecz Mónika – mbabinecz@project029.hu
Marketingmenedzser:
Kovács Judit – jkovacs@project029.hu

Ügyfélszolgálat
Telefon: 577-4301; telefax: 266-4343
e-mail: terjesztes@project029.hu

JOGI KÖZLEMÉNYEK

Molnár József
főszerkesztő

Kedves Olvasónk!

Közel kétezer év alatt megtanultuk, hogy miként kell megvédenünk értékeinket. Falakat és kerítéseket emeltünk, kialakítottuk a védelmi rendszereinket, lakat mögé zártuk a legfontosabb értékeinket. Pechünkre a jó és a gonosz örök harca a világhálóra is átterjedt, ahol a hozzánk hasonló látogatókra vadászva a web sötét bugyraiban vírusok és adathalászok várják, hogy megkaparintsák féltett információinkat, pénzünket. Véget ért a csíntevések korszaka, a modern fenyegetések nem akarják megforditani az asztalunkat, nem hívják fel magukra a figyelmet felugró ablakokkal, alattomosan várnak az első adandó alkalomra, amikor kirabolhatnak minket. Offline életünk után az online védelmi vonalainkat is fel kell építenünk, ám pechünkre ehhez nincs több ezer vagy száz évünk, azonnal reagálnunk kell minden változásra. Kiadványunkkal segítünk a „fegyverkezésben", hiszen a modern támadási technikák mellett a leghasznosabb biztonsági tippjeinket is összegyűjtöttük. Mottónk: paranoiások előnyben!

Vírus a termosztátban

A falnak is füle van – élünk gyakran a hasonlattal, ami gyakorlatilag bármikor valósággá válhat. Összegyűjtöttük a legfurább és egyben legveszedelmesebb sérülékenységeket.

Frissítsd a böngészőt! Ha kell, tiltsd le a Java beépülőt! Ne kattints gyanús linkekre, pláne ha egy vadidegen ösztönöz arra! Hosszasan sorolhatnánk még azokat a tanácsokat, amelyeket rendszeres olvasóink már mind ismernek, és remélhetőleg megfogadtak már korábban. A legalapvetőbb biztonsági óvintézkedéseket talán már az összes internetező kívülről fújja, alaposan megnehezítve ezzel a vírusterjesztők dolgát. Az ósdi kártevőtrükkök emiatt csak ritkán működnek, de ettől még nem érezhetjük privát életünket, adatainkat és pénzünket biztonságban.

Pechünkre a rosszfiúk kreatívak, és megtalálják a módját annak, hogy megkerüljék a jól felépített védelmeket. Új fegyverek kerültek a birtokukba, és már nem az Internet Explorert célozzák, hanem a virtuális gépeket, a PC-s játékokat és az internetre kötött hőfokszabályzót, hűtőszekrényt. „Minél több digitális eszköz épül be életünkbe, annál több lehetséges kiskapu nyílik meg, ahol a számítógépes bűnözők a nem tradicionális módszerekkel belopózhatnak életterünkbe, illetve bosszúból akár el is pusztíthatják eszközeinket" – nyilatkozta korábban *Toralv Dirro,* a McAfee Labs biztonsági elemzője.

Már nem az Internet Explorert célozzák, hanem a virtuális gépeket, a PC-s játékokat és az internetre kötött hőfokszabályzót

A káosz kamarája

2010 telén összehangolt támadást indítottak az Amerikai Kereskedelmi Iparkamara vezető alkalmazottai ellen. Elsősorban az ázsiai kapcsolatokért felelős beosztottakra vadásztak, és a vizsgálatok szerint pontosan tudták, hogy kik a célpontok, és hogy milyen eszközöket kell bevetni. A szofisztikált támadás több szinten zajlott, amit jól jellemez, hogy az incidens felfedezése után a szakemberek indokoltnak látták néhány gépet fizikailag elpusztítani. Nem jártak sikerrel, a kamara székházánál fura jelenségek figyelmeztettek arra, hogy a támadók még házon belül vannak: a hőfokszabályzó adatcsomagokat küldött Kínába, míg a helyi nyomtató öntudatra ébredt, és néha kínai karaktereket tartalmazó oldalakat nyomtatott ki. Mintha szellemek jártak volna az épületben.

A nyomtatók például remek célpontot jelenthetnek, hiszen a lézeresek hőt termelnek munkájuk során, így túlterhelésükkel felgyújtható az eszköz, illetve akár egy egész lakás vagy iroda. Rémisztően hangzik? Ez a valóság, biztonsági kutatók ugyanis már bebizonyították, hogy a támadás kivitelezhető, csak szerencsénkre az online bűnözők még nem éltek e sérülékenységekkel. Előbb-utóbb azonban fognak, mivel a hálózatba kötött eszközök gyakran folyamatosan elérhetők az interneten keresztül, ráadásul a könnyű elérés miatt még a céges tűzfal sem védi őket. Gyakorlatilag csak arra várnak, hogy érkezzen egy hacker, és kiolvassa a printer gyorsítótárából a korábban kinyomtatott oldalakat. Ez bármikor megtörténhet.

Andrew Howard, brit kutató szerint célpontot sem nehéz találni, hiszen egy speciálisan megszerkesztett Google-kereséssel több mint 86 ezer publikus Hewlett-Packard printernek akadhatunk a nyomára. A gond az, hogy sok rendelkezik közülük ismert sérülékenységgel, ami potenciális veszélyforrást jelent, ha az eszközhöz nem érkezik biztonsági javítás, illetve amennyiben elmarad a szükséges firmwarefrissítés.

A cégeken túl az otthoni felhasználók, többek között a játékosok is veszélyben vannak. Most a kalózszoftverek biztonsági kockázatairól nem értekeznénk, a hamis programok veszélyeivel bizonyára mindenki tisztában van. Ugyanakkor a legális szoftverek gazdái sem érezhetik magukat biztonságban, a rosszul megírt digitális jogvédelmi (DRM) rendszerek a jóhiszemű felhasználókat is veszélybe sodorhatják. Néhány éve a Ubisoft Uplay szolgáltatása került kereszttűzbe, a megoldás ugyanis csendben egy trehányul megírt böngészőbeépülőt is feltelepített. A Google biztonsági kutatója felfedezte, hogy így valójában kiskaput nyitottak a felhasználók gépein, hiszen az add-onon keresztül a támadók könnyedén átvehették az irányítást a PC-k felett. Egy demonstrációs oldal például a Számológépet nyitotta meg. Szerencsére nagyobb károkozásról nem tudni, a Ubisoft pedig sűrű elnézéskérés közepette hamar befoltozta a rést.

Ám nemcsak a francia cég sérülékenysége az egyetlen unortodox támadás, ami a játékosokat fenyegeti. Két évvel ezelőtt a ReVurn a steam:// protokollal kapcsolatban adott ki riasztást, ami lehetőséget adott kártékony kód futtatására a felhasználók gépein. A rés minden olyan gépen fennállt, amelyre a Valve programját telepítették, a kliens ugyanis installálását követően a alapértelmezett kezelőjévé nyilvánította magát, ami nem lett felkészítve a kártékony JavaScript-kódok kivédésére. A hiba leginkább a Firefox és a Safari böngészők tulajdonosait érintette, az Internet Explorer, a Chrome és az Opera nem csupán egy figyelmeztető üzenetben jelezte a potenciális veszélyt, de a teljes webcímet is megjelenítette, így a csalás könnyen kiszűrhető volt (legalábbis azoknak, akik tudatosan internetezneznek). A Mozilla alkalmazása szintén megerősítést kért, de nem írta ki a teljes URL-t, így a figyelmetlen játékosokat egyszerűen lépre lehetett csalni. A Safarinál mindez hatványozottan volt igaz, hiszen az Apple böngészője még figyelmeztetést sem küldött, automatikusan végrehajtotta az utasítást. A fenyegetés ismét egy olyan helyről érkezett, ahonnan nem feltételeztük volna.

Mi a helyzet a virtuális gépekkel? Alapesetben biztonságosak, hiszen egy elszeparált memóriaterületen futnak, így a gazda operációs rendszerrel csupán annyi a kapcsolatuk, hogy az futtatja keretrendszerüket. Nos, a hackerek immár ezt az állítást is megcáfolták. Tavaly augusztusban ugyanis a VMware figyelmeztetést adott ki, miután a Symantec mérnökei egy merőben új támadási formát fedeztek fel. A Crisis vírus direkt a VMware Workstation és Player szoftvereket célozza meg, a felhasználó gépére kerülve – egy kártékony JAR állomány formájában – átvizsgálja a merevlemezeket, és

A tévé téged néz

Remek dolog, hogy immár a nappalikat is elérte az okosforradalom, ugyanakkor jelentős biztonsági kockázatot is hordoz magában. A tévék folyamatosan a világhálón lógnak, személyes információkat tartalmaznak, beépített webkamerájuk videót tud rögzíteni a környezetéről, sőt gyakran még USB-háttértárat is csatlakoztatnak hozzájuk. Ideális célpontok! A máltai ReVuln ráadásul korábban megtalálta az első nulladik napi sérülékenységet a Samsung rendszerében, ami távoli kódfuttatást tett lehetővé. Egyelőre nem tudni olyan esetről, hogy kihasználták volna a tévék biztonsági réseit, de az biztos, hogy minél okosabbak lesznek a tévék, annál inkább megnő egy tömeges támadás lehetősége, főként ha mind több személyes adatot tárolnak. Ha ez megtörténik, akkor nézhetünk majd csak igazán!

Mivel egyre több eszköz rendelkezik beépített mikrofonnal, az ipari kémkedés mindennapossá válhat

Vírus emberbőrben

Dr. Mark Gasson, a Reading Egyetem kutatója érdekes kísérletbe fogott: egy vírusos RFID chipet ültetett be a bőre alá. Amikor a kezét egy leolvasó közelébe tette, a labor – mármint a saját egyeteméé – számítógépe beolvasta azt, és azonnal megfertőződött az adatbázisa, ráadásul később a kártevő a többi kolléga RFID-beléptetőkártyájára is átterjedt. Az eredmény meggyőző volt: a bőr alá épített implantátumok vezeték nélkül is komoly károkat tudnak okozni. *Gasson* ugyanakkor figyelmeztetni akarta a társadalmat, hogy a mechanikus szívekkel és stimulátorokkal élők védelmére fokozottan oda kell figyelni. „Képzeljük el, hogy valaki egy szolgáltatásmegtagadás-alapú támadást indít egy pészmeker ellen. Nagyon veszélyes lenne, ha lehetségessé válna" – nyilatkozta a kutató.

Simon mondja

George Ou, a ZDNet szakértője 2007-ben egy veszedelmes Vista-sérülékenységre figyelmeztetett. A hiba a Windows hangfelismerő moduljában található, ami a speciálisan szerkesztett hangutasításokat bármiféle óvintézkedés nélkül végrehajtja. Így elméletben egy speciális weboldallal átvehető az irányítás a felhasználók gépei felett. A recept adott, de a hackerek szerencsére mégsem használták ki, főként nehéz kivitelezhetősége miatt. Egyrészt az internetezőt el kell csalni a kártékony weboldalra, másrészt a hangszórónak bekapcsolva kell lennie, különben a hang nem kerül ki az éterbe. Ezen felül a hangfelismerő modulnak is futnia kell, ami a legtöbb esetben ki van kapcsolva, illetve a támadás feltétele, hogy a felhasználó tétlenül figyeljen. Ettől függetlenül nem szabad elbagatellizálni a problémát.

ha egy rendszerképet talál, akkor beágyazza magát a virtuális rendszerbe. A technológia tehát mégsem olyan biztonságos, mint gondoltuk: a virtuális gép pont annyira védi adatainkat, mint a gazdája. A VMware a rendszerképek titkosítását javasolta a támadás kivédésére, valamint hogy ne töltsünk le bizonytalan forrásból fájlokat, és figyeljünk a vírusvédelem naprakészségére. Ezek mind olyan tanácsok, amelyek a védelem alapelemeit adják.

Jobb, ha odafigyelünk az androidos készülékekre is. A Kaspersky mérnökei két kártékony, ugyanakkor érdekes alkalmazást fedeztek fel a Google Play kínálatában. A DroidCleaner és a SuperClean rendszertakarítónak adja ki magát, ám amint egy PC-hez csatlakoztatják gazdagépüket – például zenék és képek felmásolásához –, azonnal akcióba lépnek. Ha a Windowsban az automatikus futtatás engedélyezve van, egy szempillantás alatt megfertőzik a Microsoft operációs rendszerét, hogy kémkedhessenek. Nem számlainformációkra vadásznak, hanem az élő szóban elmondott információkra, hiszen a gépek mikrofonját használva figyelnek, és amint hangot érzékelnek, rögzítik azt, és elküldik a készítőknek. Az ipari kémkedés új

szintje ez, ahol az internetre kötött videokonferencia-rendszereket is előszeretettel támadják. 2010-ben például biztonsági kutatók a Cisco megoldásának sérülékenységeit kihasználva könnyedén át tudták venni az irányítást a hardverek felett. A cég szerencsére gyorsan reagált. 2012-ben pedig kiderült, hogy a világhálón keresztül több mint 150 ezer olyan videokonferencia-eszköz található meg, ami a bejövő hívásokra automatikusan reagál. A tűzfalak óta tudjuk, hogy ez egy előnytelen tulajdonság, és a rosszfiúknak lehetőséget ad arra, hogy saját házunkban és irodánkban hallgassanak le minket plusz készülék telepítése nélkül. Mivel egyre több kütyü – okostévé, okostelefon, noteszgép és táblagép – rendelkezik beépített mikrofonnal, elképzelhető, hogy az ipari kémkedés mindennapossá válik majd, és árulóink saját eszközeink lesznek.

Mi a megoldás? Egyelőre a fent részletezett sérülékenységeket széles körben még nem támadták, így nem kell tartanunk attól, hogy holnap-holnapután a tévénken keresztül lehallgatnak majd minket, illetve egy vadidegen csupán egy érintéssel tönkreteszi gépünket. Ettől függetlenül mindenképpen figyeljünk oda beállításainkra, a szoftverek naprakészségére és a biztonsági figyelmeztetésekre.

Molnár József

A MAGYAR INTERNETEZŐK TORRENTFELHASZNÁLÁSI SZOKÁSAI

A G Data reprezentatív felmérése ezerfős válaszadói panellel
Minta: 18–75 éves internetezők

Forrás: NRC Omnibusz – 2012. augusztus

Veszélyes warezvilág

Utánajártunk, milyen veszélyekkel jár a tört szoftverek használata – akár személyes biztonságunkat tekintve, akár bűntetőjogi szempontból.

Szinte a magyar virtus része ma a warezolás és torrentezés, amolyan: „tudom, hogy nem kéne, de…" Sem az egyre gyakoribb jogi lépések, sem a kártevők nem szegik a felhasználók kedvét. Hogy vajon miért? Sokak szerint az anyagi okokban rejlik a válasz; külföldön inkább megengedhetik maguknak a felhasználók a jogtiszta programok használatát. Ráadásul Magyarországon a szabályok kijátszása bizonyos körökben szinte sikk, így az unatkozó crackerek könnyen önjelölt netes Robin Hoodként lófrálhatnak a cybervilágban. Ugyanakkor a programozók nem mind jóindulatúak. Sőt.

„Közhiedelem, hogy a világon több ezer tehetséges programozó tölti azzal az idejét, hogy kereskedelmi szoftvereket feltörjön, majd ezeket teljesen ingyenesen, kvázi szeretetből mindenki rendelkezésére bocsássa" – mondta *Petrányi-Széll András*, a G Data magyarországi kommunikációs vezetője a *PC World* kérdésére, hozzátéve, hogy a valóság a vázolt hiedelemnél valamivel összetettebb. Valóban léteznek jóindulatú crackercsoportok, a torrentek jelentős része azonban bújtatott átverés. A feltört programokat a bűnözők vírusokkal csomagolják össze, és torrentoldalakon terjesztik. Az óvatlan letöltőket pedig megfertőzhetik, és egy botnet részévé tehetik számítógépeiket.

„Meglehetősen nagy a fertőzés veszélye" – nyilatkozta kérdésünkre *Béres Péter*, az ESET hazai forgalmazásáért felelős Sicontact vezető IT-tanácsadója. „Bármilyen típusú kártevőt bele lehet fordítani a letöltött és a telepített állományba, így rootkitet vagy backdoort is elhelyezhetnek az áldozat gépein, és erről a felhasználó még csak tudomást sem szerez." Arról nem beszélve, hogy nem biztos, hogy teljes funkcionalitást ad a feltört termék, és a rossz működés programütközésekhez, legrosszabb esetben akár gépössze-

omláshoz is vezethet. Ha megtörtént a baj, akkor az áldozatok magukra maradnak, miközben a jogtiszta szoftverekhez mindig jár támogatás, akár e-mail, akár chat, telefonos segítség vagy legrosszabb esetben távoli bejelentkezés formájában.

Torrent, veszély a neved

Ben Edelman, a Harvard Business School professzora nemrégiben kijelentette, hogy az összes, számítógépre veszélyes oldal közül a torrentoldalak viszik a pálmát. Itt bármilyen kártevőt összeszedhet az ember, mivel ezeknek az oldalaknak nincs „sem üzleti modellje, sem olyan megvédendő hírneve, mint például a felnőtt tartalmakat kínáló oldalaknak". Ráadásul évek óta folyamatosak az olyan kifinomult csalások, amelyek esetében szándékosan hamis és/vagy fertőzött csomagokat publikálnak a torrentoldalakra. Ennek köszönhetően jobb esetben csak kínos fényképek kerülhetnek fel rólunk a netre – *Anna Kournikova* ezt már megtapasztalta –, rosszabb esetben a következő kártyás vásárlás során megadott adatainkkal leszívhatják a számlánk teljes összegét.

Néha pedig még ennél is rosszabbul járhatunk. „Emlékezzünk vissza az Egyesült Államokban meghurcolt tanár esetére, akit gyermekpornográfia terjesztése miatt börtönnel fenyegettek, amíg egy antivírus-szakértő ki nem derítette, hogy számítógépe egy fertőzés következtében vált egy ilyen anyagokat terjesztő botnet részévé" – mondta *Petrányi-Széll András*. *Béres Péter* pedig hozzátette: „előfordul, hogy nem is létező szoftverek helyett kerülnek fel trójai programok." Ilyen volt például néhány éve a Foxit for Macintosh esete, amikor a csak látszólag létező alkalmazás letöltésekor valójában egy Mac malware települt. „De az is megesik, hogy valamilyen nagyon várt új szoftver helyett a megjelenés előtt hamisítanak egy fertőzött csomagot" – tette hozzá a Sicontact szakembere. Nemrégiben például a BlackBerry nem győzte értesíteni a felhasználóit, hogy a Google Playen található BlackBerry Messenger for Android valójában hamisítvány.

> Évek óta folyamatosak az olyan kifinomult csalások, amelyek esetében szándékosan hamis és fertőzött csomagokat publikálnak a torrentoldalakra

Az egyik legnagyobb gondot az jelenti, hogy a torrentbe ágyazott fertőző és folyamatosan adatokat továbbító féreg működése során megbéníthatja a gépen található védelmet, ami megnyithatja az utat a többi kártevő számára. Nem véletlen tehát, hogy a víruskeresők gyakran riasztanak torrentfájloknál – a legrosszabb, amit ilyenkor tehetünk, hogy egy játék, film, pár ezer forint megspórolása érdekében szabad utat engedünk a férgeknek, aminek ára később sokkal súlyosabb lehet.

Megoldások és biztonsági lépések

- Használjunk jogtiszta szoftvereket. Általában minden programnak van 30 vagy 60 napos kipróbálási ideje.
- Telepítsünk eszközünkre jogtiszta, egy megbízható gyártótól származó, folyamatosan frissített vírusirtó szoftvert.
- Ne feledkezzünk meg a különböző kiegészítő szoftverek frissítéseiről és az operációs rendszer folyamatos foltozásáról sem. Gyakran indítsuk újra a noteszgépeket.
- Vállalati szinten mindenképpen használjunk olyan végpontvédelmi megoldásokat, melyek képesek kilistázni a kliensekre telepített szoftvereket, és blokkolni tudják a nem kívánt alkalmazásokat.

Jogi háttér

Sajnos világjelenség, hogy a kereskedelmi programok feltörése kulturálisan teljesen elfogadott, legyen mégoly illegális is. Sőt, a hírhedt Pirate Bay eset nyomán még politikai tőke is született az esetleges legalizálás kérdéséből. Azóta azonban egyre több országban indult szervezett támadás a fájlcserélők ellen, így ma már nemcsak Skandináviában, de az Egyesült Államokban, Franciaországban és legutóbb Lengyelországban is elítéltek illegális letöltőket. A magyar törvények szerint is a jogi felelősségre vonást kockáztatják azok, akik warezszoftvereket használnak. *Dr. Kovács V. Gábor* infokommunikációs szakjogász és ügyvéd a *PC World*nek elmondta, hogy „szoftverek esetén a magáncélú másolás mint a szabad felhasználás esete, fel sem merülhet a magyar jog alapján, mivel a szoftverek licencszerződés nélküli másolása, a torrenten keresztüli feltöltés lehetőségének megteremtése, futtatása egyértelműen sérti a szerzői jogot".

Az audiovizuális művek esetében némileg árnyaltabb a helyzet. A letöltő gyakran védekezhet a szerzői jogi szabad felhasználás esetével, vagyis hogy csak magáncélú másolás történt. *Dr. Kovács V. Gábor* azonban hozzátette, hogy kérdés, tényleg szabad felhasználásnak minősül-e a nyilvánvalóan jogellenes forrásból származó letöltés. Mindenesetre a warezkészítőktől „a szerzői jogi jogosult a polgári jog szerint elsősorban kártérítést követelhet" – magyarázta a szakértő. „Emellett számolni kell a büntetőjogi következményekkel is. Ma a bíróság által kiszabható büntetés alapvetően két évig terjedő szabadságvesztés, de jelentős vagyoni hátrány okozása esetén akár tíz év is lehet."

A torrentletöltőknek azonos polgári jogi következményekkel kell szembenézniük jogosulatlan tartalmak használata esetén. „A büntetőjogi következmények annyi enyhítést tartalmaznak, hogy le- és feltöltés esetén csak akkor büntethető a cselekmény, ha az a jövedelemszerzés célját legalább közvetve szolgálja. Ennek megvalósulását mindig a konkrét ügyben eljáró bíróság ítéli meg" – tette hozzá a szakjogász. *Petrányi-Széll András* a vállalatoknál felmerülő komoly jogi veszélyeket emelte ki. „Az a cég, amelyik nem használ olyan végpontvédelmi rendszert, mely képes blokkolni a nem kívánt alkalmazásokat, felelősségre vonható, ha valamelyik alkalmazottja torrentfájlokat tölt le. Ezt a végpontvédelmet az sem váltja ki, ha az alkalmazásokat hálózati szinten, egy UTM-eszközzel blokkoljuk."

Vannak tehát trükkök és lehetőségek a warez felhasználására. A kérdés az, hogy vajon megéri-e? Minden egyes kalózprogram a támogatástól fosztja meg a fejlesztőt. Pedig nagy szüksége lenne minden fillérre, hiszen hosszú távon ebből javítja és fejleszti az általunk is kedvelt programot. Se pénz, se posztó, előbb-utóbb pedig program se.

Jancsó Orsolya

VELED IS MEGTÖRTÉNHET

SNAPCHAT TRÜKK

Első történetünkben azt mutatjuk meg, hogy milyen egyszerűen rá lehet venni a felhasználókat egy – akár kártékony kódot tartalmazó – alkalmazás telepítésére. A kerítő ezúttal a fiatalok körében népszerű képalapú közösségi oldal, a Snapchat volt, amely engedélyezi, hogy a felhasználóknak idegenek is küldhessenek üzeneteket, vagyis a támadók szempontjából szabad a spammelés. Az áldozatokat, jellemzően férfiakat, hamis bikinis női profilokkal keresték meg azzal, hogy megtetszett a profilképük, és szeretnének velük jobban megismerkedni. Ezt követően egy legális csevegőszolgáltatásra terelték a beszélgetést, ahol a diskurzus előre megírt feltételek – azaz ha ezt mondja, akkor én ezt válaszolom – alapján zajlott. Az aktus lényege az volt, hogy további képeket ígértek, de előtte megkérdezték, hogy az xy játékot kipróbálták-e már. Ha nem – és jó eséllyel nem –, akkor megkérték az áldozatokat a telepítésre, a hormonok által befolyásolt férfiak pedig ezt az első kérésre megtették.

Védtelenül hagyott eszközök

Megoldatlan a világhálóra csatlakozó új típusú eszközök frissítése. Cikkünkben megmutatjuk, hogyan csökkentheted minimálisra a kockázatokat.

Egyre többféle eszköz kapcsolódik az internetre, ez ma már nem csupán a számítógépek és okostelefonok kiváltsága. Ott toporognak a világhálón a legkülönfélébb „okos" eszközök – televíziók, órák, autók – mellett a „dolgok internete" (internet of thing, IoT) kategóriába sorolható háztartási gépek, testen hordott eszközök, csecsemőfigyelők, kamerák, hálózati tárolók és sok minden más.

A trend megállíthatatlan, és ezzel párhuzamosan egyre több szó esik az internetre kapcsolódó eszközök biztonságáról, ami bizony komoly kívánnivalókat hagy maga után. Márpedig a probléma hatalmassá nőheti ki magát, ha az érintettek nem teszik meg a szükséges óvintézkedéseket. A hackerek egyelőre várakozó álláspontonvannak; ők akkor lendülnek akcióba, ha a sebezhető platform használóinak száma elér egy kritikus tömeget ahhoz, hogy a támadásokkal megfelelő hasznot lehessen elérni. Nyilvánvaló, hogy az IoT-eszközök feltörésével értékes információkat lehet majd összegereblyézni, például egy okostévé esetében hozzá lehet jutni a berendezés által összegyűjtött használati adatokhoz (milyen műsort néztünk, milyen appokat futtattunk, milyen weboldalakat látogattunk meg stb.). Ha pedig a televíziót felszerelték kamerával és mikrofonnal, a hackerek mindent látni és hallani fognak, ami a szobában történik.

Buzgó adatgyűjtés: nemrég botrány tört ki egyes okostévék gyári beállítású kémkedése miatt

Aztán itt vannak a testen hordható diagnosztikai eszközök, amelyek révén az orvosok távolról is tájékozódhatnak egy beteg állapotáról. Ezek vagy az adatátvitelre használt kommunikációs csatorna feltörésével rendkívül bizalmas és értékes egészségügyi adatokhoz juthatnak a kiberbűnözők. Egyre több automatizált szolgáltatást építenek be a gyártók az autókba, amelyek segítenek elkerülni a dugókat, és jelentősen megkönnyítik a járművezetők életét. Azonban még elgondolni is rossz, hogy mi történhet akkor, ha a számítógépekkel vezérelt, egymással vezeték nélkül kommunikáló járműveket meghackelik, és így veszélybe kerül az utasok élete.

Szó sincs riogatásról, valósak a veszélyek

Nem a levegőbe beszélünk, amikor az internetre kapcsolódó eszközök biztonsági hiányosságaira hívjuk fel a figyelmet, következzen hát pár konkrét példa leírása, amikor biztonsági szakértők tüzetesen utánanéztek annak, milyen kellemetlenségekre számíthatunk a különféle okoseszközök használatakor. Szerencsére ezek egyelőre mindössze potenciális veszélyek, nem érkeztek még olyan hírek, hogy kiberbűnözők ténylegesen kihasználták a kutatók által feltárt alábbi sebezhetőségeket.

David Jacoby, a Kaspersky Lab munkatársa a budapesti Hacktivity konferencián tartott előadásában számolt be saját lakásának „meghackeléséről". Annak járt utána, hogy az otthonában található intelligens eszközök – két, különböző gyártótól származó hálózati (NAS) tároló, okostévé, műholdvevő és nyomtató – használata milyen kockázatokkal jár. Az eredmény sokkoló volt: a hálózati tárolóknál 14, az okostévénél egy sérülékenységet fedezett fel, míg a routerben több rejtett, távoli vezérlést lehetővé tevő funkciót talált. A vizsgált berendezések alapjelszava szintén gyenge volt, sok konfigurációs fájl nem megfelelő jogosultságokkal rendelkezett, és a jelszavakat egyszerű szövegben, mindenféle titkosítás nélkül tárolta. Ezen sérülékenységek révén többek között megfertőzhető az okoseszközhöz csatlakoztatott PC, man-in-the-middle típusú támadással pénz lopható az okostévé tulajdonosától, ha az a berendezésen keresztül vásárol online tartalmakat, valamint hozzáférés szerezhető az otthoni Wi-Fi-hálózatot használó többi eszközhöz.

Egy másik Kaspersky Lab kutatás a népszerű Google Glass okosszemüveg és a Samsung Galaxy Gear okosóra sebezhetőségeire hívja fel a figyelmet. Az előbbi esetében a kutatók felfedezték, hogy az eszköz és egy Wi-Fi hotspot közötti kommunikáció nem volt teljes egészében titkosítva, így ki lehetett deríteni, hogy a szemüveg használója milyen tartalmakra keresett rá az interneten. Utóbbinál pedig azt állapították meg, hogy amikor egy appot telepítenek az okosórára, az nem küld értesítést a műveletről, ami lehetővé teszi, hogy hackerek célzott támadással észrevétlenül telepítsenek rosszindulatú szoftvert az eszközre.

Nem biztonságosak az internetre kapcsolódó okosautók sem: egy, az IAB Spanyolország marketing- és digitálismédia-szervezet által – több más céggel közösen – készített tanulmány szerint a járművekhez készült okostelefonos appok ellopott bejelentkezési adatainak segítségével megállapítható a gépkocsi tartózkodási helye, és az ajtók távoli hozzáféréssel kinyithatók. A kutatás során vizsgált autómárkánál további problémát okozhat a Bluetooth-vezérlő frissítése, mert az ezt tartalmazó, internetről letöltendő fájl nem titkosított, ellenben számos információt tartalmaz az autóban futó belső informatikai rendszerekről, és módosításával lehetővé válik egy rosszindulatú program futtatása. Aggályosnak találták a kutatók ugyanennél a márkánál, hogy egyes szoftverfunkciók SMS-ek révén kommunikálnak a járműben lévő SIM-kártyával, ugyanis a kommunikáció feltörésével hamisított üzenetek küldhetők, és a hackerek saját rosszindulatú utasításaikra cserélhetik fel az eredetieket.

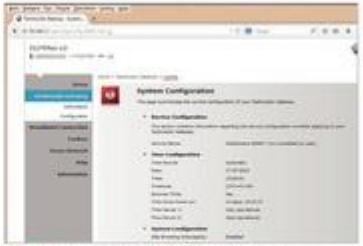
> Az IoT-eszközökkel kapcsolatban a legaggasztóbb tényező, hogy frissítésükre nem dolgoztak ki általánosan alkalmazható, hatékony módszert

Vég nélkül folytathatnánk hasonló történetekkel más eszközökről, a biztonsági konferenciák kedvelt témája mostanság az IoT biztonsági hiányosságainak bemutatása.

Komoly gondok a frissítéssel

Az IoT-eszközökkel kapcsolatban a legaggasztóbb tényező, hogy frissítésükre nem dolgoztak ki általánosan alkalmazható, hatékony módszert. Márpedig nem létezik olyan programkód, amelyben ne lenne hiba. Ha napvilágra kerül egy sérülékenység, és annak kijavítása nem történik meg, az adott eszköz folyamatosan veszélynek lesz kitéve. De hogyan értesítsék a gyártók a frissítés kiadásáról az érintett intelligens háztartási gépek, autók vagy viselhető eszközök tulajdonosait, illetve hogyan juttassák el hozzájuk a szoftvert belátható időn belül? Ezekre a kérdésekre egyelőre nem született válasz. Ráadásul sok berendezés és kütyü nem rendelkezik olyan közvetlen felhasználói felülettel, amelyen keresztül a frissítés egyszerűen elvégezhető lenne. Így – ha egyáltalán kiadnak hozzájuk szoftverfoltot – az ilyen eszközök nagy valószínűséggel használati idejük során sohasem lesznek javítva, és mindvégig sebezhetők maradnak.

Persze gyakran sem a gyártókat, sem a vásárlókat nem izgatja különösebben, hogy a berendezésük mindig naprakész állapotban legyen. Előbbiek minél több készülék eladásában érdekeltek, és az internetre csatlakoztathatóságot csupán a funkciók egyikének tekintik, ami nem a specialitásuk, míg a felhasználók többnyire azt szeretnék, hogy a megvásárolt berendezés rendeltetésszerűen működjön, és nem kívánnak vacakolni olyan kellemetlenségekkel, mint annak javítgatása, frissítése. Mi több, az esetek nagy részében egyáltalán nem szereznek tudomást arról, hogy valamelyik eszközüket feltörték, ugyanis a kiberbűnözők igyekeznek a háttérben futtatni a rosszindulatú műveleteket, az eszköz teljesítményének észrevehető lassítása nélkül. A hackelések nagy részéről tehát nem is tudunk.



Meglepő routerfunkciók: távoli vezérlési lehetőségek, amiket kihasználhatnak a hackerek is (Forrás: David Jacoby)

Így védekezhetünk

Ha meg akarjuk óvni internetre kapcsolódó eszközeinket, valamint a rajtuk tárolt, illetve általuk összegyűjtött adatokat, nem ülhetünk ölbe tett kézzel addig, amíg a gyártók megtalálják a hibajavítás hatékony módszerét. Mindenekelőtt menjünk elébe a dolgoknak, nézzünk utána, hogy eszközeink firmware-ének létezik-e a jelenleg használtnál frissebb változata. Ha igen, telepítsük ezeket az összes rendelkezésre álló biztonsági frissítéssel együtt. Második lépésként változtassuk meg az eszközök gyári felhasználónevét és jelszavát, ugyanis ezekkel próbálkoznak először a hackerek, amikor megpróbálják feltörni eszközeinket.

Kiemelt szerep jut a védekezésben a hálózati routernek. Ezek többsége lehetővé teszi, hogy elkülönített hálózati csoportokat hozzunk létre a különféle eszközök számára, így például kialakíthatunk egy szegmenst a PC-nknek, nyomtatónknak, hálózati tárolónknak és a többi, „hagyományos" informatikai berendezésünknek, egy másikat mobileszközeinknek (tabletünknek, okostelefonunknak), egy harmadikat pedig a játékkonzolunknak, okostévénknek és más problémás készülékünknek. Ezáltal ha feltörik okostévénket, a támadó csak annak hálózati szegmensébe jut be, ahonnan nem fér hozzá PC-nkhez vagy hálózati tárolónkhoz.

Mészáros Csaba

Támadás minden fronton

Immár valamennyi eszközünket célba veszik a személyes adatainkra áhítozó hackerek, így nem tehetünk mást, meg kell védenünk az összeset.

Egyre több bizalmas információt tárolunk mobileszközeinken az okostelefonok és tabletek elterjedésével, amelyekről ráadásul immár gyakrabban jelentkezünk be különféle online fiókjainkba, mint PC-nkkel vagy noteszgépünkkel. Míg azonban a hagyományos számítógépeken szinte mindenki futtat valamilyen vírusellenes szoftvert, addig a mobileszközökön alig használunk ilyet. Jól tudják ezt a hackerek is, és a legkülönfélébb módon támadják informatikai infrastruktúránk eme gyenge láncszemeit. Legfejlettebb módszereik közé tartoznak a viszonylag új irányzatnak tekinthető, úgynevezett többplatformos (más néven keresztplatformos) fenyegetések, amelyek esetében célba veszik az általunk használt összes eszközt, így próbálva megszerezni olyan bizalmas adatokat, amelyeket aztán pénzszerzésre használhatnak fel.

Trükkös ablak a böngészőben: mobilunk típusára és telefonszámunkra kíváncsiak

Ezen fenyegetések többfélék lehetnek: támadhatnak ugyanolyan módon a különböző rendszereken; minden egyes megcélzott platformhoz speciális modult használhatnak; lehet olyan komponensük, amely lehetővé teszi futásukat különböző szoftveres környezetekben, vagy az egyik platformon végrehajtott támadást kiterjeszthetik egy másikra.

Egy kis történelem

Többplatformos vírusok már a mobil- és tabletcunami kitörése előtt is léteztek (lásd a mellékelt táblázatot). Ha egy sérülékenység kihasználásához szükséges kódot több operációs rendszerhez is megírják a hackerek, azzal olyan fenyegetéshez jutnak, amellyel a windowsos, maces és linuxos gépeket egyaránt veszélyeztethetik. Ez különösen hatékonyá teszi egy vírus terjesztését, hiszen nem csupán többféle eszköz fertőzhető meg vele, hanem egyszerűen át lehet vinni a fertőzést az egyik platformról a másikra, ami közönséges programkártevők esetében nem megvalósítható. Kifejezetten jól támadhatók ilyen módon a több rendszerrel kompatibilis szoftverek (például a Java) sérülékenységei.

Az egyik legismertebb többplatformos féreg, a Windowst és Macet fertőző Koobface 2009-ben tűnt fel, különféle változataival egy év leforgása alatt több mint kétmillió dollárt söpörtek be készítői. Eredetileg közösségi (Facebook, Skype, Yahoo Messenger) és e-mail szolgáltatások (Gmail, Yahoo Mail, AOL Mail) használóit támadta, majd amikor ezek javítottak védelmükön, fejlesztői átalakították többplatformossá, hogy teljes hálózatokat tudjanak megfertőzni vele. Bejelentkezési információkat gyűjt, a megfertőzött gépeket peer-to-peer bothálózatba köti. Ezt rosszindulatú programok pénzért történő terjesztésére használja, továbbá a keresések eltérítésével hirdetéseket jelenít meg a feltört számítógépeken. A 134 országban több mint 62 ezer gépet megfertőző Koobface által letöltött komponen-

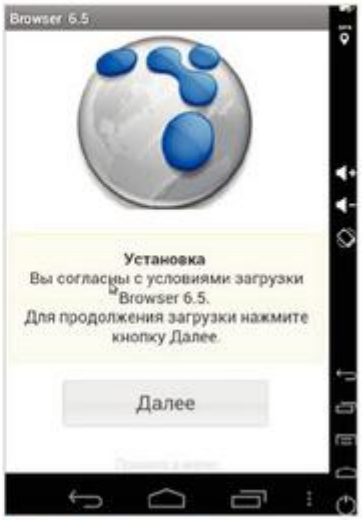
Többplatformos vírusok

Elnevezés	Támadott platform	Felfedezés ideje
Koobface	Windows, Mac OS X	2008. december
Jnanabot/Boonana.a	Windows, Mac OS X, Linux	2011. január
Backdoor:OSX/GetShell.A.	Windows, Mac OS X, UNIX	2011. július
Crisis	Windows, Mac OS X	2012. augusztus
McRAT	Java	2013. március
Janicab.A	Windows, Mac OS X	2013. július
JV/BackDoor-Fazy	Java	2013. augusztus
TROJ_Droidpak.A	Windowsról Androidra	2014. január
USBattack.A	Androidról Windowsra	2013. január

sek között megtalálható egy DNS-szűrő, amely blokkolja a hozzáférést egyes biztonsági webhelyekhez.

Bankszámlánk veszélyben

Beveti a többplatformos trükköt a kétfaktoros azonosítás – az SMS-ben küldött egyszeri jóváhagyókód – kijátszására a bankszámlák megcsapolására szakosodott hírhedt Zeus is. Amikor a programkártevővel megfertőzött számítógép tulajdonosa bankja weboldalára navigál, a Zeus észleli, hogy az áldozat egy, a listáján található címet látogat meg. HTML-beillesztéssel módosítja a weboldalt a böngészőben, így az online banki szolgáltatásba történő bejelentkezéshez begépelt felhasználónév és jelszó nem a bankhoz kerül, hanem a Zeus vezérlőközpontjába. Mivel a pénzintézetek a csalások megakadályozására bevezették a mobiltelefonra küldött jóváhagyókód használatát, valamikor 2010 szeptembere táján a hackerek új funkcióval egészítették ki a vírust. A hamis banki oldal új változata a bejelentkezési információk mellett adatokat – típus, gyártó, telefonszám – kért a felhasználó mobiltelefonjáról is, azt állítván, hogy azokra a „biztonsági tanúsítvány" frissítéséhez van szüksége. A gyanútlan nyilatkozók később szöveges üzenetet kaptak, amelyben arra kérték őket, hogy telepítsék az új biztonsági tanúsítványt, amely valójában a Zeus



Malware rendszer szerint: böngésző képében további kártevőket telepít az androidos komponens

mobilváltozata, a ZitMo (ZeuS-in-the-Mobile) volt. A hackerek újabb és újabb trükkökkel veszik rá a banki ügyfeleket ennek telepítésére, így például mostanában már közvetlenül a feltört banki oldalon kéri meg áldozatát a Zeus, hogy az SMS „biztosítására" töltsön le egy androidos biztonsági appot. Ehhez átirányítják egy másik weboldalra, ahonnan egy QR-kód beszkennelésével vagy a megadott hivatkozásról töltheti le okostelefonjára a legális appnak hitt ZitMo-t. Amely aztán banki bejelentkezéskor továbbítja a hackereknek a bank által üzenetben küldött kódot, így átvehetik az ellenőrzést az áldozat bakszámlája felett.

Androidról Windowsra és vissza

A legújabb keresztplatformos fenyegetések azt használják ki, hogy időről időre összekapcsoljuk PC-nket és mobileszközeinket adataink szinkronizálására, illetve fájlok – videók, fényképek és más tartalmak – átmásolására. Ez kiváló alkalmat kínál a hackereknek arra, hogy az egyik megfertőzött eszközről megfertőzzék a másikat, aminek révén az áldozat összes személyes információjához hozzá tudnak férni.

Mivel a mobil operációs rendszerek között egyre nagyobb dominanciára tesz szert az Android, nem csoda, hogy a hackerek ehhez írják a legtöbb rosszindulatú programot. A keresztplatformos kategória egyik hírhedt szereplője az Androidos_USBattack.A azonosító alatt nyilvántartásba vett információlopó programkártevő,

Adatgyűjtés hacker módra: hamis űrlap bankkártyaszám ellopására

amely DroidCleaner nevű tártisztító segédprogramnak álcázza magát. Több törlési funkciót is kínál, bármelyiket is válasszuk azonban, nem csinál ezzel kapcsolatban semmit azon kívül, hogy jelzi, milyen serényen dolgozik. Annál inkább aktív a felhasználó személyes adatainak – földrajzi helyzetének, kapcsolati listájának – összegyűjtésében és feltöltésében vezérlőszerverére. Képes továbbá SMS-ek küldésére és törlésére, valamint hívások kezdeményezésére. Ha ez még nem lenne elég a rosszból, a mobiltelefon SD-kártyájára három fájlt tölt le, amelyek közül az egyik nem más, mint egy klasszikus windowsos autorun vírus. Ha az áldozat az USB-n keresztül csatlakoztatja mobilját a PC-jéhez, a rosszindulatú program automatikusan futni kezd, és megfertőzi a számítógépet. Itt aztán a PC mikrofonja segítségével felveszi a felhasználó hangját.

A fordított irányú – Windowsról Androidra történő – fertőzésre jó példa a Troj_Droidpak.A néven futó trójai, amely egy rosszindulatú APK fájlt tölt le és telepít a megfertőzött számítógéphez csatlakoztatott androidos eszközökre. Ez az app online bankolásra használt alkalmazásokat keres a mobileszközön, és megpróbálja átverni áldozatát, hogy az telepítse ezek rosszindulatú változatát, amelyekkel aztán a hackerek hozzáférhetnek a bankszámlájához. A trójaival más vírusok által vagy rosszindulatú web-

oldalak meglátogatásakor lehet megfertőződni, és a kártevő – miután telepítette az androidos malware-t – automatikusan törli magát.

Léteznek olyan fenyegetések is, amelyek az érintett eszköz operációs rendszerével kompatibilis malware-t vetnek be céljaik elérésére. Így működik a WhatsApp üzenetküldő appal kapcsolatos spamkampány is. Ennél a potenciális áldozatot e-mailben értesítik arról, hogy hangüzenetei érkeztek, amelyek meghallgatásához kattintania kell a megadott hivatkozáson. Ha így tesz, egy rosszindulatú fájl töltődik le a gépére, amely attól függően változik, hogy milyen operációs rendszert használ.

Vigyázat, csalok: hasznos appnak álcázza magát a Windowst fertőző androidos vírus

Antivírust minden eszközre

Ha meg akarjuk védeni személyes adatainkat és bankszámlánkat, nem tehetünk mást, mint hogy egy megbízható fejlesztőtől származó biztonsági programmal kiterjesztjük a védelmet minden általunk használt informatikai eszközre. Különösen igaz ez az androidos okostelefonok és tabletek tulajdonosaira, mivel – nem győzzük hangsúlyozni – a hackerek a legnépszerűbb mobil operációs rendszert támadják a legnagyobb erőkkel. Több biztonsági cég kínál olyan, úgynevezett többeszközös (multi device) csomagokat, amelyek tartalmazzák az általunk használt platformokhoz való összes antivírusprogramot. Ezek különálló alkalmazások a leggyakoribb operációs rendszerekhez (Windows, Mac OS X, Android és iOS), amelyek egyenként is megvásárolhatók. Elengedhetetlen továbbá a biztonságtudatos szemlélet kialakítása, hiszen, mint a fenti példákból is kitűnik, az esetek nagy részében egyszerű trükkökkel veszik rá a gyanútlan felhasználókat olyan ártalmatlannak tűnő cselekedetekre, amelyek végső soron PC-jük vagy mobileszközük megfertőzéséhez vezetnek.

Mészáros Csaba

VELED IS MEGTÖRTÉNHET

KÜLDJETEK PÉNZT!

Áldozatunkat a közösségi oldalakon fellelhető adatok alapján célzott támadással rávették arra, hogy lépjen be a Facebook profiljába. Az üzenetben lévő link azonban egy a közösségi oldalhoz kísértetiesen hasonlító weblapra vezetett, ahol az adathalász megtudta emberünk felhasználónevét és jelszavát, majd átirányította őt, hogy az egészből semmit se vegyen észre. Ezek után azonban belépett az ő identitásával, és az összes ismerősének egy levelet írt, mely szerint kirabolták, elvitték mindenét, és emiatt Londonban ragadt, majd pénzt kért a hazautazáshoz, amelyhez egy Western Union számlaszámát adta meg. Az áldozat ismerősei közül sokan átutalták a pénzt, mivel azt hitték, hogy a barátjuk bajban van, ám az összeg valójában a támadóhoz került. Ez csak egy módszer, ahogyan a trükkös tolvajok pénzzé tehetik az ellopott közösségi oldal profilokat, kihasználva azt, hogy az emberek bíznak abban, akit jól ismernek. Ha hozzánk is hasonló kérdéssel fordulnak, a legjobb, ha telefonon vagy más kommunikációs csatornán felvesszük vele a kapcsolatot, mielőtt bármit teszünk.

Flappy Doge
Flappy.me

Flappy Fish
One Minute Game

Flappy 2048
DmWork

Flappy Nyan
isTom Games

A klónok támadása

Az alkalmazásboltokban rengeteg silány programba futhatunk bele. Az egyik legnépszerűbb játék jelenleg például egy másolat másolata.

Nincs szükséged egy androidos képszerkesztőre, netán egy játékra? Bármikor vehetsz egyet nagyjából úgy, mintha egy könyvet rendelnél az egyik webáruházból. A világ „fejlesztői" tömegével árulják a megunt applikációikat, amelyektől szabadulni akarnak, lehetőleg minél nagyobb haszonnal. Az idézőjel alkalmazása tudatos, hiszen sok a szélhámos, akik újrahasznosított programokat árulnak, nagy megtérülésben reménykedve. Ők az App Store farkasai, te pedig a bárány, amennyiben nem vagy kellően körültekintő. Vigyázz velük, még a profik életét is megkeserítik. Ennyit útravalóul, most pedig térjünk rá az üzletre.

Appot vegyenek!

A kínálatot a marketplace.apptopia.com oldalon találod, ahol minőségi, bejáratott, magas letöltésszámmal rendelkező programokba is belefuthatsz, sokszor csomagban. Érdemes elsőként kikérdezni az eladót, hogy rájöjjünk motivációjára. Ha azért akar túladni a programon, mert kiderült, hogy nem rentábilis, inkább álljunk tovább, amennyiben mi sem látunk benne fantáziát. Az optimális eset az, ha a fejlesztő egy remek kódot kínál eladásra, aminek csak annyi a gyengesége, hogy ő nem tudja üzletileg működtetni. Ezek a jó fogások – nem véletlen, hogy külföldön sok ügynökség vadászik a jó programozási képességekkel, ámde pocsék vállalkozási ismeretekkel megáldott fejlesztők megoldásaira. Megveszik a programot bagóért, költenek egy keveset marketingre, majd busás haszonnal működtetik tovább az appot, annak valódi készítője pedig eközben a falat kaparja, hogy mit adott ki a kezéből. Farkasok ezek, akik között nekünk is ordassá kell válnunk. Nézzük át alaposan a megosztott adatokat; szerencsére az Apptopia piacterén minden fontos információt láthatunk: az elmúlt hat, három hónap és harminc nap letöltésszámait, valamint az azokból realizált bevételt, illetve a programra leadott értékeléseket. Minél jobbak a felhasználói vélemények, annál mélyebben a zsebünkbe kell nyúlnunk. Az árak 500 dollártól (körülbelül 120 ezer forinttól) kezdődnek, és a határ tényleg a csillagos ég, cikkünk írásakor például volt olyan tétel, amit 1,5 millió dollárért árultak.

Algoritmus újrahasznosítása

Jobban járunk, ha nem a kész programot, hanem annak csak részeit vesszük meg, majd a hátteret, más grafikai elemeket, a zenéket és a szövegeket kicserélve, egy kissé átcsomagolva újra kiadjuk. Nagyon sokan tesznek így. Szerencsére az Apptopia oldala erre is kínál megoldást, a sablonok (template) között már 100 dollártól vehetünk „átalakítható" programokat. Az oldal ráadásul buzdítja olvasóit a klónok készítésére, annál is inkább, mivel eljárásuk alapján mindössze annyi a dolgunk, hogy megvásárolunk egy kész sablont, lecseréljük grafikai elemeit (például a motoros helyére egy lovat rakunk, beállítunk egy másik hátteret), és beépítjük a kódba, új ikont és képernyőképeket készítünk hozzá, majd optimalizáljuk a

> Megveszik a programot bagóért, költenek egy keveset marketingre, majd busás haszonnal működtetik az appot tovább, a valódi készítő pedig eközben a falat kaparja

felbontást a különböző eszközökre. Ennyi, már készen is vagyunk, mehet a publikálás. Hasonló szolgáltatást kínál a chupamobile.com, az eltérés csupán annyi, hogy a program inkább az újrahasznosított kódokra és azon belül is a játékokra összpontosít, illetve árusai gyakran online tanácsadást, pénz-visszafizetési garanciát is kínálnak kódjaik mellé. Itt jellemzően már 200 dollár alatt is találunk kincseket, ám kétségtelenül szükségünk lesz fejlesztői ismeretekre a személyre szabáshoz, máskülönben programozót kell felbérelnünk, hogy elkészíthessük saját klónunkat. Ha gátlástalanok vagyunk, adhatunk a programnak egy megtévesztő nevet, ikont, teleszórhatjuk reklámokkal, mikrofizetést állíthatunk be, a semmiért egy vagyont kérve, illetve kártevőt is beilleszthetünk a kódba. Ezeket senki se tegye! Csupán arra akartuk felhívni a figyelmet, hogy milyen veszélyei vannak az alkalmazás-áruházakat elárasztó klónoknak, melyek egyre nagyobb számban és mind erőszakosabban fojtogatják a professzionális fejlesztőket. Az újrahasznosított kódok miatt rendkívül könnyű a dolguk, és mint láthattuk, a vírusterjesztők akár jól menő appokba is bevásárolhatják magukat. Számukra azonban egyszerűbb és jövedelmezőbb, ha letöltenek egy éppen népszerű, ámde fizetős programot, feltörik azt (erre is van módszer: hopp.pcworld.hu/11[illegible]), beleteszik a vírusukat, majd publikálják egy alternatív boltban, warezoldalon az eredeti alkalmazás nevével, épp csak mögé teszik a Free utótagot. A felhasználók harapnak erre.

Apptopia: bejáratott, menő appokat is vehetünk

> Androidnál legtöbbször nem emberek, hanem robotok nézik át a publikálásra váró programokat

Hiányos ellenőrzés

A jóhiszemű programozók viszont alaposan megszenvedik az újrahasznosított kódok létét, hiszen nem elég, hogy csinálnak egy kiváló programot, mindent megtesznek annak sikeréért, bevezetnek egy jó üzleti modellt, még a másolókkal is meg kell küzdeniük. Példának érdemes megemlíteni a Beautiful Mess esetét, amely klónok garmadával találta szembe magát az Apple és a Google hivatalos boltjában még tavaly nyáron. A kollázskészítő, képszerkesztő program rövid időn belül fényes karriert futott be. Debütálásakor rögtön az App Store fizetős appokat gyűjtő toplistájának harmadik helyén találta magát hatékony marketingkampányának köszönhetően, nem sokkal később pedig az első pozíciót is megszerezte. Aztán megjelent az első klón, hasonló ikonnal és képernyőképekkel, csak éppen a neve volt más: Beautiful Mess Free. Követője is akadt később a Beautiful Mess Plus és hat másik klón személyében. Az olcsóbban kínált másolatok sikeresek lettek, az Apple alkalmazásboltjában egyikük a top 50 alkalmazás közé is be tudott férkőzni, miközben az eredeti program – aminek elkészítésével ténylegesen dolgoztak – visszaesett. Az Ars Technica beszámolója alapján a cég megpróbálta érvényesíteni szerzői jogait a cupertinói cégnél, ám sokáig eredménytelenül. A probléma az, hogy az Apple ellenőrei leginkább a forráskódot vizsgálják át, csak ritkán nézik azt, hogy hasonló néven van-e már szoftver boltjuk kínálatában, valamint hogy az ikon hasonlít-e egy másik programnál használtra. Így elméletben egy „Instagram Social+" appot is publikálhatnánk, bár vélhetően ez azért már szemet szúrna. A Google Play-en azonban talán átjutna a rostán, hiszen az Androidnál legtöbbször nem emberek, hanem robotok nézik át a publikálásra váró programokat, könnyebb túljárni az eszükön. Nem véletlen, hogy a legtöbb klón és silány alkalmazás a zöld robot szoftverboltjában bukkan fel. Idén májusban például a népszerű 1Password jelszókezelőre úgy sza-

badult rá egy klón, hogy annak csupán a nevét írták át, képernyőképeit cserélték, valamint logóját elforgatták 90 fokban.

A három sokszorozódik

Híres eset a Flappy Birdé is, ami egy rendkívül idegesítő és végtelenül egyszerű játék volt mindaddig, amíg fejlesztője meg nem unta azt a hisztériát, amit kirobbantott. Nyomában özönleni kezdtek a klónok: a Flappy Bee, a Flappy Plane, a Flappy Vacum Cleaner, a Flappy Justin Bieber, és még nagyon sokat kellene írnunk, ha mindet fel akarnánk sorolni. Aki tud, keressen rá iOS- vagy Android-eszközön a „Flappy" szóra az alkalmazásbolton belül, leginkább így tapasztalható meg, milyen méreteket ölt immár az appszemét. Egy másik remek példa a mostanság rendkívül népszerű 2048 játék, ami valójában egy másolat másolata. Az eredetije az Apple áruházában elérhető – több díjat is bezsebelő – Threes!, melyért fejlesztője mindössze 1,79 dollárt kér el. A játék rendkívül addiktív, ennek ellenére sokan nem akartak fizetni érte, és így született meg első klónja, az „1024". Ez már a leírásában sem rejtette véka alá, hogy mely program inspirálta; ugyanazt az élményt kínálta, csak éppen ingyen. Nem sokkal később a böngészőben futó változata is megjelent. Jött azonban az újabb követő, mikor *Gabriele Cirulli* olasz fejlesztő egy hétvége alatt elkészítette az 1024-re épülő, új animációkkal gazdagított 2048-at, amit leginkább gyakorlásként csinált, de lavinát indított el azzal, hogy feltöltötte forráskódját a GitHub-ra, így később bárki hozzáférhetett. Az applikációáruházakat elkezdték elárasztani a 2048 klónok, a másolat másolatának másolatai. Egyre nehezebb ezt követni... Napjainkra már odáig fajult a helyzet, hogy az 1024 büszke arra, hogy ő a 2048 eredetije, pedig szintén másolatról van szó.

> A klónok tömegében könnyedén el lehet rejteni a kártevőket

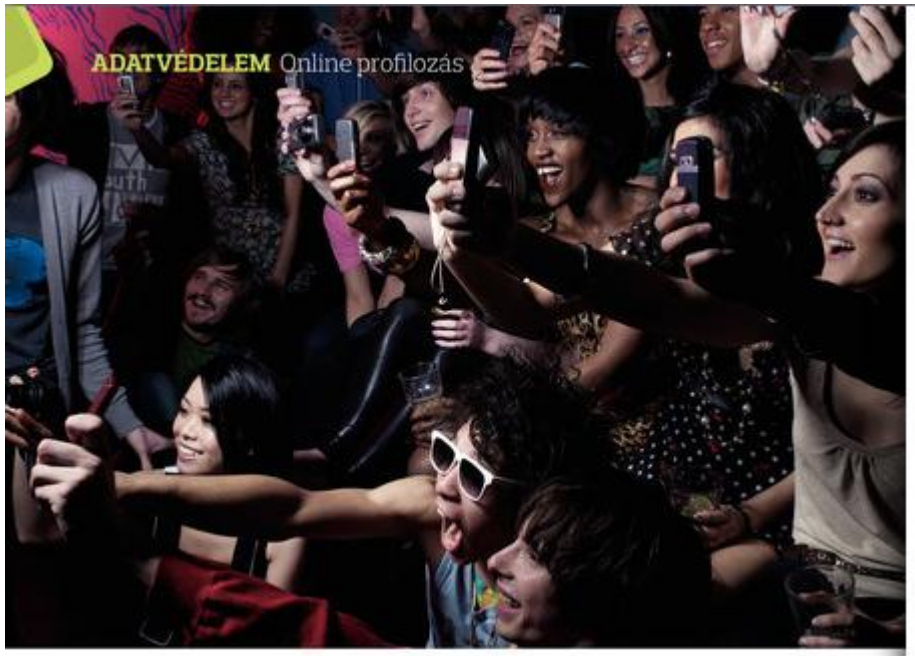
A szomorú tény az, hogy napjainkban már nem kell nagy erőbefektetés egy applikáció elkészítéséhez. Sajnos sok a silány app, ám ennél is nagyobb gond, hogy a klónok tömegében könnyedén el lehet rejteni a kártevőket tartalmazó másolatokat. Emiatt kerüljük el az alternatív alkalmazásboltokat, a gyanúsan jó ajánlatokat (értsd: egy fizetős app ugyanazon funkcionalitást kínáló ingyenes variánsát), és mindenképpen telepítsünk okostelefonunkra egy vírusvédelmi alkalmazást.

Molnár József

VELED IS MEGTÖRTÉNHET

IPAD HELYETT VÍRUS

„Kiválasztottuk Önt az Apple ingyenes ajándékára! Látogasson el a http://apple.hu.vx5.cc... oldalra most, és tekintse meg nyereményét. Kod 8487." Tavaly sokan kaptak ilyen üzenetet nehezen visszanyomozható külföldi telefonszámokról, amely felhívásnak kétségtelenül nehéz ellenállni, hiszen ki nem szeretne ingyen egy táblagépet? Azok jártak jól, akik azonnal törölték az SMS-t, míg akik a telefonszámukat is tartalmazó speciális hivatkozásra kattintottak, azok egy csali oldalra kerültek. Itt megtudtuk, hogy a mobilszolgáltatóknak köszönhetjük a nyereményt (természetesen erről szó sem volt), majd a kód beírása után arra kértek, hogy válaszoljunk néhány kérdésre. Eddig még nagy baj nem történt. A ceremónia végén viszont arra kérték a felhasználókat, egy megadott telefonszámra küldjenek egy SMS-t, hogy esélyük legyen megnyerni a táblagépet. Valójában senkinek sem volt esélye rá, de minden üzenetküldő az SMS-sel feliratkozott egy emelt díjas szolgáltatásra, melynek árát a hónap végén kellett megfizetniük.



A megosztás mellékhatásai

Lájkolunk, feltöltünk, posztolunk és megosztunk – internetes lábnyomunk hónapról hónapra gyarapszik. Az apró információmorzsák alapján azonban kiismerhetők és sebezhetők vagyunk.

Csempész Béla 2012-ben meghackelte a világ egyik legnépszerűbb keresőjét, így a Google keresőjében a „kurvák" kifejezésre a Fidesz, a Magyar Katolikus Egyház és a TV2 weboldala, míg a „gengszterek" szóra az RTL Klub, a rendőrség és a Centrum Parkoló Kft. honlapja bukkant fel. A jelenség nem számít egyedinek, hiszen az Egyesült Államokban pár évvel ezelőtt az akkori amerikai elnök, *George Bush* lett hasonló gonosz tréfa áldozata.

A Google-bombázásnak nevezett támadáshoz nem kell más, mint keresőoptimalizálási szaktudás, valamint sok idő és a megtámadott oldalakra mutató hivatkozás a kiválasztott kulcsszóval. *Csempész Béla* részben emiatt volt beazonosítható, másrészről vesztéhez az is hozzájárult, hogy még a bombázások közepette is dolgozott. A fórumokon elhelyezett ötszáz bejegyzés többségében ugyanis nemcsak a fent említett honlapokon helyezett el hivatkozást, hanem egy csempe-webáruházat is folyamatosan megemlített, természetesen a „csempe" kifejezést használva. A szakemberekben rögtön felvetődött a kérdés, hogy egy gonosz tréfát űző személy miért végez keresőoptimalizálást egy csempeboltnak. Az érintett áruházhoz jutva már nem volt nehéz felkutatni azt, hogy melyik céget bízták meg a munkával, majd a keresőoptimalizáló ügynökség dolgozóinak névsorából már egyértelműen ki lehetett következtetni, ki állhatott a támadás mögött. Innentől pedig a G Data szakértői pontosan tudták, kivel van dolguk, milyen zenét szeret Béla, és így tovább.

A hálózat morzsái

Csempész úr – akit nem lepleznénk le – a jelek szerint keni-vágja a világháló működését, ismeri annak apró trükkjeit, ám még ő sem tudott elmenekülni a fürkésző szemek elől. Aki internetezik, az nehezen tud elbújni. Minden nap nyomokat hagyunk magunk után, minden egyes megosztás, fórum- vagy blogbejegyzés, megjelenés növeli láthatóságunkat. Valójában egy e-mail cím alapján rengeteget meg lehet tudni annak tulajdonosáról. Ha mindezt más adatokkal is kombináljuk, akkor még pontosabb személyiségrajz alkotható.

Hihetjük azt, hogy csak ritka esetekben fordíthatják ellenünk, vagy használhatják fel kereskedelmi célokra elszórt adatainkat, de valójában a nagy cégeknél már bevált módszer az adatbányászat, hogy a kinyert információt többek között marketingcélokra felhasználhassák. Az egyik nagy,

Facebook: a nyilvános bejegyzésekből lakcím és telefonszám is kimenthető

Nick: a Facebook esetenként a beceneveket is elárulja

globális cég adatvédelmi szabályzatában például a következő sorok olvashatók: „Információbeszerzési folyamatai (adatbányászat és profilozás) során a (...) rendszeresen elemzi a közösségi számítási környezetet marketingcélra használható információkért, a meglévő kapcsolatok esetén adategyeztetés, az esetleges új kapcsolatok esetén pedig adatbeszerzés céljából. Ez automatikus módon történik." Persze rögtön hozzáteszik, hogy mindehhez engedélyt kérnek a felhasználóktól, de utóbbit akár egy hosszú felhasználói szerződésben is el lehet rejteni. Másik példaként a Facebookot tudjuk felhozni. Ha ugyanis egy külső szolgáltatásba a közösségi oldalon használt profilunkkal lépünk be, azzal rengeteg értékes információt oszthatunk meg az adott céggel, amely ezt követően kombinálhatja a rendelkezésére álló adatokat.

Visszaélések szerencsére e téren nem jellemzőek, maximum csak több és célzottabb marketinganyaggal árasztanak el minket, amikre nem kötelező igent mondanunk. Rosszabb a helyzet, ha adathalászok célkeresztjébe kerülünk, az internetes bűnözők ugyanis előszeretettel alkalmazzák a profilozást meglehetősen jó hatékonysággal. Ezt támasztja alá, hogy a felmérések szerint évről évre nő a célzott támadások száma, és egyre kisebb cégek kerülnek az alvilág célkeresztjébe. A közösségi oldalak táplálják munciójukat, hiszen az ott kinyerhető információkból könnyen kitapintható a célszemély gyenge pontja.

Google+: használjuk a köröket

Vegyük például egy kutatás-fejlesztéssel foglalkozó vállalat vezetőjét, aki aktív LinkedIn életet él, több száz kapcsolattal. A céges közösségi oldal információi részint publikusak, azokból bárki tud informálódni. Támadónk felkeresi a cégvezető profilját, azt, hogy mivel foglalkozik, és kik a kapcsolatai. Az egyik ismerősére hivatkozva ezt követően küld egy levelet hitelesnek tűnő e-mail címről, amiben egy remek ajánlatra hívja fel a figyelmet, egy – nulladik napi sérülékenységet kihasználó – PDF-csatolmányon keresztül. Megnyitnánk? Ha hitelesnek tűnik, akkor jó eséllyel igen, és így azon nyomban megfertőznénk gépünket és a céges hálózatot, ahova a hacker már könnyedén besétálhat. Rémisztő? Valóban az, főként hogy az internetes feketepiacon jó pénzért majdnem mindig lehet kapni nulladik napi sérülékenységet.

Pokolba a lánclevelekkel

Régen is végeztek hasonló felderítéseket, ám a közösségi oldalak korszaka előtt nehezebb volt az adathalászok dolga. Próbálkozások akkor is voltak, s nem is gondolnánk, hogy közülük talán a legveszedelmesebb a hoax volt. „Ezt a levelet küldd tovább még tíz embernek, és akkor..." – bizonyára mindenki találkozott ilyen üzenetekkel, melyeket az kezelt jól, aki olvasás után azonnal törölte az e-mailt. A kapcsolatok feltérképezésére és a levélcímek gyűjtésére ugyanis a hoax remek eszköz volt, mert a támadó rendszerint titkos címzettként szerepelt. Minden egyes átvert felhasználó újabb e-mailekhez és kapcsolati hálóhoz juttatta a támadás kitervelőjét. Minél több adat volt a delikvensről beszerezhető – fórumokból, blogokból és így tovább –, annál hatékonyabb volt a csalilevél. Ám nem véletlen az, hogy az elmúlt években eltűntek ezek a levelek: egyrészt a közösségi oldalak feleslegessé tették a hoaxokat, másrészt az internetezők is felismerték azok rejtett hátsó szándékát.

GplusData: Facebook Graph klón Google+-felhasználókhoz

E ponton rögtön megadnánk az első jó tanácsot: soha ne küldjünk ki tömeges e-mailt egymás számára idegen címzetteknek úgy, hogy a címeket nem a titkos másolat mezőbe rakjuk. Nemcsak idegesítő ugyanis az, amikor egy hivatalos e-mail listájáról több mint ötven vagy netán száz vadidegen ember postafiókját olvashatjuk le, hanem veszélyes is. Elég, ha a címzettek között egyetlen rosszindulatú személy van, máris megtörténhet a baj.

Gyors önvizsgálat

Most, hogy már tudjuk, miért veszélyes a túlzott megosztás, nézzük, mennyi információ található a neten rólunk, jobb, ha mi találunk meg elsőként egy olyan adatot, amit egyébként nem tennénk közszemlére. Ha időben lépünk, még megelőzhetjük a bajt. Elsőként célszerű a Google keresőjét bevetni, mivel olyannyira kézenfekvő a használata, hogy mások is vélhetően ott fognak próbálkozni elsőként. Mondjuk a HR-es is így fog leinformálni minket, ha egy állásra jelentkezünk.

Jelen esetben tudjuk a célpont nevét (mivel rólunk van szó). Keressünk rá nevünkre, ami akár instant

eredménnyel is járhat, ha ritka családnévvel rendelkezünk. Ha túl sok a találat, kombináljuk a kifejezést egy olyan információval, ami köztudott rólunk, például munkahelyünk, munkakörünk vagy lakóhelyünk célravezető lehet (például: „Molnár József PC World", vagy „Molnár József újságíró" és így tovább). Ha netán olyan találatra bukkannánk, ahol személyes adataink – lakcím, telefonszám – is elolvashatók, azonnal cselekedjünk. Ha csak egy adott szolgáltatáson vagy oldalon szeretnénk kutatni, szűkítsük le egy domainre a keresést (például „site:pcworld.hu Molnár József"). Ezzel a formulával egyébként hasznos a közösségi oldalakat is átkutatnunk („site:linkedin.com Molnár József" vagy „site:facebook.com Molnár József"). Mark Zuckerberg közösségi oldalánál az utóbbi formula sok esetben azonnal hasznosítható eredményt hozhat, hiszen az egyedi URL igénylésekor sokan a nicknevüket adták meg, melynek ismeretében tovább kutathatunk. Saját példám is ezt mutatja, hiszen facebook.com/hmolnarj című oldalam alapján beazonosítható vagyok, a Google keresőjében ugyanis a „hmolnarj" kifejezést begépelve számos olyan szolgáltatás bukkan fel, amit a nevem alapján egyébként nem lehetne egyértelműen hozzám rendelni. Sőt akár fotókra is rátalálhatunk, a keresőrobotok ugyanis a profilképeket és a képfeltöltő szolgáltatások nickhez köthető fájljait is megtalálják.

Pipl: Hamar lebuktatnak minket az adatbányászok

Amennyiben nem járnánk sikerrel, egyrészt kivételesen ne keseredjünk el, mert az a jó, másrészt vessük be a nehéztüzérséget. Ilyen például a hazánkban is jól használható pipl.com, ami hatékony fegyver lehet akkor, ha egy kör-e-mail kerül a birtokunkba. Menyasszonyomnak például anno az új oktatási intézménye nem titkos címzettként értesítette ki a felvett személyeket, ami nagy hiba volt, hiszen a Pipl segítségével fél óra alatt rengeteg mindent kiderítettünk új csoporttársairól. Nevüket, kedvelt zenéiket, korábbi iskoláikat, politikai hovatartozásukat, és még hosszasan sorolhatnám a kinyert információkat, pedig csak egyetlen keresőt használtunk.

A pipl.com a hagyományos keresőknél sokkal mélyebbre tud hatolni a web nyilvános, kereshető adattábláiban. A szolgáltatás megpróbál egy adott kifejezéshez – legyen az egy név, e-mail cím vagy nick – kigyűjteni minél több releváns információt egyetemi publikációkból, bírósági papírokból, közösségi oldalakról stb. Végezzünk itt is önvizsgálatot. Keressünk rá a nevünkre, és vizsgáljuk át a kapott eredményt. Ha nem túl gyakori névvel rendelkezünk, akkor szinte biztos, hogy az oldalsávon azonnal megjelenik majd az arcképünk, s ezt követően a személyes és üzleti adatok között is könnyen előjöhet egy hozzánk köthető találat, ám azt biztosan megtudhatjuk, hogy a weben mely névrokonunk rendelkezik a legnagyobb webes lábnyommal. Következő lépésként keressünk rá az e-mail címünkre és a gyakran használt felhasználónevünkre, amely esetekben vélhetően sok konkrét, hozzánk köthető tartalomhoz fogunk jutni. Minél több a találat, annál nagyobb a digitális lábnyomunk.

Ahol mindenki leinformálható

A rengeteg nyilvános adatbázisnak köszönhetően az Egyesült Államokban már egész iparág született a legális adatbányászatra, illetve ellenpólusként a fellelhető találatok eltüntetésére. Az online háttérelemzés a tengerentúlon már olyan szinten elterjedt, hogy több fejlesztőcég is kínál ilyen szolgáltatást. Hazánk e téren (is) lemaradásban van részben a publikus adatbázisok csekély száma miatt – talán mondhatjuk, hogy szerencsére –, és egyelőre nem úgy tűnik, hogy ez rövid időn belül változna. Pedig az amerikaiak így le tudják előre informálni bébiszitterüket, leendő orvosukat, illetve azt a környéket, ahol élnek, vagy ahova terveznek költözni. A zabasearch.com például név és állam alapján megjeleníti a keresett személy lakcímét és telefonszámát, míg a whitepages.com az üzletek elérhetőségeit is fel tudja kutatni. A puszta telefonkönyv-helyettesítésnél többet kínál a criminalsearches.com, ami megmondja, hogy a keresett személy büntetett előéletű-e, és ha igen, akkor mit követett el. Az ingyenes szolgáltatások közül megemlíthető még a publicrecords.searchsystems.net is, ami anyakönyvi és házassági kivonatot is kínál, igaz, a teljes adatlapért fizetni kell.

Megregulázott megosztások

A webes keresők után kutakodjunk a közösségi oldalakon. A Google+, a Facebook, a LinkedIn és a Twitter audit egyaránt fontos. Elsőként lépjünk be *Mark Zuckerberg* közösségi oldalára, majd a kattintsunk a felső vezérlősáv utolsó előtti elemére, a lakatos

felsorolás ikonra, majd a [Ki láthatja a dolgaimat?] csoporton belül keressük a [Megtekintés mint...] hivatkozást, amely megmutatja azt, hogy vadidegen emberek mit láthatnak a profilunkat meglátogatva. Ha valami olyat találunk, amit nem szeretnénk másoknak is megmutatni, próbáljuk meg elrejteni a beállítások adatvédelmi szekciójában, bár nem mindent lehet. Ha egy szenzitív információ az oldalsávon található, egyszerűbb dolgunk van, hiszen a dobozok jobb felső sarkába húzva az egeret megjelenik a szakaszok szerkesztésének lehetősége, ahol elrejthetjük az egyes boxokat. Külső segítségként érdemes még bevetni a Privacy Fix megoldását (privacyfix.com), ami egy böngészőbeépülőn keresztül adatvédelmi szempontból ráncba tudja szedni Facebook-jelenlétünket.

A Twitterre nem pazarolnánk túl sok szót, mivel a mikroblogon jellemzően minden megosztás publikus, így ott semmilyen személyes adatot nem ajánlatos kicsiripelni. Ha korábban mégis elkövettük ezt a hibát, akkor navigáljunk a tweethez, és a kuka ikonjára klikkelve töröljük a bejegyzést. A Google+ pedig túl kicsi, de ha mégis aktív életet élünk rajta, akkor jobb, ha visszanézzük, hogy milyen információkat osztottunk meg publikusan, illetve hogy a privátnak vélt köreinkben valóban csak ismerős egyéneket találunk-e.

Végezetül foglalkozzunk a LinkedInnel, amire különösen fontos odafigyelni, hiszen a céges információkra és dolgozókra vadászó adathalászok előszeretettel szemlézik. Mivel egy szakmai telefonkönyvről van szó, nem tehetjük meg, hogy teljesen eltüntetjük róla adatainkat, ám van, amit érdemes elrejteni. A művelethez a profiloldalunkon az [Edit] gombra kattintva a [Manage public profile settings] opciót válasszuk, majd rejtsük el korábbi munkahelyeinket, iskoláinkat; aki keres, az amúgy is jellemzően jelenlegi pozíciónk miatt akar velünk kapcsolatba lépni. Ha végeztünk, dőljünk hátra, egy fokkal nehezebb lesz kiismerni/átverni minket.

Molnár József

Jó tanácsok

- A közösségi oldalakon kerüljük a publikus megosztásokat: telefonszámunkat, lakcímünket és egyéb személyes információinkat még véletlenül se adjuk meg idegeneknek.
- Csak olyan adatot osszunk meg cégünkkel kapcsolatban, amit a munkahelyi konyhában is elmondanánk vadidegeneknek.
- Az emberek általában szokásaik rabjai, előszeretettel használják ugyanazt a felhasználónevet majd' minden szolgáltatásnál. Ha lehet, váltogassuk a becenéveket.
- A fórumokra írt több évvel ezelőtti hozzászólásaink is bármikor napvilágra kerülhetnek. Saját nevünkkel, illetve gyakran használt felhasználónevünkkel csak olyasmit posztoljunk, amit évek múltán is vállalnánk.
- Amit mi megtalálunk magunkról, azt mások is meglelhetik.
- Ne nyissunk profilt gyermekünk nevében egyik közösségi oldalon sem, várjuk meg, hogy ő tegye meg azt.
- Ha gyermekünk előszeretettel szörföl a közösségi oldalakon, vagy cseverészik a neten keresztül, használjuk a szülői felügyelet szoftverek adatszivárgás elleni védelemét.
- Ha idegen személytől e-mail érkezik, ami egy csatolmány megnyitására buzdít, legyünk kellően elővigyázatosak.

Privacy Fix: adatvédelmi böngésző segéd

Mindent eltörölni

A regisztrálás a legtöbb népszerű webes szolgáltatás esetében pofonegyszerű, ám ha deaktiválni akarjuk profilunkat, akkor számos buktatóba belefuthatunk. Teszteltünk és menekültünk, de nem mindig sikerrel.

Nehézségi fokozatok

Cikkünkben a szolgáltatóknál ötfokozatú skálán osztályoztuk a kilépés nehézségi fokozatait. Minél több futó embert látsz, annál távolabb kerülhetsz a megoldásoktól. Egy pont esetén például nem mondhatjuk fel klubtagságunkat, két rohanó embernél lehet, de nem könnyű szabadulni a szorításból, míg az öt pont a felhasználóbarát oldalakat jelöli. Listánk nem teljes, inkább figyelemfelkeltésre alkalmas.

Facebook

Nem egyszerű megtalálni a közösségi oldalon a törlés lehetőségét. A [Beállítások] alatt ugyan a [Biztonság] menün belül a sor legalján megláthatjuk a [Fiók felfüggesztése] lehetőséget, ám ez nem végez teljes takarítást, hiszen bármikor újra aktiválhatjuk fiókunkat. Ettől függetlenül a Facebook úgy tesz, mintha végleges búcsút venne tőlünk, megmutatja ismerőseinket, akikkel már soha nem fogunk kapcsolatba lépni (legalábbis az arckönyv oldalán), illetve a kilépés okáról is meginterjúvol minket. Ne dőljünk be neki, ez nem a törlés, ami viszont egy kissé el van rejtve, de nem jelenti azt, hogy nem létezik (**hopp.pcworld.hu/5[illegible]**). Az oldalon az OK gombra kattintva jelszavunkkal és egy Captcha-kód megadásával kell megerősítenünk szándékunkat, majd csupán arra kell figyelnünk, hogy lehetőleg 14 napig ne jelentkezzünk be újra, mivel az érvényteleníti törlési kérvényünket. Illetve aki szeret angol nyelven levelezni, az a **privacy@facebook.com** e-mail címen kérvényezheti a törlést, bár arra készüljünk fel, hogy jó eséllyel napokig nem érkezik majd válasz.

SZÖKÉS NEHÉZSÉGE

Microsoft

Jól gondoljuk meg, mielőtt egy Microsoft- vagy régebbi nevén Live ID-fiókot törlünk, mivel a folyamat visszafordíthatatlan, az utasítás kiadását követően már nem fogunk tudni bejelentkezni korábbi profilunkba. E téren a redmondiak megoldása jól vizsgázott, de azért nem tökéletesen, mivel a szoftvercég egy kevés adatot megtart magának, anonim módon járulunk hozzá termékeink fejlesztéséhez. A meneküléshez a **login.live.com** oldalon jelentkezzünk be, majd a megjelenő oldalon kattintsunk a [Biztonság és adatvédelem], majd a felugró weblap alján lévő [Fiók megszüntetése] lehetőségre, és kövessük az utasításokat. Fontos, hogy ha rendelkezünk csatolt fizetős szolgáltatásokkal (Xbox Live, Hotmail Plus), akkor azokat is be kell zárnunk a fiók teljes bezárása előtt. Persze lehet, hogy ekkor nem érdemes kilépni.

TIPP **60 napos türelmi idő**

Ha egy gyors hivatkozásra vágysz, akkor keresd fel az **account.live.com/CloseAccount.aspx** oldalt. Fontos, hogy ebben az esetben csak inaktívvá válik a fiók, s akkor törlődik teljesen, ha 60 napig nem lépünk be.

SZÖKÉS NEHÉZSÉGE

A Google klubból is meglehetősen egyszerű kijelentkezni, s szerencsére több lehetőség közül is választhatunk: törölhetjük csak a Google+ profilunkat, bezárhatjuk Gmail postafiókunkat, eltüntethetjük a böngészési előzményeinket, illetve akár az összes Google aktivitásunknak búcsút mondhatunk. Utóbbit az accounts.google.com oldalon tehetjük meg, ahova bejelentkezve a főoldal [Fiókkezelés] profiljában válasszuk a [Google-fiók és a hozzá tartozó adatok törlése] lehetőséget, ekkor a Google szembesít majd minket azzal, hogy mi mindennek intünk búcsút. Ha eltökéltek vagyunk, akkor erősítsük meg szándékunkat. Profiloldalunkon egyébként a [Profil törlése és a kapcsolódó Google+ funkciók eltávolítása] lehetőségen belül kérhetjük csak a pluszos profilunk bezárását. Ha csupán Gmail levelezőfiókunkkal akarunk leszámolni, akkor azt a hopp.pcworld.hu/[illegible]2 oldalon tehetjük meg, míg internetes keresési előzményeinket a hopp.pcworld.hu/[illegible]3 webcímen nullázhatjuk le, ha nem akarunk releváns hirdetéseket és találatokat.

SZÖKÉS NEHÉZSÉGE

Rossz hírünk van az Apple híveinek. Jelenleg az Apple ID törlése nem lehetséges, akárhol kerestük, nem találtuk az erre létrehozott linket. Ez azért van, merthogy nincs is, a fórumbejegyzések alapján ugyanis az Apple ügyfélszolgálatával kell felvenni a kapcsolatot e-mail vagy telefon útján, és akkor elindítják a törlési eljárást. Ám ekkor sem biztos, hogy sikerrel járunk, mivel egy elhalálozott személynél például bekérik a halotti bizonyítványt, amit ekkor a cég jogi osztálya is átnéz, és ha megalapozott a kérés, jóváhagyják. Nem egyszerű tehát az Apple felhőjéből kimenekülni, így jelenleg csak egy lehetőségünk van: lépjünk be profilunkba, töröljük ki valós nevünket, és írjuk át bankkártya-adatainkat, legalább a pénzünkhöz ne férhessenek hozzá. Ha korábban vásároltunk zenét, akkor azt teljes egészében elveszítjük, mivel az Apple DRM-védelemmel látja el muzsikáit. Szerencsére utóbbit könnyen megkerülhetjük az AimerSoft ingyenes iTunes DRM Remover (hopp.pcw[illegible].hu/[illegible]) szoftverével.

SZÖKÉS NEHÉZSÉGE

Pár évvel ezelőtt még főként a növekedésre összpontosított a céges közösségi oldal, s mint ahogy az lenni szokott, a lehető legjobban megnehezítette a klubból kilépést. A törlés több napot vett igénybe, az ügyfélszolgálat e-mailjét vissza kellett igazolni, ráadásul addig folyamatosan küldözgették a leveleket, hogy maradásra bírják a távozni vágyókat. Immár könnyebb dolgunk van, hiszen a LinkedIn jobb felső legördülő menüjén belül a [Privacy & Settings] alatt, majd a megjelenő oldalon az [Account] csoportban ott találjuk a [Close your account] linket, amin keresztül bezárhatjuk közösségi fiókunkat. Ne várjunk tökéletes eredményt, hiszen 30 napon belül újraaktiválhatjuk profilunkat, azaz legalább egy hónapig megtartják fontos információinkat. Sőt a felhasználói szerződés 2.2-es pontja (hopp.pcworld.hu/[illegible]) alapján a regisztrációval feljogosítjuk a LinkedInt arra, hogy az általunk megadott információkat, ötleteket és koncepcióinkat szabadon felhasználhassa, analizálja, kereskedelmi célokra felhasználja. Vagyis csak óvatosan osszuk meg információinkat.

SZÖKÉS NEHÉZSÉGE

Nincs könnyű helyzetben az, aki törölni akarja Skype-fiókját, ugyanis csak nagyon macerásan lehet. A csevegő és VoIP-szolgáltató terméktámogatási oldala (hopp.pcworld.hu/[illegible]) szerint nem lehet önkiszolgáló módon megtenni ezt, csak úgy, ha levelet írunk a cég ügyfélszolgálatának, amelynek – a cég bevallása alapján – legalább két hétre van szüksége a deaktiváláshoz. Így ez esetben a Skype azt ajánlja, hogy profilunkról tüntessünk el minden személyes információt, így legalább a felhasználók nem fognak ránk találni.

SZÖKÉS NEHÉZSÉGE

A Twitterről sem tudunk azonnal kivonulni, mivel csak deaktiválásra van lehetőség, ami 30 nap inaktivitás után végleges törléssé alakul át. A részleges kijelentkezéshez lépjünk be a fiókunkba, klikkeljünk a fogaskerékre, majd a [Beállítások] opcióra. A megjelenő oldalon a [Fiók] csoport alján keressük meg a [Felhasználói fiókom deaktiválása] hivatkozást, majd válasszuk a deaktiválást.

SZÖKÉS NEHÉZSÉGE

Tisztességes háziúr a Dropbox, hiszen amint jelezzük kilépési szándékunkat, csupán szomorúságát fejezi ki, ámde azonnal elenged minket. A művelet a dropbox.com/account/delete oldalon végezhető el, ahol a jelszavunk újra begépelése után a [Delete my account] gombra klikkelve azonnal véget vethetünk dropboxos pályafutásunknak. Fontos, hogy ilyenkor csak a felhőben tárolt állományaink vesznek el.

SZÖKÉS NEHÉZSÉGE

Az Adobe által kínált felhasználói fiókhoz meglehetősen könnyű hozzájutni, ám annak törlése már igazán kemény dió, angol nyelvtudás nélkül gyakorlatilag lehetetlen. Vagy levelet kell írnunk a privacy-officer@adobe.com e-mail címre, vagy munkaidőben tárcsáznunk az Egyesült Államokban lévő 800-833-6687 telefonszámot, bejelentve igényünket. Az időeltolódásra mindenképpen figyeljünk oda.

SZÖKÉS NEHÉZSÉGE

VELED IS MEGTÖRTÉNHET

CSALI HOTSPOT

Legyen újabb történetünk szereplője János, aki az egyik reggel arra ébred külföldön, hogy az éjszaka elpókerezte a pénzét. Hogyan lehetséges ez? A hotelbe megérkezve gyorsan ellenőrizni akarta a leveleit, de mivel a drága roaming miatt a 3G hálózatra nem akart rácsatlakozni, ezért tett egy próbát a szálláshely Wi-Fi-jével. Sikerült a kapcsolatot kiépíteni, majd megjelent egy felület, mely szerint napi 2 euróért cserébe ingyen használhatja a hálózatot, amihez meg kellett adnia a bankkártyaadatait. Akik utaznak, azoknak nem lesz új ez az egyébként legális megoldás, ám a gonosz ikerre csak kevesen számítanak, sőt sokan nem is tudják, hogy az mire való. Ez az adathalászok kedvelt megoldása, akik egy legitimnek tűnő hely nevében csali Wi-Fi hálózatot alakítanak ki, amelynek forgalmát végig figyelik. Jánostól így tudták kicsalni bankkártyaadatait. Este aztán az adataival a támadók beléptek egy privát pókerszobába, ahol a tolvaj direkt veszített, hogy így átjátssza a társai számlájára a tisztára mosott pénzt.

Mit árulnak el rólad eszközeid?

Árulkodik a telefon, a laptop, a tábla: megjegyzik, merre jártunk nap közben, mire kerestünk rá az interneten, és kivel beszélgettünk. Utánajártunk, mit tudhatnak rólunk megfigyelőink.

Edward Snowden kiszivárogtatásai nyomán 2013 májusában kirobbant megfigyelési botrány igazolta, amiről az összeesküvés-elméletek rajongói már régóta beszélnek: *George Orwell* Nagy Testvére tényleg figyel minket. És nem csak „ő". Az amerikai és a brit kormány, az NSA és a GCHQ mellett sajnos mások is kémkednek az internetezők és mobilfelhasználók után. Köztük a hirdetők, a kommunikációs szolgáltatók, az alkalmazásfejlesztők, a közösségi oldalak és az online infrastruktúrát üzemeltető IT-vállalatok is: a Google, a Microsoft és az Apple. Az adatvadászoknak számos rendkívül hatékony eszköz áll a rendelkezésükre, hogy összeszedhessék az őket érdeklő információkat. Köztük olyanok is, amelyek egész nap ott vannak a zsebünkben, az íróasztalunkon vagy a hálószobánkban – az okostelefonoktól és táblagépektől a PC-ken és televíziókészülékeken át a hordható elektronikai eszközökig és az okos mérőeszközökig.

Okosabb vagy, mint a telefonod?

Az első iPhone 2007-es bemutatása óta az okostelefon-piac az IT-ipar legsikeresebb szegmensévé vált. A gyártók az Apple-től a Google-ig, a Samsungtól a Lenovóig sorra mutatják be az újabb és újabb modelleket; 2013-ban már több okostelefon fogyott, mint „buta": közel 968 millió darab.

De vajon mennyire okos egy okostelefon? Nos, épp elég okos ahhoz, hogy minden mozdulatunkat nyomon kövesse, és minden szavunkat rögzítse. Ezeket a készülékeket kifinomult hardverek egész arzenáljával fegyverezték fel a gyártók: van bennük mikrofon, GPS-chip, gyorsulásmérő, Wi-Fi-antenna és különféle szenzorok. Elsődleges céljuk, hogy megkönnyítsék számunkra a kommunikációt és az információkhoz való hozzáférést – de egyúttal az adatainkra ácsingózók dolgát is egyszerűbbé teszik. Nem véletlen, hogy a biztonsági szakemberek szerint egyre több kártékony program tenyészik a mobileszközökön. Köztük olyan távoli hozzáférést biztosító trójaiak is, amelyek képesek arra, hogy Bond-filmbe illő kémkütyüt csináljanak a telefonunkból: elemeljék jelszavainkat, titokban video- és hangfelvételeket készítsenek rólunk, vagy támadást indítsanak más rendszerek ellen.

Okostelefonjaink többféle módon is feltörhetők. 2010-ben a New Jersey-i Rutgers Egyetem kutatóinak sikerült rootkittámadást intézniük okoskészülékek ellen, ami lehetővé tette, hogy a mikrofont bekapcsolva rögzítsék a felhasználók beszélgetéseit, és a GPS segítségével megfigyelhessék mozgásukat. A mobilos kártevők ráadásul sokkal ártalmasabbak lehetnek, mint a hagyományos számítógépekre írt társaik. Telefonunkat mindenhová magunkkal visszük, így a hackerek sokkal többet tudhatnak meg rólunk, mintha a PC-nket fertőznék meg: akár bizalmas üzleti vagy magánbeszélgetésekbe is belehallgathatnak.

Zsebkémek

A tulajdonosaik után kémkedő okostelefonok nemcsak azokra nézve lehetnek veszélyesek, akiknek takar-

A biztonsági szakemberek szerint egyre több kártékony program tenyészik a mobileszközökön

Árulkodó okostelefon: a gyártók is megfigyelnek minket

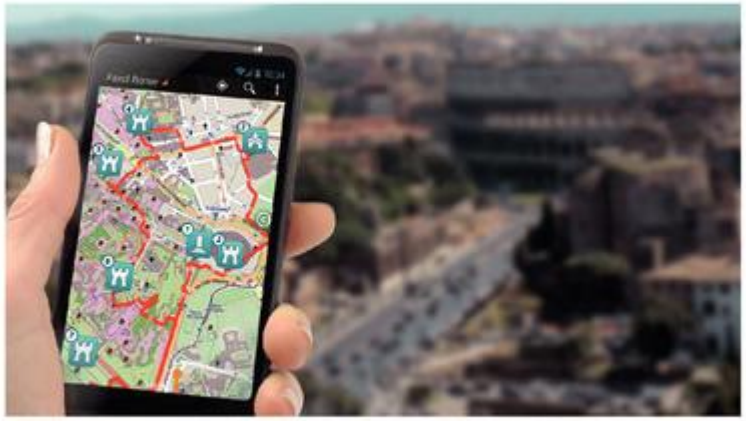
gatnivalójuk van. Egy, az Egyesült Államok hadserege által kifejlesztett Android-alkalmazás például képes arra, hogy a kamera és a gyorsulásmérő segítségével háromdimenziós térképet készítsen egy készülék környezetéről. A PlaceRaider nevű app ártalmatlan kameraalkalmazásnak adja ki magát, de valójában folyamatosan gyűjti az adatokat a felhasználókról, amelyeket aztán egy külső szerverre továbbít. Segítségével akár betörők, személyiségtolvajok vagy más bűnözők is pontos, valós idejű és részletes alaprajzot készíthetnek lakásunkról vagy irodánkról.

Nemrégiben a University of Alabama kutatói számoltak be egy új, minden eddiginél szofisztikáltabb fenyegetésről: az úgynevezett kontextustudatos (context-aware) támadásokat bizonyos hangok, mágneses vagy vizuális ingerek aktiválják. Ezek a kártékony programok olyan vírusok, amelyek „alvó ügynökké" változtatják telefonunkat, amely aztán a megfelelő pillanatban aktivizálódva minden titkunkat kiszolgáltatja a bűnözőknek.

Az okostelefonok mellett a táblagépek is veszélyesek lehetnek. A legtöbb táblagépen ugyanaz az operációs rendszer fut, és ugyanazokkal a technológiákkal szerelték fel őket, mint a modern mobilokat – nem véletlen, hogy a velük kapcsolatos biztonsági fenyegetések is hasonlók. Ott van mindjárt a gyorsulásmérő. Ez az eszköz felel többek között azért, hogy ha elfordítjuk a táblát a kezünkben, a kijelző képe is vele forduljon. Sajnos, az életünket is a feje tetejére állíthatja; ahogy azt egy, a University of California kutatói által készített tanulmány is bizonyítja, akár személyes azonosítóink eltulajdonítására is használható. Az egyetem munkatársai készítettek egy speciális billentyűzetfigyelő alkalmazást, amely 70 százalékos pontossággal képes nyomon követni, hogy milyen gombokat nyomunk meg táblagépünk virtuális klaviatúráján. Nyugtalanító helyzet: a TouchLogger nevű app segítségével a csalók minden adatunkhoz hozzájuthatnak.

A tévé visszanéz

Sajnos a hackerek nemcsak mobileszközeinken keresztül kémkedhetnek utánunk, használhatják akár a tévénket is. A ReVuln kiberbiztonsági vállalat szakemberei 2012 decemberében felfedezték, hogy súlyos biztonsági rés tátong a Samsung egyik okostévéjének szoftverében. A hibát kihasználva a hackerek játszva megtudhatták, hogy milyen filmeket néztek a felhasználók, hozzáférhettek a merevlemezen tárolt fájlokhoz, és azokat az eszközöket is megfertőzhették, amelyek USB-porton keresztül csatlakoztak a készülékhez. *Luigi Auriemma és Donato Ferrante,* a ReVuln társ-vezérigazgatói szerint minden olyan berendezés sebezhető, amely valamilyen módon – például Wi-Fi-n keresztül – kapcsolatba kerülhet más eszközökkel. „Egy eszköz akkor is veszélybe kerülhet, ha nem csatlakozik az internetre. Elég egy fertőzött PC, hogy a helyi LAN-hálózaton keresztül megtá-



Adatgyűjtők: szinte minden mobilalkalmazás gyűjti az adatainkat

madhassák a hackerek; de akár egy Wi-Fi- vagy USB-kapcsolat is támadási felületet jelenthet" – nyilatkozta a *TechNewsDaily*nek adott interjújában *Auriemma* és *Ferrante*.

A gyártók egyre több háztartási eszközt látnak el ilyen „támadási felületekkel", amivel párhuzamosan egyre nő az esélye annak, hogy kémprogramok valamennyi otthoni és irodai eszközünket megfertőzzék. Mint a 2012-ben felfedezett Flame (más néven Flamer vagy Skywiper) „mega malware", amely USB-kapcsolatról USB-kapcsolatra terjedve több száz Windows XP-t, Vistát és Windows 7-et futtató számítógépet fertőzött meg, lehetővé téve a hackerek számára, hogy kifinomult kémakciókat hajtsanak végre. A Flame – amelyet valószínűleg valamelyik kormány programozói írtak – a billentyűleütések rögzítésére, képernyőfelvételek készítésére, az online és offline felhasználói aktivitás nyomon követésére, a ki- és bemenő kommunikáció monitorozására is alkalmas volt. Sőt, arra is, hogy olyan eszközökről lopjon le információkat, amelyek Wi-Fi-hálózaton keresztül csatlakoztak a fertőzött gépekhez. Belegondolni is rossz, mi mindenre lennének képesek a hackerek, ha Android- vagy iOS-rendszerekre is telepíthetők lennének hasonló férgek.

A kábel másik végén

Sokan azt gondolják, hogy mivel televíziókészülékük nem csatlakozik az internethez, tévénézési szokásaikat senki sem tudja nyomon követni. Sajnos tévednek. 2011-ben a Verizon amerikai kommunikációs szolgáltató benyújtott egy szabadalmi kérelmet az USA illetékes hivatalához. A technológiai leírásban egy olyan set-top-box szerepelt, amelyet audio- és mozgásszenzorokkal is elláttak, hogy nyomon követhessék a felhasználók mozgását és kommunikációját, és az így kapott információkat elemezve célzott hirdetésekkel bombázhassák őket. Ha jóváhagyják a szabadalmat, az új korszakot nyithat a felhasználói adatok gyűjtésében – és egyúttal azt is jelentheti, hogy többé egyetlen szórakoztatóelektronikai eszköz közelében sem érezhetjük majd biztonságban a személyes adatainkat.

Kémkedő tévé: a kémprogramok a tévénket is megfertőzhetik

Szerencsére, a felhasználók után kémkedő set-top-boxok egyelőre még nem jelentek meg a piacon. Ott vannak viszont a játékkonzolok: a Microsoft Kinect mozgásérzékelő rendszerrel felszerelt Xboxai például szorgosan gyűjtik a különféle információkat tulajdonosaikról. A gyártó 2010-ben dobta piacra az első ilyen készüléket, tavaly pedig bemutatták a doboz legújabb változatát, az Xbox One-t. A One az Xbox Live szolgáltatáson keresztül kapcsolódik az internetre – amely, ha a felhasználók nem kapcsolják ki manuálisan, folyamatosan küldi az információkat a távoli szerverekre. Tovább bonyolítja a helyzetet, hogy nem tudni, milyen adatbázisokba továbbítja a tulajdonosairól gyűjtött információkat a konzol. Érdemes azonban megjegyezni, hogy a Verizonhoz hasonlóan a Microsoft is beadott egy szabadalmi kérelmet: egy olyan alkalmazást szeretnének levédetni, amely folyamatosan nyomon követi felhasználói szokásainkat, és az így szerzett adatok alapján különféle kampányokkal, akciókkal és más promóciókkal célozhat meg minket.

Akkor sem vagyunk biztonságban, ha eldobjuk okostelefonunkat, száműzzük a nappaliból a tévét és a játékkonzolt. Az „okos" háztartási berendezések – mint amilyenek az érintőkijelzővel felszerelt hűtőszekrények vagy a vezeték nélküli mérőeszközök – is segíthetnek a hackereknek, hogy belessenek otthonunkba. Tavaly egy csapat német mérnök egy kísérlet során bemutatta, milyen járulékos sérülékenységei vannak az okos mérőeszközökből álló rendszereknek. A szakembereknek sikerült betörniük egy elektronikai szolgáltató vezeték nélküli hálózatába, és megszerezniük a felhasználók bizalmas adatait. A lakások fogyasztásának „digitális ujjlenyomatából" meg tudták mondani, mikor tartózkodtak otthon a tulajdonosok; könnyen belátható, milyen veszélyeket rejtene magában, ha bűnözők – például hackerekkel összedolgozó betörők – tennék rá a kezüket ilyen információkra.

Bevett üzletmenet

Ahogy azt korábban is említettük, nem csak a hivatásos hírszerzők vagy a számítógépes bűnözők kémkednek az internet- és mobilfelhasználók

Mit tudnak rólad a népszerű mobilalkalmazások?

Alkalmazás	Felhasználónév/jelszó	Kontaktlista	Kor, nem	Helymeghatározó adatok	Telefon azonosító	Telefonszám
Angry Birds	☑	☑	✗	☑	☑	✗
Dictionary.com	✗	✗	✗	☑	☑	✗
Facebook	◕	◕	✗	◕	✗	✗
Foursquare	◕	✗	◕	☑	✗	◕
Google Maps	☑	✗	✗	☑	✗	✗
MyFitnessPal	◕	✗	◕	☑	☑	✗
NYTimes	✗	✗	✗	☑	☑	✗
Shazam	✗	✗	✗	☑	☑	✗
WhatsApp Messenger	✗	✗	✗	✗	✗	◕
YouTube	◕	✗	✗	✗	✗	✗
Beautiful Widgets	✗	✗	✗	☑	✗	✗
Dictionary.com	✗	✗	✗	✗	☑	✗
Facebook	◕	✗	✗	✗	✗	✗
Foursquare	◕	✗	✗	☑	✗	◕
Fruit Ninja	☑	✗	✗	✗	☑	✗
Google Maps	✗	✗	✗	◕	✗	✗
Launcher Pro	✗	✗	✗	✗	☑	✗
NYTimes	✗	✗	✗	✗	☑	✗
TweetCaster	☑	✗	✗	☑	☑	✗
YouTube	✗	✗	✗	✗	✗	✗

✗ Nem gyűjtenek adatokat ◕ Az alkalmazás fejlesztőjéhez/forgalmazójához továbbítják az adatokat
☑ Harmadik félnek is kiadják az adatokat

Megfigyel a konzol: a játékkonzolok is veszélyesek lehetnek

után: azok a cégek is gyűjtik az adatokat, amelyek eszközeit, infrastruktúráját, weboldalait és alkalmazásait használjuk. Az alkalmazásbiztonsággal foglalkozó Appthority szerint például szinte valamennyi mobilalkalmazás megfigyeli felhasználóit – különösen azok, amelyeket ingyen tölthetünk le a szoftveráruházakból.

Az Appthority App Reputation Report című tanulmánya szerint a 200 legnépszerűbb ingyenes iOS- és Android-alkalmazás 95, a fizetősöknek pedig 80 százaléka mutat „kockázatos viselkedést". A cég ilyennek tartja a földrajzi adatok nyomon követését, a felhasználók vagy a készülékek egyedi UDID-azonosítójának rögzítését, ha az alkalmazás hozzáférést kér a telefonkönyvhöz, illetve a kontaktlistához, közösségi oldalakra jelentkezik be a nevünkben, támogatja az appon belüli vásárlásokat, hirdetési hálózatokkal vagy elemzőcégekkel osztja meg adatainkat.

A vállalat szakemberei szerint az ingyenes alkalmazásoknak 70, a fizetősöknek pedig 44 százaléka nyomon követi a felhasználók mozgását. Az ingyenes appok több mint fele használ közösségi hálózatokon való bejelentkezést, azonosítja a felhasználókat, kínál alkalmazáson belüli vásárlási lehetőséget, vagy megoszt információkat a hirdetési hálózatokkal. A tanulmány készítői azt találták, hogy az ingyenes Android-alkalmazások nagyobb valószínűséggel mutatnak rizikós viselkedést, mint az iOS-esek. Az ingyenes és fizetős appokat nézve már más a helyzet: az iOS-szoftverek 91, az androidosoknak pedig 83 százaléka teszi ki veszélynek letöltőit.

Dávid Imre

Nyomtalanul a neten

Hackerek, titkosszolgálatok, marketingesek kíváncsiskodnak utánunk, valahányszor csak kimerészkedünk az internetre. Az alábbi tippek segítségével kikerülhetünk a célkeresztből.

Digitális lábnyomunk minimalizálása érdekében az első lépés, amit tehetünk, hogy áttérünk a privát böngészési mód használatára: ezt az üzemmódot minden komolyabb program támogatja. Privát üzemmódban a neten szörfölés közben összegyűjtött információkat – többek között a felkeresett webhelyek listáját, az általuk küldött sütiket, amelyekkel nyomon követhetik online tevékenységünket, valamint az űrlapokba, keresőkbe beírt adatokat – nem menti el a böngésző, így az általunk használt géphez hozzáférő más személyek nem szerezhetnek tudomást arról, hogy mely webhelyeket látogattunk meg.

Mind az Internet Explorerben, mind a Firefoxban a [Ctrl+Shift+P] billentyűkombinációval nyithatunk meg a legegyszerűbben egy új privát böngészési ablakot. Az előbbinél a címmező előtti kis kék, InPrivate feliratú címke, utóbbinál egy lila maszkot ábrázoló ikon jelzi a böngészőablak fejlécének jobb szélén, hogy ebben az üzemmódban vagyunk. Szintén érdemes még bekapcsolni a nyomon követést megakadályozni hivatott funkciót, ez az Internet Expolorerben alapértelmezés, a Firefoxban pedig az [Eszközök/Beállítások] menüparancsokkal megjeleníthető ablak [Adatvédelem] lapjának tetején lévő [Nem akarom, hogy a webhelyek kövessenek] lehetőség bejelölésével tehető meg. Ám e funkció aktiválásával a siker még nem garantált, mivel a webhelyek együttműködésére is szükségünk lesz.

Tovább növeli a privát internetezés hatásfokát, ha a Sandboxie alkalmazással együtt használjuk, ami lehetővé teszi, hogy böngészőnket – és más programokat is – a rendszertől elkülönítve futtassunk, így az semmilyen adatot nem fog tudni számítógépünkre menteni. Így nemcsak a kíváncsiskodóktól védhetjük meg magánszféránkat, hanem a rosszindulatú programoktól is.

De mi lesz a Flash sütikkel?

A privát böngészési üzemmód önmagában nem garantál anonimitást a világhálón, internetszolgáltatónk, munkáltatónk tudni fogja, hogy merre barangoltunk, és ha az adatforgalom nem volt titkosított, internetes kommunikációnk továbbra is lehallgatható marad. Ugyancsak megmaradnak a Flash multimédialejátszó program által telepített sütik. A Flashről mindenki tudja, hogy sok webes médiatartalom csak vele tekinthető meg, azt már kevesebben tudják, hogy széles körű használata miatt biztonsági rései a hackerek első számú célpontjai közé tartoznak, azt pedig még kevesebben, hogy kiválóan használható netezési szokásaink feltérképezésére, tevékenységünk nyomon követésére, mivel rejtett, soha nem lejáró sütijei a böngészők által kínált hagyományos módszerekkel nem törölhetők.

Szerencsére létezik a Firefoxhoz telepíthető Better Privacy plugin, amely lehetővé teszi a gépünkre mentett, LSO-nak (Local Shared Objectnek) is nevezett Flash-sütik kilistázását és automatizált törlését a böngésző be-

Better Privacy: eltávolíthatók vele a rejtett nyomkövető Flash-sütik

zárásakor és elindításakor vagy időzített módon. Ezek a makacs nyomkövetők a rendszerünkre vonatkozó speciális információkat tárolnak és tesznek hozzáférhetővé illetéktelenek számára engedélyünk nélkül, s nem lehet egyszerűen meghatározni, hogy melyiket használják nyomon követésre. A pluginnel manuálisan is kezelhetők a sütik, így kizárhatók az automatikus törlésből a játékbeállításokat vagy belépési adatokat tároló tételek, amelyek eltávolítása nem célszerű.

Álcázás a neten VPN-nel és Torral

Az anonimitás problémájára kínálnak hatékony megoldást a virtuális magánhálózat (VPN) szolgáltatások, amelyek havi pár ezer forintos előfizetési díjért (alkalmi, havi néhány száz megabájtos adatforgalomig terjedő használat esetén pedig ingyenesen) biztonságos böngészést kínálnak. A VPN ügyfélprogram titkosított adatforgalmú csatornát képez számítógépünk és a szolgáltató szervere között, így illetéktelenek nem tudják kideríteni, hogy milyen adatokat továbbítunk az interneten, ha például egy nyilvános Wi-Fi-hotspoton keresztül szörfölünk. Megkerülhetők vele a munkahelyi hálózatok korlátozásai is, ráadásul valós IP-címünket egy másikra cseréli fel, így a meglátogatott webhelyek nem tudják beazonosítani tartózkodási helyünket. Az igényesebb szolgáltatóknál több

Tor hálózat: a PC World kerülőúton elért weboldala Flash-reklám nélkül

tízezer „csere" IP-cím közül választhatunk számos országban, amelyek váltogatásával végképp megnehezíthetjük a nyomkövetők dolgát. A külföldre költözés olyannyira hatékony, hogy még a kizárólag helyiek számára fenntartott webes szolgáltatásokat is megtéveszthetjük vele.

Ugyancsak az IP-cím elrejtésével valósítja meg az anonimitást az eredetileg az amerikai haditengerészet elektronikus kommunikációjának védelmére kifejlesztett, nyílt forráskódú Tor hálózat (torproject.org), amelynek előre konfigurált böngészőjét előszeretettel használják a magukat veszélyben érző politikai aktivisták, menekültek, elnyomás alatt élők és hasonlók, de bárki számára ingyenesen hozzáférhető. A TorBrowserrel történő internetezéskor a forgalom a Tor hálózat véletlenszerűen kiválasztott, önkéntesek által működtetett csomópontjain halad keresztül, amelyek világszerte szétszórva találhatók. Az adatok útjuk során többszöri titkosításon mennek keresztül, míg elérik a kilépési pontot, amely a Tor hálózat utolsó számítógépe. Itt feloldják a titkosítást, és az adatokat elküldik a célszámítógépre úgy, hogy a küldő személyét nem fedik fel.

Mindegyik csomópont csak az előtte lévő és az utána következő csomópont IP-címét ismeri, így nem lehet feltérképezni a küldő számítógép és a megcélzott webhely közötti teljes adatátviteli útvonalat. Ráadásul minden megvalósult útvonal csupán tíz percig él, ennek elteltével új átjárót generálnak. Ha később meglátogatunk egy másik weboldalt, a hálózat egy új, véletlenszerűen kialakított utat fog választani. Ez megakadályozza, hogy internetszolgáltatónk vagy bárki más tudomására jusson, hogy mely webhelyeket látogatunk meg, a webhelyek üzemeltetői pedig csak a kilépési pontot megvalósító számítógép IP-címét ismerik. Előbbi láthatja, hogy egy Tor csomóponthoz kapcsolódunk, utóbbiak pedig a kilépési pontok nyilvános listájából megtudhatják, hogy a Tor hálózaton keresztül érjük el.

Az adatok „megjáratása" miatt a Tor hálózaton lassúbb a böngészés, mint egyébként. További hátrányt jelenthet, hogy a TorBrowser blokkolja a bedolgozókat – Flash, RealPlayer, QuickTime stb. –, ami rontja az internetezés élményét. Ezek manipulálásával ugyanis kideríthető valódi IP-címünk, akkor meg minek ez az egész hercehurca? Azért a YouTube-videókról nem kell feltétlenül lemondanunk, köszönhetően a videomegosztó HTML5-lejátszójának (youtube.com/html5).

Újabb probléma: böngészőnk ujjlenyomatot hagy

Ha viszont maradunk jól bevált, hagyományos böngészőnknél, feltétlenül tudnunk kell azt is, hogy szószátyár programról van szó, amely nagyon sok mindent elárul rólunk a meglátogatott webhelyeknek. *Peter Eckersley*, az Electronic Frontier Foundation (EFF) jogvédő szervezet technológiai projektigazgatója szerint hiába szabadulunk meg a közönséges és Flash-sütiktől, valamint változtatjuk meg IP-címünket, a böngészőnk által kiadott további információkkal, a böngésző úgynevezett „ujjlenyomatával" egyértelműen be-

Több tízezer „csere" IP-cím közül választhatunk számos országban

azonosíthatók lehetünk, mivel azok egyedi kombinációt alkotnak. Pletykák szerint léteznek olyan webes kutató-elemző cégek, amelyek ezeket az ujjlenyomatokat használják a felhasználók nyomon követésére.

Az EFF kutatói annak megállapítására, hogy mennyire egyediek a felhasználók böngészői, létrehozták a jelenleg is működő Panopticlick weboldalt (panopticlick.eff.org), melynek segítségével elemezték az odalátogatók böngészője által szolgáltatott adatok egy részét. (Ahhoz, hogy egyértelműen beazonosíthatók legyünk, 33 bitnyi információra van szükség. „Böngésző-ujjlenyomat nyolcféle adatból" című táblázatunkban látható, hogy a vizsgált adatok átlagosan hány bitnyi információt kínáltak.) Számos további információ is begyűjthető *Eckersley* szerint, melyek még egyértelműbbé tehetik az ujjlenyomatot. Így például megmérhető, hogy mennyi számítógépünk kvarckristályának órajel-csúszása, ami egy rendkívül egyedi, nehezen elrejthető hardverjellemző, és teljesen független a telepített szoftverektől.

Közel ötszázezer látogató adatainak elemzése után a kutatók a böngészők által nyújtott adatcsomagok közel 85 százalékát találták teljesen egyedinek. Ha pedig csak azokat a böngészőket nézték, amelyekre telepítve volt vagy a Java, vagy a Flash (ami egy tipikus konfiguráció az asztali gépek esetében), akkor az egyediségi arány 94 százalék fölé ment. És csupán az összes böngésző egy százaléka rendelkezett olyan ujjlenyomattal, ami kettőnél többször fordult elő a vizsgált mintában. Jól szerepeltek ugyanakkor a mobilos böngészők, minden bizonnyal a pluginek és betűválaszték hiánya miatt. A kutatók nem is próbálták megbecsülni statisztikai módszerekkel, hogy a viszonylag kis mintán mért eredményből milyen következtetések vonhatók le a teljes internetező népességre vonatkozóan: vajon kevésbé egyediek a felhasználók digitális lábnyomai? Azt viszont megállapították, hogy bár a böngésző-ujjlenyomatok gyakran változnak – telepítünk egy új fontot vagy plugint, upgrade-eljük a programot stb. –, kis módosulások esetén mégis nagy pontossággal megbecsülhető, hogy mi volt az előző állapot,

Panopticlick: egy böngésző-ujjlenyomat nyolcféle adatcsoportból, amely 20,11 bitnyi azonosító információt közöl

Tails OS: zsebben hordható biztonság

A Tor hálózatot használja a kifejezetten a magánszféra védelmére és anonim internetezésre kifejlesztett, Debian Linux-alapú Tails (The Amnesic Incognito Live System) operációs rendszer (tails.boum.org). Bárhol, bármely számítógépen lehetővé teszi a cenzúra és más korlátozások kikerülését, és nem hagy maga után semmilyen nyomot, csak ha szándékosan így konfiguráltuk. Egy teljes körű, önállóan használható rendszerszoftverről van szó, amit DVD-ről, USB-memóriáról vagy SD-kártyáról történő futtatásra terveztek. Nem függ a gépen lévő operációs rendszertől, és nem változtatja meg azt. Miután befejeztük a vele való munkát, a gép újraindul eredeti rendszerével. Elkerüli a merevlemez használatát, kizárólag a RAM-ot használja tárolásra, de lehetőséget nyújt az elkészített dokumentumok külső adathordozóra mentéséhez. Minden alkalmazás a Tor hálózaton keresztül kapcsolódik az internetre, s ha valamelyik megpróbálja más úton elérni a világhálót, a Tails biztonsági okokból automatikusan blokkolja a kommunikációt. A rendszert felszerelték a legújabb adattitkosító eszközökkel. A LUKS segítségével elrejthetők az USB-memóriák és a külső adathordozók, a HTTPS Everywhere kiegészítővel pedig automatikusan titkosítható a kommunikáció egy sor ismertebb webhellyel. E-mailek titkosítására és aláírására szolgál az OpenPGP, míg a fájlok biztonságos, végleges törlésére a Nautilus Wipe használható.

Hordozható rendszer: a Tailsszel bárhol nyom nélkül dolgozhatunk, netezhetünk

így továbbra is nyomon lehet követni minket.

Joggal merül fel a kérdés, hogyan védekezhetünk a böngésző ujjlenyomatának felhasználásával történő azonosítás ellen. Az EFF kutatói a leghatékonyabb védekezési módnak a JavaScript blokkolását említették – például a TorBrowser használatával vagy a Firefox esetében a NoScript bedolgozóval –, minek révén jelentősen csökkenthetjük a böngésző ujjlenyomatának egyediségét.

Netezés mindig más böngészővel

Egy másik módszer a szörfölés nyomon követésének kivédésére, ha folyamatosan, jelentős mértékben megváltoztatjuk böngészőnk ujjlenyomatát amellett, hogy igyekszünk egyediségét is csökkenteni. Erre szolgál a Random Agent Spoofer böngészőplugin a Firefoxhoz, amely fondorlatos módon meghamisított adatokat küld számítógépünkről a meglátogatott webhelyeknek. A Firefoxot használjuk, de Safarinak álcáz minket, Windows 7-et futtatunk és virtuálisan a 8.1-es változatnak hazudja rendszerünket. A program rengeteg további beállítási lehetőséget kínál a böngésző ujjlenyomatának jelentős megváltoztatására, illetve egyediségének csökkentésére. Automatikus üzemmódjában pedig véletlenszerűen váltogatja a böngésző–operációs rendszer kombinációkat.

Random Agent Spoofer: folyamatosan változtatható vele a böngésző ujjlenyomata

Ugyancsak hasznos kiegészítő a TorBrowser és a Tails által is használt, az EFF és Tor Project együttműködésében kifejlesztett HTTPS Everywhere (eff.org/https-everywhere), amely a Firefoxhoz – az androidoshoz is –, valamint béta-változatban a Chrome-hoz és az Operához érhető el. Biztonságosabbá teszi az internetezést a titkosított (HTTPS) kommunikáció bekapcsolásával. Sok webhely kínál korlátozott támogatást a HTTPS-hez, de megnehezíti ennek használatát. Például alaphelyzetben a titkosítatlan HTTP protokollt használja, vagy a titkosított oldalakon a webhely titkosítatlan részére mutató hivatkozásokat helyez el. A HTTPS Everywhere megszünteti ezeket a problémákat intelligens technológiájával, lehetővé téve a titkosítás használatát a szerkeszthető fehérlistáján lévő webhelyeken.

Így óvhatjuk meg személyes adatainkat

Digitális lábnyomunk részei a nyilvános online tevékenységünk – szakmai és közösségi oldalak látogatása, fórumokon való szereplés stb. – során magunkról publikált adatok, képek, videók is, amire szintén érdemes kiemelten odafigyelni. Általánosságban elmondható, hogy ha valamit felteszünk az internetre, az kikerül az ellenőrzésünk alól; bárki letöltheti és felhasználhatja kényekedve szerint. Igaz ez a közösségi oldalakra is, ahol bár korlátozhatjuk a hozzáférést, például egy képhez, barátainkra vagy egy szűkebb csoportra, de hogy ők mit fognak kezdeni vele, az már nem rajtunk múlik. Ha továbbítják saját ismerőseiknek, és ez többször megismétlődik, az már szinte olyan, mintha nyilvánosságra hoztuk volna.

Naprakész védelem

Miután gondoskodtunk arról, hogy minél kevesebb olyan információt hagyjunk magunk után az interneten, ami később gondot okozhat, illetve hogy online tevékenységünknek minél kevesebb nyoma maradjon számítógépünkön, ne hanyagoljuk el a helyben tárolt adatok védelmét sem. Alapkövetelmény, hogy mivel a világhálóra kapcsolódó eszközünk ki van téve a legkülönfélébb támadásoknak,

Böngésző-ujjlenyomat nyolcféle adatból

Böngészőinformáció	Azonosításra alkalmas bitek átlagos száma
User Agent (verzió, operációs rendszer)	10,0
HTTP_ACCEPT fejléc (milyen fájlformátumokat vár a böngésző a szervertől)	6,09
Telepített pluginekre vonatkozó adatok	15,4
Időzóna	3,04
Megjelenítés felbontása és színmélysége	4,83
Rendszerfontok	13,9
Engedélyezettek-e a sütik	0,353
Szupersütik (Flash-sütik)	2,12

Forrás: Electronic Frontier Foundation

Meghajtótitkosítás: egyszerűen biztonságba helyezhető az egész merevlemez a BitLockerrel

a frissítések azonnali telepítésével tartsuk naprakész állapotban operációs rendszerünket, a futtatott alkalmazásokat és ismert fejlesztőtől származó vírusellenes programunkat. Ezen túlmenően mindenképpen érdemes felkészülnünk arra, hogy minden óvintézkedés ellenére megfertőződünk, mondjuk egy titkosító vírussal, amely elérhetetlenné teszi fájljainkat, ha ellopják a laptopunkat, vagy ha hardvermeghibásodás miatt adatvesztés történik. Pótolhatatlan dokumentumaink külső meghajtóra történő rendszeres mentésével elkerülhetjük az előbbiekből eredő károkat, és a vírusmentesítés, illetve a hiba kijavítása után egyszerűen visszaállíthatjuk az eredeti állapotot.

Sok mindentől megvéd a titkosítás

Ha azt akarjuk, hogy a számítógépünk merevlemezén tárolt bizalmas dokumentumok semmilyen körülmények között ne kerülhessenek illetéktelen kezekbe, vegyük fontolóra titkosításukat egy megbízható programmal. A legkézenfekvőbb megoldásnak a Windows 7 Ultimate és Enterprise, valamint a Windows 8 Pro és Enterprise változatában megtalálható BitLocker program ígérkezik, amivel teljes meghajtókat titkosíthatunk, USB-memóriákat és külső meghajtókat is. A szolgáltatás használatához a Vezérlőpulton kattintsunk a [BitLocker meghajtótitkosítás] utasításra, a titkosítani kívánt meghajtó mellett pedig válasszuk a [BitLocker szolgáltatás bekapcsolása] lehetőséget, majd kövessük a program utasításait. Ha olyan Windows-változatot használunk, amelynek nem része a BitLocker, érdemes fontolóra venni az upgrade-et, vagy valamelyik ismert biztonsági cég titkosítómodult tartalmazó termékét választani. Ezen a területen ne sajnáljuk a pénzt, hiszen értékes információink megóvásáról van szó. A kevésbé ismert fejlesztőktől származó ingyenes, nem tanúsított szoftverek nem garantálják fájljaink biztonságát, és sok esetben csak a biztonság illúzióját jelentik. Jó példa erre a sokáig ingyenes BitLocker-alternatívaként funkcionáló TrueCrypt, ami rejtélyes gyorsasággal szűnt meg egyik pillanatról a másikra, cserbenhagyva használóit.

Használjunk digitális radírt

Még a törölt fájlok sincsenek biztonságban a kíváncsi szemek elől. Amikor ugyanis egy fájlt átadunk az enyészetnek, voltaképpen csak a számítógépes nyilvántartásból töröljük. Bitjei mindaddig hozzáférhetők lesznek egy erre specializált programmal – például a Piriformféle Recuvával –, amíg felül nem írjuk a merevlemezen azt a területet, amit elfoglalnak. Egy hasznos alkalmazás, az Eraser (eraser.heidi.ie) segít a gondon: lehetővé teszi az egyenkénti és a csoportos biztonsági

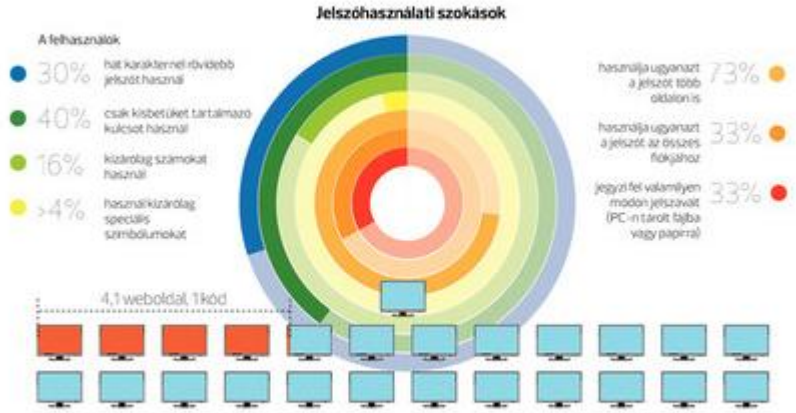
Végleges törlés: többszöri felülírással szabadul meg visszavonhatatlanul a fájloktól az Eraser

törlést, valamint az üres lemezterület felülírását. Számos törlési módszer közül választhatunk, melyek többszöri – akár 35-szöri – felülírással gondoskodnak a visszafordíthatatlan megsemmisítésről.

A felhő veszélyei

Egyre többen tárolnak adatokat a felhőben, mivel a korlátozott méretű memóriával felszerelt mobileszközöknek alapszolgáltatásává vált a gyártó által kínált felhőbe mentési lehetőség. Ráadásul a feltöltés szinkronizálás formájában gyakran automatikusan történik, aminek az lesz az eredménye, hogy olyan adatokat tárolunk majd a messze távolban, amelyeket legszívesebben nem engednénk ki az eszközünkről. Érdemes rászánni az időt, és kialakítani egy otthoni adatvédelmi politikát arra vonatkozólag, hogy mely adatokat tároljuk a felhőben, és melyeket nem, továbbá gondoskodni arról, hogy mobileszközeink ne töltsenek fel automatikusan, tudtunk nélkül fájlokat a felhőbe. Általános jó tanácsként elmondható, hogy a ránk vonatkozó leginkább bizalmas munkahelyi és személyes információkat ne bízzuk a felhőre. Gondoskodjunk továbbá a felhőszolgáltatások esetében is erős jelszóról, és amennyiben lehetséges, használjunk kétfaktoros azonosítást a belépéskor.

Mészáros Csaba



Feltörhetetlen jelszó

Rettegsz, hogy fiókjaid belépési kódjait illetéktelenek megkaparintják? A PC World segít, hogy ilyen irányú félelmeidet mindörökre elfelejtsd.

Sajnos sokan úgy gondolkodnak, hogy amint egy felületet sikeresen levédtek jelszóval, onnantól kezdve virtuális életük azon kis darabja már az idők végezetéig biztonságban lesz, és kizárólag csak ők férhetnek hozzá. Pedig ez korántsincs így. Biztonsági kulcsaink megalkotásakor hajlamosak vagyunk arra, hogy egy számunkra könnyedén fejben tartható karaktersorozatot válasszunk. Ez rögtön egy óriási biztonsági réshez vezet, hiszen így valószínűleg egy ránk jellemző (kedvenc csapat, hobbi), illetve valamilyen módon hozzánk köthető (fontos név vagy dátum) kombinációt fogunk alkotni. Ezt pedig az adattolvajok a rólunk az interneten keringő információk alapján könnyedén visszafejthetik, és azok birtokában kedvükre csemegézhetnek az általunk féltve őrzött információk között. Ha valóban olyan védelemre vágyunk, ami megdolgoztatja vagy elkedvetleníti az esetleges digitális betörőket, akkor már kicsit komolyabb szoftveres, esetleg némi hardveres segítséget is igénybe kell vennünk.

A feltörhetetlen jelszó anatómiája

- legalább 12 karakter hosszú
- nem tartalmaz hozzánk köthető, illetve rólunk bármilyen módon megszerezhető adatokat
- kis- és nagybetűket, illetve speciális karaktereket váltogatva tartalmaz
- szótárral nem támadható (nincs benne értelmes szó)
- gyakran változtatjuk
- a korábbi jelszavak és az új jelszó között nincs kapcsolat

Biztonsági intézkedések

Leginkább arra érdemes odafigyelnünk egy jelszó kiválasztásakor, hogy annak megadását ne legyen könnyű kifigyelni. Nyilvános helyen, ha csak tehetjük, kerüljük a bejelentkezéseket, és a kulcsok tárolását is felejtsük el. Vezeték nélküli hotspotok esetén érdemes mellőzni kiemelt biztonságú kódjaink használatát, ugyanis a közösen használt (legtöbbször titkosítatlan) Wi-Fi-hez csatlakoztatott számítógépekről – egy kis ügyeskedéssel – az avatott kezek azt viszik el, amit csak akarnak. Persze otthoni lokális hálózatunkon is leselkedhetnek ránk veszélyek, mégpedig a gyakran a háttérben futó keylogger alkalmazások formájában, melyek vélhetően a saját hibánkból (vírusos üzenetként vagy fertőzött adathordozón) kerülnek a számítógépre. Ezek ellen legtöbb esetben megfelelő tűzfalvédelemmel vagy a kimenő adatok blokkolásával léphetünk fel, méghozzá eredményesen. Elővigyázatosságból titkosított fájlokban tárolt jelszavaink vágólapról történő bemásolásával is feleslegessé tehetjük a leütést naplózók működését, hisz így a billentyűink figyelése hasztalanná válik.

Arra is figyeljünk, hogy kódjainkat ne tartalmazzák szótárak, vagyis az értelmes szavakat, szószerkezeteket kerüljük, ugyanis a hackerek egyik gyakran használt módszereként egy adatbázisnyi értelmes kifejezést szabadítanak rá felhasználói fiókunkra. Sokszor így minimális

munkával képesek megszerezni a kívánt adatot. Ez ellen a legjobb védekezés, ha például adott karaktereket számokra cserélünk (az e-ből 3, vagy az i-ből 1-es lesz), mert így nemcsak kódunk lesz biztonságosabb, de a szótárakat is sikeresen kijátszottuk.

Böngészőnk használatakor se feledkezzünk meg a biztonsági intézkedésekről, elektronikus üzeneteinket spamgyanú esetén ne olvassuk el, és semmi esetre se töltsünk le megbízhatatlan forrásból származó fájlokat. Ha csak tehetjük, blokkoljuk a reklámokat és a felugró ablakokat is. Az AdBlock nevű beépülővel könnyedén megszabadulhatunk a kéretlen hirdetésektől és egyben a bennük rejlő veszélyektől.

Időnként váltsunk

Jelszavainkat – főleg amiket gyakran, több gépről is használunk – bizonyos időközönként cserélgessük, hisz minél sűrűbben elvégezzük ezt a műveletet, annál kevésbé válunk kiszolgáltatottá. Ha ugyanis valaki ostromolni kezdi fiókunkat, de mi közben megváltoztatjuk a titkosítókódunkat, a hacker kezdheti elölről az addigi munkáját. És minél régebben változtattuk meg a kódot, annál több időt hagytunk neki a próbálkozásokra. Emellett, ha csak tehetjük, ne használjuk ugyanazt a jelszót több helyen, és arra mindenképp ügyeljünk, hogy a kiemelten fontos adatokat (például online bankot) védő kulcsszavak egyediek legyenek. Vagy szerezzünk be egy tokent.

Mesterjelszó: a KeePass ügyel arra, hogy ez valóban bombabiztos legyen

Arcfelismerés: a Blink! élesítésével könnyedén új szintre emelhetjük a PC-s védelmet

Persze ez óriási mennyiségű megjegyzendő kódot jelent, amit szinte lehetetlen lenne fejben tartani. Ilyenkor léphetnek képbe a jelszókezelő, illetve -generáló alkalmazások, melyek segítségével elérhetjük, hogy ne kelljen a kulcsokkal memóriánkat terhelni. Mivel a legtöbb bejelentkezési felületünk webes oldalakhoz köthető, rengeteg jelszókezelő található böngészőink beépülői között. A *LastPass* névre hallgató plugin segítségével néhány kattintással tárolhatjuk kódjainkat, illetve ugyanilyen könnyedén elő is hívhatjuk őket. Természetesen elérhető ilyen szoftver asztalról futtatható formában is, amennyiben komplett bejelentkezési adatainkat is tárolni szeretnénk. Pontosan ezt a szolgáltatást nyújtja a *KeePass*, melynek biztonsági rendszerében bátran elhelyezhetjük legféltettebb kódjainkat is. Egy password-manager program használatakor arra kell kiemelten odafigyelnünk, hogy megfelelően erős mesterjelszóval védjük le a mögé helyezett tartalmat.

Egy másik lehetséges módszer, amivel borsot törhetünk a tilosban szaglászók orra alá, hogy nemcsak megszokott karaktereinket alkalmazzuk, hanem a teljes ASCII palettát segítségül hívjuk, vagy több nyelv karakterkészletét összemixelve készítjük el a biztonsági kulcsunkat. Általánosságban ugyanis elmondható, hogy a hackerek többsége már a speciális karaktereknél is feladja, ám szinte tehetetlenné válnak, ha még ennél is nagyobb karaktertáblából kell előhalászniuk a célfiók hozzáféréséhez szükséges szimbólumokat.

Természetesen nem lehetünk képesek védekezni egy elavult (esetlegesen hibás) operációs rendszerrel, de biztonsági réseinket óriási mértékben csökkenthetjük csupán azzal, ha számítógépünk rendelkezik a legújabb frissítésekkel, különös tekintettel a védelmi feladatot ellátó programokra (tűzfal, vírusirtók) és a rendszerhez kapcsolódó szoftverekre.

Jelszó öt lépésben

A könnyen megjegyezhető, mégis megfelelően biztonságosnak tekinthető jelszó megalkotásához kövessük az alábbi lépéseket:

1. Vegyünk legalább egy tíz szót tartalmazó mondatot (vagy többet), és jegyezzük meg azt. Például: „Véletlenszerű karaktereket megjegyezni nem egyszerű. Szerencsére van rá egy jó módszerünk."
2. Az első karakterek alapján hozzuk létre kódunkat, ez példánk szerint: vkmnesvrejm
3. Helyezzük el benne a nagybetűket: VkmneSvrejm
4. Egészítsük ki számmal (írjuk bele szerencseszámunkat, vagy egyes karaktereket cseréljük számra): Vkmn3Svr3jm
5. Végül helyezzünk el benne pár speciális karaktert is (például a mondat végi írásjeleket): Vkmn3.Svr3jm.

Generált jelszavak

Jelszavaink feltöréséhez – a módszerektől függően több vagy kevesebb –

időre van szükség, ami a kódszó méretének függvényében folyamatosan nő, vagyis minél hosszabb egy belépésazonosító, annál nehezebb lesz kitalálni. A jelszó karakterszámának növelésével könnyedén kiiktathatjuk a brute force módszerrel adataink védvonalát áttörni kívánó tolvajokat. Tovább növelhetjük biztonságérzetünket, ha kódunkban kis- és nagybetűket váltakozva használunk, vagy ha számokkal, esetleg speciális karakterekkel dobjuk fel biztonsági kulcsunkat. Egy – megjegyezhető – randomizáltnak tűnő karaktersorozat megalkotása nem mindig egyszerű, de szerencsére könnyedén generáltathatunk magunknak egy ilyet, ha szükségünk van rá.

Rengeteg online és offline forrásból elérhetők e biztonságnövelő céllal létrehozott jelszógenerátor alkalmazások, tehát ha kifogytunk az ötletekből, érdemes ezeket az oldalakat felkeresnünk, és segítségükkel megalkotnunk egy megfelelően erős védelmi vonalat. Ilyen szolgáltatást kínál többek között a jelszogenerator.hu, amellyel egy webes felületen pillanatok alatt biztonsági kulcsok egész arzenálját gyárthatjuk le, mindössze annyi a dolgunk, hogy megadjuk, milyen hosszú jelszót szeretnénk, és ebből mekkora mennyiséget állítson elő nekünk az alkalmazás. Hasonló elven működik a safepasswd.com oldal is, egy csúszkával állíthatjuk be leendő kulcsunk hosszát és a használni kívánt karakterkészletet, majd a Start gombra kattintva pillanatok alatt elkészül betörőbiztos kódunk.

LastPass: mindegy, milyen böngészőt preferálunk, jelszavainkat biztonságosan eltárolja

Bár a legtöbb esetben a regisztrációs felület is méri begépelt kulcsunk erősségét, ha tisztában szeretnénk lenni védelmünk valós képességeivel, érdemes felkeresnünk a passwordmeter.com oldalt, itt a beírt jelszóról egy bonyolult, ám részletesen kifejtett értékrendszer alapján megtudhatjuk, mennyire mondható hackerbiztosnak. Annyival nyújt többet ez az oldal a beépített erősségmérőknél, hogy itt láthatjuk, milyen téren kellene fejlesztenünk a karaktersorozatot a tökéletesség eléréséhez. Ha arra is kíváncsiak vagyunk, mennyi ideig tartana feltörni kulcsunkat egy átlagos gép teljesítményével, látogassunk el a howsecureismypassword.net nevű oldalra. Az oldal üzemeltetője kiemelten felhívja arra is a figyelmet, hogy milyen könnyen képesek az ilyen weboldalak ellopni jelszavainkat, ezért legyünk körültekintőek, és még egy látszólag ártalmatlan oldalon se adjuk ki titkainkat.

Alternatív megoldások

Kellően biztonságos megoldásnak tekinthető a gesztusokon alapuló azonosítás. Ezt a megoldást alkalmazzák már elég régóta az okostelefonok érintőképernyőin, melyeket kívánság szerint ábrákat rajzolgatva oldhatunk fel. Az ötletben rengeteg cég meglátta a lehetőséget, és sorra érkeznek az asztali gépekre is elérhető „rajzolós" jelszavak. Egy bonyolultabb ábra ez

Azonnali feltörés: a „password" szó nem a legjobb választás

esetben is nagyban nehezíti az átjutást, sőt itt egy megfelelően beállított mozdulatsorokat követő rajzocska szinte feltörhetetlenné teszi a mögé rejtett adatokat. A Windows 8-ban fellelhető, ilyen alapokon nyugvó zárolási képernyő magas szintű biztonságot kínál, hiszen az ábraalapú képjelszó majdhogynem lehetetlenné teszi a bejutást az illetéktelenek számára, illetve kiküszöböli az „1234" egyszerűségű kulcsok használatát. E beépített funkciót a Gépház megnyitásával érhetjük el, ahol is a [Felhasználók] menüpont alatt a [Képjelszó létrehozása] opciót kiválasztva már ki is jelölhetjük a jelszóként használni kívánt fotót. Ezután mindössze annyi a teendőnk, hogy ezen a felületen az egér (vagy érintőképernyő esetén ujjunk) segítségével pontokat kötünk össze, és már kész is a képjelszavunk.

Webkameránkon keresztüli arcfelismeréssel is próbálkozhatunk,

ehhez kínál szoftvert a holland Luxand cég Blink! névre keresztelt alkalmazása, ami a beállítása során több szögből is memorizálja felhasználója arcát, és a bejelentkezési képernyőn túl nem is enged be mást, mint jogos tulajdonosát. Sőt a loginkísérletekről fotók is készülnek, melyek naplózásra kerülnek, így az előzményeket böngészve könnyedén kiderül, ki próbált meg belépni gépünkre. Kipróbálásra mindenképp jó lehet, az első húsz bejelentkezésig ugyanis ingyenes a szoftver. Ha megtetszik a program, a Pro változatra frissítve még több lehetőséget kapunk, egyetlen Windows-fiókhoz több aktiválásra alkalmas felhasználót is hozzárendelhetünk.

Sajnos ezek a módszerek még nem igazán kiforrottak a teljesen biztonságos azonosításhoz, így általában külön jelszóval is le kell védenünk a fiókot arra az esetre, ha valamiért mégsem működne arcunk felismerése, vagy elfelejtenénk rajzunkat.

Mit hoz a jövő?

Szépen lassan eljutunk oda, hogy a személyes jelszó valóban olyannyira egyénre szabott lesz, hogy adataink eléréséhez saját magunkat fogjuk kulcsként használni. A biometrikus azonosítás – hála az Apple ujjlenyomat-érzékelőjének – ismét központi témává vált. Valóban jó megoldás lehet az ujjbegyünk vagy a retinánk alapján azonosítani magunkat, hiszen ez egyénenként eltérő és egyedi azonosítót jelent, azonban mint azt láthattuk, a feltörhetetlennek beállított Apple-szabadalmat is sikerült néhány ravasz trükkel kijátszani.

A biometrikus azonosítók egymással kombinálása valóban elhozhatja a szóban forgó feltörhetetlen jelszót, hiszen egy ilyen, több lépcsőből álló azonosítási procedúrához már a kulcsot birtokló személy elrablására

Jelszógenerálás: hacker legyen a talpán, aki egy ilyen kódsorozatot visszafejt

Ujjlenyomat-olvasó: kikerülhetetlennek tartották, a rafinált hackereknek mégis csak pár napba telt átverni

lenne szükség. A fentieknél radikálisabb megoldásokról is szó esik néha, ilyenek a bőr alá ültetett, azonosításra szolgáló eszközök, a kapszulaként a szervezetünkbe juttatható mikrochip formájában adatot tároló, lenyelhető jelszavak, vagy a tetováláshoz hasonló, azonosításra szolgáló jelek. Persze e módszerek és a biometrikai azonosítók is gyerekcipőben járnak még, de ha az ötletek igazán kiforrnak, valóban zökkenőmentesebb és gördülékenyebb lesz az azonosítás, és feltörhetetlen jelszavaink kulcsává saját testünk válik. Amíg azonban ez nem következik be, érdemes kellően körültekintően megválasztanunk biztonsági kulcsainkat, hogy az illetéktelenek semmi esetre se juthassanak hozzájuk.

Biztonságtechnológiával foglalkozó szakemberektől még bizonyára hallani fogjuk párszor, hogy feltörhetetlen jelszó márpedig nem létezik, ám az elméletileg feltörhetetlennek nyilvánított karaktersorozat már könnyedén meggátolja az illetéktelenek hozzáférését olyan információkhoz, amiket nem szeretnénk kiadni. A védelmi technológiák fejlődése következtében pedig lassacskán eljutunk arra a szintre, hogy amit elrejtünk, azt akaratunkon kívül senki sem fogja felfedni.

Lukács Richárd

Állítsuk meg a levélszemetet

Levelezz akár hagyományos levelező klienssel vagy a közösségi oldalakon, a spammerek megtalálnak. Trükkjeinkkel kicselezheted őket.

Világháló nélkül szinte már elképzelni sem tudjuk életünket, és ehhez még netfüggőnek sem kell lenni. Többségünk számára a napilapok helyett az internet vált a legfontosabb információforrássá, időérzékünket elvesztve szabad óráinkat – látszólag másodpercek alatt – jobb esetben tartalmas webhelyek böngészésével ütjük el. Sajnos az aktív internethasználat velejárója, hogy rendszeresen meg kell adnunk e-mail címünket, hiszen a webes szolgáltatások vagy éppen a kereskedelmi tevékenységet végző portálok működési sajátosságaiból fakadóan muszáj egyénileg azonosítanunk magunkat. Ezzel önmagában semmilyen probléma sincs, azonban a legtöbb postafiók néhány hónappal a létrehozása után a káosz és anarchia bemutatótermévé válik: szükségtelen értesítések, kihagyhatatlan ajánlatok és klasszikus spamek garmada maga alá temeti fontos és érdekes leveleinket.

Túláradó szemét

A Kaspersky Lab jelentése szerint 2013 második negyedévében a világ összes elektronikus üzenetének durván 71 százaléka volt spam, illetve a kártékony e-mailek 2,3 százaléka tartalmazott valamilyen veszedelmes csatolmányt. Szezonok és rendfenntartói intézkedések függvényében jelentős – akár tíz százalékon felüli – tud lenni a fluktuáció, ám mindkét fenti érték körülbelül „normálisnak" tekinthető.

A netezők jelentős tábora esetében rendkívül kellemetlen mértékű a levélszemét mennyisége, szerencsére a népszerű e-mail szolgáltatók manapság hatékonynak nevezhető automatikus szűrést nyújtanak, kevés tradicionális tömeglevél érkezik a beérkező üzenetek mappába. A problémát egyre inkább a legális szolgáltatások jelentik: elárasztják postafiókunkat üzenetekkel, továbbá kiadhatják az e-mail címünket különféle hirdetőcégeknek.

Megelőzés

Természetesen az adatok átadásának lehetősége benne van a szerződési feltételekben, ám azt kevesen olvassák át. A Polgári Törvénykönyv szerint bármikor vissza lehet vonni az adatkezelési jogot, ám ha erre nincs valamiféle „gépesített" lehetőség, akkor egyénileg kell felvenni a kapcsolatot a reklámcégekkel, ami nem hatékony. A levélszemét csökkentésének három fontos sarokköve van, az egyszerűbbekkel kezdve, egyrészt muszáj elolvasni az ÁSZF-et (vagy legalább a releváns részét), hogy kiszúrhassuk a rosszindulatú szolgáltatásokat. Másrészt óvakodni kell az olyan portáloktól, amelyek bármely internetező számára megmutatják e-mail címünket, hiszen így azokat a spamküldők is láthatják. Példaként egyes fórumok publikus profiloldalai hozhatók fel.

Eldobható e-mail címek

Ha nem akarunk elsődleges és másodlagos e-mail fiókokkal veszódni, megoldást nyújthat az eldobható e-mail címeket adó szolgáltatások használata (például 10minutemail.com és getairmail.com). Ezek lényege, hogy generáltathatunk magunknak egy működőképes címet, amit meg tudunk adni a portálokon történő regisztrációkor. A bejövő leveleket szolgáltatásonként eltérő ideig őrzik meg, azaz lehetőség van a portálok által kiküldött levelekben található linken megerősíteni a regisztrációt. Egyes szolgáltatásokkal levelek küldése is megoldható, noha az így eleresztett üzenetek jó eséllyel maguk is automatikusan a címzett spammappájában landolnak.
Természetesen hátránya is akad az efféle szolgáltatásoknak. A fiókunkba történő bejelentkezés pusztán a kapott e-mail cím megadásával történik, így annak ismeretében bárki elolvashatja bejövő leveleinket, ám mindenképp érdemes megemlíteni, hogy az eldobható fiókok esetében alapvetően nyitott a felhasználási kultúra. Aki nem szeretné, hogy esetleg mások kotorásszanak a spamjei között, az inkább regisztráljon magának egy hagyományos másodlagos fiókot. Érdemes megemlíteni, hogy a legtöbb szolgáltatás esetében titkosítatlan az adatátvitel a felhasználó böngészője és a levelezőszerver közt.

A harmadik rendkívül fontos sarokkő a több levelezőfiók használata. Sajnálatos módon vannak olyan weboldalak, amelyek jó ízlésre és törvényi keretekre fittyet hányva egyszerűen eladják adatainkat bármely fizetőképes személynek, ezek után pedig özönleni kezdenek a hagyományos spamek. A megbízható weboldalakra regisztrálás esetén érdemes az elsődlegesnek tartott e-mail címünket használni, míg minden egyébhez másodlagos fiókot szükséges készíteni.

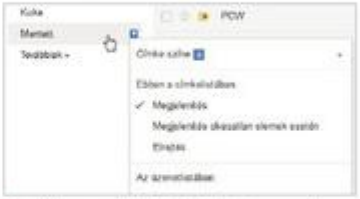
Ez talán nem a legkényelmesebb megoldás, ám különösebben macerásnak sem mondható, lévén a kettes levelezőrendszerben szinte biztosan be lehet állítani, hogy a bejövő leveleket automatikusan elsődleges címünkre továbbítsa a rendszer. A felállás előnye, hogy a nyilvánvaló spameket előszűri a másodlagos fiók szolgáltatója, a maradékot pedig manuálisan is meg lehet jelölni hulladékként, így a spam döntő többségén kívül jó eséllyel semmiről sem fogunk lemaradni. E rövid bevezető után nézzük, hogyan szortírozzuk a maradékot, miképp csendesíthetjük le a kikerülhetetlen szolgáltatásokat.

Szűrés levelezőrendszerek alapján

Gmail

Alapértelmezett beállítások mellett a korábbitól eltérően a beérkező levelek már nem listaszerűen vannak felsorolva a Gmailben, hanem tematika alapján automatikusan négy fülbe próbálja sorolni őket a rendszer. Ez már önmagában rengeteget segít a zsúfolt beérkező levelek mappán; a rendszer tévedései „fogd és vidd" módszerrel korrigálhatóak, csak rá kell húzni az elkallódott leveleket a megfelelő fülre. A hagyományos bejövő levelek mappára áhítozók kikapcsolhatják az újfajta rendezést, ehhez a fülek mellett jobbra lévő + jelre kell kattintani, majd a megjelenő felületen minden elől kiszedni a pipát.

A manuálisan rendezkedni szeretők számára érdekes témára rátérve a Gmailben alapvetően négyféle módon csoportosíthatjuk az információkat: csillagozással, fontosnak jelöléssel, címkézéssel és szűréssel. Az első kettő hasonló, ám csillagozni manuálisan lehet, míg a fontosnak jelölést a Gmail statisztikai alapon próbálja megoldani. A baloldali oldalsávból elérhető címkék segítségével kategóriákba, azokon belül pedig alkategóriákba rendezhetők a különféle levelek. Ezek közt is lehet húzogatással rendezkedni, plusz az IMAP-on mappaként is megjeleníthetők a címkék. A lehetőség az oldalsáv és [Fogaskerék ikon], [Beállítások], [Címkék] lapon szabható testre.



Gmail: a megfelelő címkézés a rend kulcsa

Gmail: automata szűrőkkel nem kell rendőr a forgalomirányításhoz

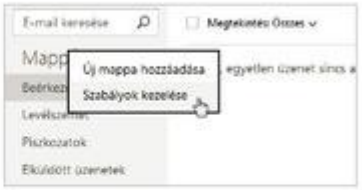
A Gmail igazi sztárja ettől függetlenül a [Fogaskerék ikon], [Beállítások], [Szűrők] helyen vezérelhető szűrési funkcionalitás. Segítségével többek közt feladó, tárgy és tartalmazott szavak alapján nemcsak összetett keresést lehet végrehajtani, hanem végleges filterek is létrehozhatók, például: egy bizonyos kifejezést tartalmazó, csatolmánnyal érkező levelek automatikusan kapjanak meghatározott címkét, továbbá legyenek megcsillagozva.

Outlook.com

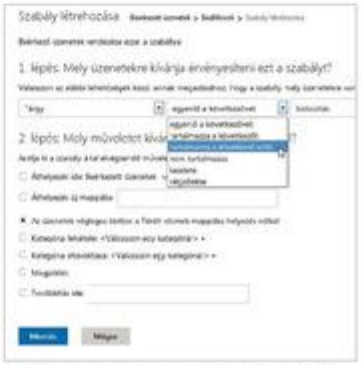
A Hotmail utódjával a Microsoftnak sikerült egy rendkívül letisztult és jól használható levelezőt létrehoznia. Első pillantásra az Outlook.com szortírozás szempontjából nem tűnik túlságosan sokrétűnek, ám ez csalóka, ugyanis lehetőség van mappák és kategóriák létrehozására. A kettő közti különbséget az képezi, hogy a mappák a Gmail címkéihez hasonlóan a levelek konkrét áthelyezésére használhatók, míg a kategóriák bizonyos paraméterek alapján csak csemegéznek az összes mappa tartalmából.

A legegyszerűbb rendezési módszer egy új mappa létrehozása a bal oldali sávon: csak rá kell kattintani az [Új mappa] feliratra, majd elnevezni azt. Innentől kezdve a meglévő mappákból fogd és vidd módszerrel áthúzhatók a levelek. A kategória készítése ugyanez, csupán a bal oldali hasáb Gyorsnézetek szövege alatti „Új kategória" feliratot kell kiválasztani.

Az előkészületek elvégzése után már csak életet kell csiholni a gépezetbe: a jobb egérgombbal kattintsunk a Mappák vagy Gyorsnézetek feliratra, majd ott válasszuk a [Szabályok kezelése] menüpontot. A megjelent oldalon az [Új] gombra kell klikkelni, ezen a felületen lehet létrehozni a szűrési szabályokat. Szerencsére a Gmailhez hasonlóan több szűrési paramétert adhatunk meg az Outlook felületén is ([...], majd [Szabály létrehozása]): ha a feladó nevében benne van egy kifejezés; ha a tárgy nem végződik a precízen megadott mintával; esetleg ha a másolatot kap mezőben benne van X, akkor történjen ez vagy az. A lehetséges tevékenységek közt megtalálható a mappákba vagy kategóriákba helyezés, az azonnali továbbítás, a fontosnak jelölés, továbbá a végleges törlés.



Outlook: a jobbklikkes menükkel gyorsabb a funkciók elérése



Outlook: csak egyszerű szabályokkal uralható a játszótér

Freemail

Az őshonos szolgáltatás megjelenésre kevésbé trendibb a Gmailnél és Outlook.com-nál, azonban a levelek szortírozása szempontjából nagy koponya. A szükséges beállítási lehetőségeket tartalmazó almenük a bal szélső oldalsáv Beállítások feliratára kattintva érhetők el. Riválisaihoz hasonlóan a [Mappáim] almenüt kiválasztva a Freemailben is létre lehet hozni egyéni mappákat, ám fogd és vidd módszerrel nem húzogathatjuk az elemeket közöttük. Ehelyett régimódi megoldással a mappákba belépve, a leveleket egyenként vagy csoportosan az erre szolgáló menüponttal lehet áthelyezni.

A filterezés a [Szűrők] almenüben állítható. Ide belépve első körben ki kell választani, hogy egyszerű vagy haladó módot szeretnénk-e igénybe venni: előbbi az egyetlen paraméternek köszönhetően könnyű használatot tesz lehetővé, míg utóbbival rafinált feltételrendszerek hozhatók létre. Haladó módban nemcsak szimplán több paramétert lehet megadni, de ezek közt logikai kapcsolatok is létrehozhatók: például a levél kerüljön egy meghatározott mappába, amennyiben X a feladója, de a mérete kisebb Y kilobájtnál. Haladó módban ezen felül sorrendet is fel lehet állítani az egymástól teljesen független szűrők közt, az egyik teljesülése pedig akár meg is szakíthatja az utána következők lefutását.

Freemail: mappákba szortírozhatók a bejövő levelek

Freemail: meglepően komplex szabályok hozhatók létre

A konkurenciától eltérően a Freemailben lehetőség van SMS-t kérni a beérkező levelekről, ráadásul ezt szűrőhöz is lehet kötni, azaz csak akkor jelezzen a telefon, ha a bejövő levél megfelel bizonyos kritériumoknak. Sajnos az árak után hajtóvadászatot kell indítani (emelt díjas SMS-ben tíz darab értesítés 400 forint + áfa), a tájékoztatási fegyelem hiánya rendkívül negatív benyomást kelthet az érdeklődőkben.

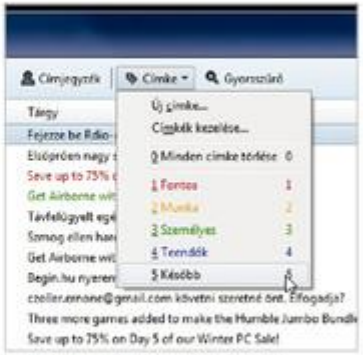
Mozilla Thunderbird

Összeállításunk mondhatni kakukktojása az ingyenes, nyílt forráskódú és multiplatform Thunderbird levelezőkliens. A programmal foglalkozni kell, hiszen sokan nem szeretnek rendszeresen bajlódni a webmailfiókjukba történő bejelentkezéssel, vagy éppen több aktívan használt e-mail cím birtokában szeretnék az összeset egy helyről kezelni.

A Thunderbird számos módot ad a levelek rendezésére és szortírozására: a legegyszerűbbel kezdve a mappákban a leveleket felsoroló terület címsorában kattintgatva többek közt feladó és dátum szerint rendeztethetők az elemek. Ugyanezen sor legelején kapcsolható be a szálas beszélgetési elrendezés, amely esetében csoportokba rendezve, lépcsőzetes vizuális jelöléssel egymás alá kerülnek a másokkal történt üzenetváltásaink. A menüsor [Címkék] lehetőségével praktikusan színkódokkal különböztethetők meg a levelek.

Az egyes postafiókokon belül új mappák is készíthetők, ám ha a levelezőszerver IMAP helyett a régimódi POP3 protokollal van bekötve, akkor a manuálisan létrehozott könyvtárak nem lesznek visszaszinkronizálva a szerverre, csak a saját számítógépen léteznek majd. A mappák közt fogd és vidd módszerrel rendezhetők a levelek.

A Thunderbird rendelkezik egy első pillantásra is feltűnő keresőmezővel, nem szabad szavas kutakodáshoz a menüsor [Gyorsszűrő] lehetőségét kell igénybe venni. Erre kattintva a leveleket felsoroló ablakrész tetején megjelenik egy kisebb menüsor: a rajta található gombokkal megoldható, hogy például csak a csillagozott, olvasatlan vagy bizonyos címkével ellátott levelek jelenjenek meg, ráadásul a kezes eszköztáron lévő lehetőségeket kombinálni is lehet.



Thunderbird: színes címkékkel egyszerűbb a tematizálás

Thunderbird: a Gyorsszűrővel sokféle paraméter alapján kereshetünk

Értesítések megzabolázása

Facebook

Mark Zuckerberg többek közt hazánkban is piacvezető közösségi hálója nagyon sokáig rengeteg levelet küldött ki a felhasználóknak, azonban jó egy évvel ezelőtt ez teljesen megváltozott, alapértelmezett beállítások mellett csak a rendkívül fontos eseményekről – például ha valaki ismerősnek jelöl – kapunk e-mailt. A változtatás „spammelési" szempontból pozitívnak mondható, ám cserébe sűrűbben kell bejelentkezni a szolgáltatásba, ha nem akarunk lemaradni a kevésbé érdekes történésekről; a módosítás mögötti szándékról mindenkinek meglehet a maga véleménye.

A túlságosan sok vagy kevés értesítés egyaránt kúrálható: a Facebookra bejelentkezve kattintsunk a kijelentkezés lehetőségét is tartalmazó leugró menüre, ott válasszuk a [Beállítások] opciót, a megjelenő lap bal oldali hasábjában pedig az [Értesítések] lehetőséget. A „Hogyan kapsz értesítéseket?" szekcióban az e-mail sorra kell klikkelni, ahol elfogadható keretek közt testreszabható, hogy miről kapjunk a jövőben értesítést.

Google+ és YouTube

Az átlagos felhasználók körében a YouTube nem tartozik a legrosszabb hírű spammelők közé, ráadásul a felhasználói profilok lényegében már beleolvadtak a Google+ rendszerbe, amelynek a baloldali oldalsávon elérhető [Beállítások] menüpontjában kezelhetjük a közösségi oldallal és a videomegosztóval kapcsolatos értesítési beállítást. Ettől függetlenül érdemes átnézni a YouTube saját értesítési opcióit is: jelentkezzünk be, kattintsunk a jobb oldalon látható profilképünkre, majd a fogaskerék ikonra.

A megjelenő oldalon számunkra jelen esetben az [E-mail] gyűjtőelem a fontos. A felületen tisztességes meny-

Facebook: egy éve már sokkal kevesebb értesítést küld

YouTube: a lap alján kikapcsolható az e-mailek küldése

nyiségű beállítás található: kapjunk-e értesítést, ha új csatornákra iratkozunk fel, ha más iratkozik fel a miénkre, amennyiben egy élő esemény kezdődik, vagy éppen befejeződött videónk feltöltése. A többség számára a lap alján található hírleveles részleg a fontos, itt kapcsolható ki az összes automatikusan generált e-mail kiküldése, sőt: legalul egy kattintással a lehető legteljesebb mértékben letiltható az értesítések kiküldése.

Twitter

Cikkünk közösségi oldalai közül az egyik legnagyobb szemetelő a Twitter, ezek szerint 140 karakteres dobozkákban mégsem fér el minden. Viszont jó hír, hogy a már tőzsdén is jegyzett szolgáltatás esetében egyetlen perc időráfordítással véget lehet vetni a spammelésnek; bejelentkezés után kattintsunk a felső fogaskerekes ikonra, a leugró menüben válasszuk a [Beállítások] opciót, azon belül pedig az [E-mail értesítések]-et.

A megjelent oldalon vérmérséklet és igény szerint alapos pusztítást lehet végezni a levelekben történő kommunikáció témakörében, köszönhetően a zseniális opciók nagy számának. A többség valószínűleg nem kér e-mailt arról, ha küldött valaki másnak egy privát üzenetet, retweetelik a retweetjeit, kedvencként jelölik a csiripeléseit, vagy éppen az őt megemlítő tweeteket. Néhány furcsa opciónak egyébként van értelme, csak épp az átlagos felhasználók helyett a híres személyek vagy márkák online jelenlétét intéző marketingesek számára lettek kitalálva.

LinkedIn

A Twitterhez hasonlóan a LinkedIn is a nagyobb mennyiségű e-mailes értesítést kiküldők közé tartozik, aminek egyik oka vélhetően felhasználóik komoly levélfüggősége (a szolgáltatás egyik mániája, hogy címlistáinkért könyörög), másrészt pedig a portál relatíve – például a

Twitter: sok a kikapcsolandó értesítés, de legalább szórakoztatók az opciók

Pinterest: a hasáb tetején kikapcsolható minden értesítés küldése

LinkedIn: van munkája az értesítésekből nem kérőknek

Facebookhoz mérten – kis felhasználói bázisa. A regisztrálókat szakmájukra alapozva összekötni kívánó szolgáltatás lassan hazánkban is terjed, éppen ezért is közérdekű információ, hogy miként lehet csökkenteni spammelését.

A bejelentkezés után vigyük az egérmutatót a jobb felső sarokban lévő profilképünk felé, ott válasszuk a [Privacy & Settings] lehetőséget, majd látogassunk el a [Communications] csoportba. Itt számos lehetőséget találhatunk, amelyekkel precízen beállítgatható a személyektől és csoportoktól kapott vagy bármely egyéb aktivitás miatt kiküldött levelek mennyisége. Külön említést érdemel a [Turn on/off partner InMail] lehetőség, ugyanis itt lehet kikapcsolni a cégektől származó fizetett tartalmak postázását.

Pinterest

A szolgáltatás az utóbbi évek egyik legérdekesebb közösségi hálós kezdeményezése, lévén teljes mértékben fotók megosztására és rendezésére fókuszál. Érdekesség, hogy kimondottan hölgyeknek tervezték, egy ideig férfiak hivatalosan nem is regisztrálhattak, amelynek következtében csak még több hímnemű volt kíváncsi rá. Ez teljesen érthető, hiszen az ilyen helyek tanulmányozásával képet lehet alkotni az ellenkező nem pszichológiájáról.

A Pinterest egy efféle weboldaltól elfogadható mennyiségű levelet küld ki, ám sok és aktív ismerős mellett gyorsan elegünk lehet értesítéseiből. A levelek számának csökkentéséhez kattintsunk felhasználói nevünkre, majd a menüben válasszuk ki a [Settings] lehetőséget. Az [Email Notifications] blokk első lehetőségével rögtön kikapcsolható mindennemű levélküldés, míg a kevésbé drasztikus megoldások hívei testreszabhatják alatta, hogy pontosan mikor kérnek értesítést.

Wiezner István

Ne engedjünk a zsaroló vírusoknak!

Félrevezetéssel, megfélemlítéssel, gépünk és személyes állományaink hozzáférhetetlenné tételével próbálnak meg pénzt kierőszakolni a zsarolóprogramok, amelyek ellen a megelőzés a legjobb védekezés.

A hétköznapi programkártevők köszönik, jól vannak, és egyre gátlástalanabb formában támadják a céges és otthoni számítógépeket. A leginkább veszélyesek közé tartoznak az ismét virágkorukat élő zsaroló (ransomware) programok, amelyek egyik legrettegettebbje, a tavaly több mint 250 ezer gépet megfertőző CryptoLocker új, kártékonyabb változattal jelentkezett. Testvéréhez hasonlóan a CryptoDefense is szöveges fájlokat, Office és PDF dokumentumokat, képeket, videókat vesz célba, erős, 2048 bites RSA-kulccsal titkosítja őket, majd váltságdíjat követel a kétségbeesett felhasználótól – aki nagy valószínűséggel akkor sem kapja meg a bűnözőktől a pótolhatatlan állományai eléréséhez szükséges kulcsot, ha fizet.

CryptoLocker: ettől az üzenettől mentsen meg minket a sors

Ijesztgetők, megfélemlítők, titkosítók

Ellenségünknek sem kívánhatjuk, hogy ransomware-rel fertőződjön meg, szerencsére a zsaroló vírusok többsége fájljaink elvesztése nélkül is eltávolítható a számítógépről. A gonosz programkártevők egy része ugyanis csupán ijesztgeti áldozatait. E scareware programok jellemzően antivírusprogramnak vagy optimalizáló segédprogramnak adják ki magukat, és folyton-folyvást megjelenő, rövid időn belül az agyunkra menő felugró üzenetekkel bombáznak minket. Ezekben azt állítják, fertőzést vagy a működést lassító beállítási problémákat találtak a gépünkön, és pénzt kérnek azért, hogy megszüntessék a fertőzést, illetve kijavítsák a hibákat. Valójában persze kizárólag ők maguk jelentik a problémát. Súlyosabb esetekben mondandójuknak alátámasztására megakadályozzák, hogy futtathassuk programjainkat.

Még nagyobb kellemetlenségekkel jár, ha a szakirodalomban policeware-nek nevezett zsaroló-programot szedünk össze. Ez blokkolja a PC-nket, teljesen használhatatlanná téve azt, és a Windows elindítása után egy teljes képernyős üzenetben a rendőrség vagy más hatóság nevében közli velünk, hogy szerzői és kapcsolódó jogokat sértettünk meg, vagy például gyermekpornó tartalmakat tárolunk, ami komoly következményekkel jár. Az illetékes hatóságok emblémájával megtámogatott üzenet szerint ezért több éves börtönbüntetést szabhatnak ki ránk, ami alól mentesülhetünk, ha most megfizetünk egy pár tízezer forintos összeget. A zsaroló üzeneteket a kiberbűnözők lokalizálják, a helyi hatóságok logóit teszik bele, és helyi nyelven szólítják meg potenciális áldozataikat. Magyarországra is eljutott már ez a veszélyes fenyegetés, szerencsére a külföldi hackerek magyartudása messze van a tökéletestől, így csak a nagyon beijedtek hihették, hogy az üzenetet valóban a magyar a hatóságok küldték. Márpedig a policeware fő fegyvere a megfélemlítés, hiszen a meglengetett büntetés súlyától, valamint a megszégyenüléstől – mi lesz, ha a családom, a főnököm megtudja, hogy pornót nézegetek a számítógépemen – való félelem sokakat késztethet a

Zsarolóprogramok

Típusok	Így működnek	Ismertebb kártevők	Védekezés, megelőzés
Álantivírus (scareware)	Üzenetekkel bombáznak, azt állítják, hogy a gép fertőzött. Pénzt kérnek az irtást elvégző teljes verzióért	Antivirus Security Pro 2014, Windows Defence Unit, Futurro Antivirus	Naprakészen tartott antivírusprogram, biztonságtudatos viselkedés
Policeware	Blokkolják a géphasználatot, hatóságok nevében pénzt követelnek, hogy áldozatuk megússza a feltételezett bűncselekmény miatti komoly felelősségrevonást	IcePol (Reveton), Ukash, Moneypak	Naprakészen tartott antivírusprogram, biztonságtudatos viselkedés
Titkosító	Erős kulccsal titkosítják a személyes állományokat, a kulcsért pénzt követelnek	CryptoLocker, CryptoDefense, PowerLocker	Naprakészen tartott antivírusprogram, rendszeres mentés külső adathordozóra

váltságdíj megfizetésére. Sajnálatos módon már tragédiához is vezetett a kiberbűnözők gátlástalansága: egy román férfi annyira komolyan vette a fenyegetést, hogy előbb kisgyermekével, majd magával is végzett, mivel a zsaroló vírus által kért szokatlanul magas, ötmillió forint körüli összeget nem tudta kifizetni, a börtönt pedig – mint búcsúlevelében írta – nem lenne képes elviselni.

A zsaroló programok csúcsragadozói, a CryptoLocker és társai, miután megfertőzték a számítógépet, a háttérben szisztematikusan titkosítják a személyes fájlokat. Mikor végeztek, az eredeti fájlokat törlik, és egy üzenetet jelenítenek meg arról, hogy fájljainkat zárolták, s ennek feloldásáért pénzt – általában néhány tízezer forintot – követelnek. A fizetést Bitcoinban kérik, mivel a virtuális valuta útja nem követhető nyomon. A fizetési határidő túllépésekor – mint például a parkolási bírságnál – az összeg megemelkedik. Ha pedig nem fizetünk, a bűnözők a titkosítási kulcs megsemmisítésével fenyegetőznek, amikor is aztán végleg búcsút mondhatunk személyes állományainknak.

Védekezés és megelőzés

Zsaroló programot – mint minden más kártevőt – leggyakrabban PDF vagy más veszélytelen állománynak álcázott levélmelléklet megnyitásával vagy ismeretlen forrásból származó hivatkozásokra való kattintással szedhetünk össze, bánjunk hát ezekkel körültekintően. Ugyancsak terjesztik őket fájlmegosztókon, azonnali üzenetekben. Az ismertebb antivírusprogramok felismerik őket, és megakadályozzák a fertőzést. A hatékony védekezés része továbbá a fontos fájlok rendszeres biztonsági mentése egy online szolgáltatásra vagy külső tárolóeszközre, így egy esetleges megfertőződés esetén egyszerűen visszaállíthatjuk őket. De vigyázzunk, a CryptoLocker legújabb változata képes a külső meghajtókon a backup fájlokat is titkosítani, így ügyeljünk arra, hogy a mentéshez használt eszköz ne csatlakozzon állandóan a gépünkhöz. Jó megoldás az is, ha a mentéseket csak olvasható optikai lemezekre készítjük.

Eltávolítás és helyreállítás

Ha mégis megtörtént a fertőzés, először távolítsuk el gépünkről a programkártevőt. Ijesztgető álantivírusok esetében indítsuk el a Windowst csökkentett módban, majd egy víruskeresővel kutassuk fel és írtsuk ki a zaklatót. Ha a zsarolóprogram megakadályozza a Windows elindítását vagy a programok futtatását, a rendszer-visszaállítás funkcióval helyezzük vissza az operációs rendszert egy korábbi, működésképes állapotába. Ilyenkor a rendszerállományok helyreállítása történik, személyes fájljainkat nem érinti a beavatkozás. A számítógép bekapcsolása után tartsuk lenyomva az

Álantivírus: ez az élősködő megszólalásig hasonlít egy igazira

[F8] billentyűt még a Windows emblléma megjelenése előtt, a [Speciális rendszerindítási beállítások] képernyőn válasszuk a [Számítógép javítása] menüpontot, majd nyomjuk le az [Entert]. Jelöljük ki a megfelelő billentyűzetkiosztást, majd kattintsunk a [Tovább] gombra, és a [Rendszer-helyreállítási beállítások] menüben válasszuk a [Rendszer-visszaállítás] lehetőséget. Ha a rendszer-helyreállítási beállítások menü ily módon nem érhető el, a Windows telepítőlemezét használhatjuk a rendszer-visszaállító eszköz eléréséhez.

Ha a rendszer-visszaállítás nem vezet eredményre, és továbbra sem tudjuk elindítani a Windowst a kártevő eltávolításához, egy bootolható lemezről vagy USB-meghajtóról futtassunk le víruskeresést/-eltávolítást. Abban a ritka esetben, ha ez sem oldja meg a problémát, végső megoldásként jöhet szóba a gyári állapot visszaállítása.

A legveszélyesebb CryptoLocker-variánsokat illetően az eltávolítás a legkönnyebb feladat, ami az igazi gondot okozza, az a titkosított fájlok visszaszerzése. Ha a ransomware nem végzett titkosítást, csupán elrejtett ikonokat vagy fájlokat, kapcsoljuk be a rejtett fájlok megjelenítését, és ha előkerülnek az elveszett dolgok, jól jöttünk ki a problémából. Ha azonban történt titkosítás, sajnos szinte semmi esélyünk sincs annak feloldására, mivel a titkosítókulcsot a bűnözők saját szerverükön tárolják. A váltságdíj kifizetése a statisztikák szerint csak igen ritka esetben hoz megoldást, ezért a biztonsági cégek ezt egyáltalán nem javasolják. Ha elővigyázatosak voltunk, és van mentésünk, amelyhez a CryptoLocker nem fért hozzá, biztos, ami biztos, futtassunk le ezen egy vírusellenőrzést, majd állítsuk vissza a fájlokat a ransomwaretől immár megszabadított gépünkre. Ha nincs mentésünk, vagy az is elérhetetlen, megpróbálkozhatunk még a Windows rendszer-visszaállítási szolgáltatásához tartozó, úgynevezett Shadow Copy állományokból való adatvisszanyeréssel, sajnos azonban a legújabb CryptoLocker-verziók ezeket is megsemmisítik. És végül még egy lehetőség: ha a törölt eredeti állományokat még nem írta felül az operációs rendszer, egy törlés-visszaállító segédprogrammal (például a Recuvával) megkísérelhetjük helyreállításukat.

Mészáros Csaba

Mennyire biztonságosak a felhőtárhelyek?

Megnéztük, hogy milyen technológiákkal védi érzékeny adatainkat a Dropbox, a Google Drive, a OneDrive és társaik.

Sorra bukkantak fel az újabbnál újabb szereplők az online tárolók piacán. A szoftveres megoldásoknak hála a legtöbben mára már mellőzik a pendrive-ok használatát, és rengeteg mappát, illetve fájlt tárolnak az online adatszinkronizációs szolgáltatások szerverein.

Célkeresztben a biztonság

A piaci igények, illetve a kormány adatvédelmi intézkedéseinek hatására az utóbbi időben a felhőben tárolt adatok biztonságára tolódott át a hangsúly a médiában és a vállalatok kutatás-fejlesztési részlegeinél egyaránt. Egyes cégek – mint a SpiderOak vagy a Tresorit – kimondottan szolgáltatásuk biztonságos működését hangsúlyozzák az érdeklődő vásárlók felé. A felhasználóknak manapság már nem elég, hogy adataikat egyszerűen kezelhetik a felhőben; szeretnék azokat biztonságban is tudni, hogy kizárólag ők férhessenek hozzá.

A webes szolgáltatások biztonságával kapcsolatos aggályok és feltételezések azonban még erősebb hátszelet kaptak, amikor az Apple iCloud egyes fiókjaihoz külső támadók fértek hozzá. Emellett a Dropbox háza táján történt események is elgondolkodtatták a felhasználókat. *Christopher Soghoian* biztonságtechnikai aktivista állítása szerint a széles körben ismert tárhelyszolgáltató megtévesztette a fogyasztókat, amikor azt állította, hogy a regisztrációnál megadott jelszó nélkül senki sem férhet hozzá a Dropboxon tárolt adataikhoz. Ez technológiai szempontból nem helytálló állítás; a vállalat azóta többször változtatott a szolgáltatásához tartozó leíráson, hogy pontosítsa az adatbiztonságra vonatkozó bekezdéseket.

Két pont között

Biztosítást egyik vállalat sem adhat arra, hogy adataink nem kerülnek rossz kezekbe egy esetleges szoftveres hiba vagy támadás esetén. Viszont egy jól megválasztott szolgáltatóval növelhetjük adataink biztonságát. Fájljaink saját, otthoni gépünkről indulnak útnak a távoli szerverek háttértárai felé. Hogy a mozgásban lévő biteket ne lehessen elkapni, a legtöbb szolgáltató SSL vagy TLS technológiákkal védi meg azokat, miközben a két végpont között utaznak. Ez a fajta védelem olyannyira alapkövetelménynek számít, hogy a cikkben vizsgált összes szolgáltató kivétel nélkül ezzel a technológiával dolgozik.

A fent említett módszerrel biztonságosan lehet mozgatni az adatokat két pont között, viszont amint a fogadó oldal megkapja a fájlokat, dekódolja őket. Ez azt jelenti, hogy adataink alapesetben ugyan sértetlenül elértek a szolgáltató szervereire, viszont ott kódolatlanul tárolják őket. Pár évvel ezelőtt több vállalatnál (például a Google-nél és a Microsoftnál) ez volt a bevett módszer;

mára azonban majdnem mindenhol titkosítják a beérkezett biteket. Ez annyit jelent, hogy az átvitel után még egyszer titkosítják adatainkat, általában AES-256-os szabvány alapján. Az AES-256-ost bankok és hasonló intézmények használják, ezzel a szabvánnyal kódolt adatainkhoz kizárólag az férhet hozzá, akinél a dekódoláshoz szükséges kulcs van.

Pontosan ehhez kapcsolódik a következő probléma. Ugyan a legtöbb vállalat már az említett, igen erős kódolást használja fájljaink titkosításához, viszont a dekódoláshoz szükséges kulcsokat is a vállalati rendszeren tárolják. Amennyiben fizikai vagy online támadás éri a szerverparkot, adatainkhoz ugyanúgy hozzá tudnak férni a kulcsok segítségével. Ha nagyon leegyszerűsítjük a problémát, akkor ez a zárban hagyott kulcs esetére hasonlít.

Helyi titkosítás

Nagyrészt ezekkel a biztonsági technológiákkal fogunk találkozni minden szolgáltatónál; TLS kódolás másolás során és AES-256 tárolás esetén. Azonban van egy-két cég, akik ennél is több figyelmet fordítottak a biztonságra. A Bitcasa, SpiderOak és a Tresorit egy úgynevezett „Zero-knowledge" technológiát használ, ami annyit jelent, hogy a felhasználón kívül senki sem férhet hozzá az adatokhoz. Mivel a szolgáltatók többsége saját maga kezeli a dekódoláshoz szükséges kulcsokat, az adatokhoz is bármikor hozzáférhetnek. Az említett három vállalat azonban már a felhasználó gépén lekódolja a fájlokat, és csak utána kezdi átmásolni a saját szervereire. Mivel a titkosításhoz használt kulcsok a felhasználónál vannak, a szolgáltató nem tud hozzáférni az adatokhoz, hiszen csak azok titkosított verzióját látja. Éppen ezért behatolás vagy kényszerített adatszolgáltatás esetén is biztonságban tudhatjuk fájljainkat.

Felhőtárhelyek biztonsági megoldásai

Tárhely-szolgáltató	Titkosított átvitel	Titkosított tárolás	Applikáció-védelem	Kétlépcsős azonosítás	Az üzemeltetők hozzáférhetnek a fájlokhoz?
Dropbox	SSL/TLS	AES-256	✓	SMS, szoftveres	✓
Google Drive	SSL/TLS	✓	✓	SMS, telefonhívás, token, szoftveres	✓
OneDrive	PFS, SSL/TLS	✗	✓	SMS, szoftveres	✓
Sugarsync	SSL/TLS	AES-256	✗	✗	✓
Bitcasa	SSL/TLS	AES-256	✓	✗	✗
Tresorit	SSL/TLS	✓	✓	✗	✗
SpiderOak	SSL/TLS	AES256, HMAC-SHA256	✓	✗	✗
Box	SSL	AES-256	✓	SMS	✓
Cubby	SSL/TLS	AES-256	✓	E-mail, szoftveres	✗

A leggyengébb láncszem

Minden lánc annyira erős, mint a leggyengébb szeme, tartja a mondás. Ez a felhőalapú tárolóknál sincs másképp; hiába titkosítjuk adatainkat AES-256-os szabvány szerint vagy használjuk a beépített helyi titkosítást, hogy még a szolgáltató se férhessen hozzá fájljainkhoz, ha az egész rendszert egyetlen jelszó védi. Amennyiben ez a jelszó kikerül a kezünk közül, féltve őrzött adataink úgy tárulnak fel a behatolók előtt, mint egy földalatti széf, amihez megszerezték a kulcsot. Ezek után a támadó lemásolhatja, letörölheti, és végleg megsemmisítheti adatainkat. Nem kell mást tennie, mint a webes felületen keresztül belépni, letölteni az adatokat, letörölni a fájlokat és megszüntetni a felhasználói fiókot, amivel az összes ott tárolt adat törlésre kerül. Amint a weben törölték fájljainkat, a szolgáltatáshoz feltelepített szinkronizációs szoftver miatt helyi szinten is törlődnek adataink. Amennyiben lehetőségünk van rá, ennek elkerülése érdekében minden belépésnél használjunk kétlépcsős azonosítást. Ezen felül nem árt, ha érzékeny adatainkról helyi szinten is készítünk biztonsági mentéseket.

Dropbox: egyszerű kezelhetőség és alapvető titkosítás

Dropbox

Rengeteg átalakuláson ment keresztül a Dropbox 2007-es bemutatkozása óta. A szolgáltatás főként az egy-

szerű használhatóságra fókuszál, de egyúttal megfelelő biztonsági beállításokkal is felszerelték a szoftvert. A fájlok SSL/TLS kapcsolaton keresztül mozognak a távoli szerverek és gépeink között, és AES-256-os titkosításban részesülnek, amint megérkeznek a Dropbox szervereire. A program nem használ beépített helyi titkosítást, ezért a szolgáltató bármikor hozzáférhet adatainkhoz, illetve harmadik fél nyomására kiadhatja azokat. Amennyiben feltörnék a Dropbox rendszerét, adataink az AES-256 titkosítás ellenére sem lennének biztonságban, mivel a dekódoláshoz szükséges kulcsokat is a szervereken tárolják. A Dropboxnál lehetőségünk van kétlépcsős azonosítást használni, illetve jelszóval védeni a szolgáltatáshoz szükséges mobilapplikációinkat. A szolgáltatás üzleti verziója havi 12 eurótól (kb. 3600 forint) érhető el, amely korlátlan tárhellyel és további funkciókkal szolgál felhasználóinak. A bizniszcsomag legkisebb megvásárolható egysége öt felhasználó.

Google Drive: az AES-256-os kódolás itt is alapvető

Google Drive

A Google behozta lemaradását, és az utóbbi években jóval biztonságosabb lett a keresőóriás cloud tárhelye. A többi megoldáshoz képest a Drive nagy előnye, hogy szorosan integrálódik a keresőóriás többi szolgáltatásába, ami rengeteg munkafolyamatot leegyszerűsít (például egy Gmail-csatolmányt egy kattintással küldhetünk át felhőtárhelyünkre). A Drive emellett biztonsági funkciók sorát nyújtja felhasználóinak: SSL/TLS fájlátvitel, AES-256 titkosítás a cég szerverein, illetve jelszóval védhető mobilapplikáció. A kétlépcsős azonosításnál a Google az egyetlen szolgáltató, amelynél négyféle azonosítási forma közül választhatunk. A szolgáltatás üzleti verziója még több biztonsági funkciót és korlátlan tárhelyet nyújt, felhasználónként havi tízdolláros (kb. 2400 forint) árért cserébe.

OneDrive

A régebben SkyDrive-nak nevezett rendszer a Microsoft agresszív árleszállító stratégiája miatt a legolcsóbb megoldások közé tartozik a piacon. A redmondi cég ugyan nem biztonságtechnikai megoldásairól híres, de a szolgáltatás ilyen szempontból is egészen jól szerepel. A személyes fiókokhoz kapunk SSL/TLS titkosítást, kódolható mobilapplikációkat és kétlépcsős azonosítási funkciót. Viszont a vizsgált szolgáltatások közül a Microsofté az egyetlen, amely nem titkosítja adatainkat a távoli szervereken, tehát nincs AES-256 védelem. A OneDrive mellett szól a PFS átvitel használata (Perfect Forward Secrecy), amely még magasabb szintre emeli a fájlátvitelek biztonságát. A vállalat üzleti csomagjai öt dollártól (kb. 1250 forint) kezdődnek, amelyhez egy terabájtnyi tárhelyet, illetve AES fájltitkosítást kapunk. Az egyterás személyes, illetve a biznisz kategóriájú fiókokhoz ingyenesen jár a Microsoft Office 365 is.

Bitcasa-anomália

A cikk írása során kipróbáltuk a Bitcasa ingyenes verzióját. Öt gigabájt tárhely, Zero knowledge technológia, beépített streaming, mobiltámogatás és további fantasztikus funkciók sora szerepelt a leírásban.
A Bitcasa úgy működik, mint egy külső meghajtó. A fájlok nem tárolódnak a helyi lemezeken; minden Bitcasa meghajtóra másolt bit a felhőben landol, és onnan is nyílik meg. Mivel az amerikai cég megoldása helyi titkosítást használ, a Dropbox mappámból áthelyeztem olyan fájlokat a Bitcasa szervereire, amelyekhez jobban szerettem volna, ha rajtam kívül senki nem fér hozzá. Miután a gép befejezte az áthelyezést, újraindítottam a Windowst. A Bitcasa szoftvere azonban több próbálkozás után sem indult el. Ez még nem lett volna gond, de a webes felületen keresztül sem tudtam hozzáférni a föltöltött fájljaimhoz. Minden próbálkozásnál egy pirosra színezett üzenetet kaptam: „Ismeretlen probléma." Néhány jól célzott Google-keresés után kiderült, több felhasználó is tapasztalt hasonlót, de a vállalat nem válaszolt a hetekkel ezelőtt bejelentett hibajegyekre és fórumbejegyzésekre. Az én esetem szerencsés, mert a Dropbox verziókezelő rendszerén keresztül vissza tudtam állítani adataim eredeti állapotát. Ez az eset azonban jól szemlélteti, hogy bármennyire is bízunk a szolgáltatások mögött álló vállalatokban, nem ésszerű csak ilyen megoldásokra hagyatkozni, mert privát adataink, illetve munkánk láthatja kárát.

SugarSync

Régi motoros a felhőalapú tárolók piacán a SugarSync, a Dropboxhoz hasonlóan, a vállalat használta biztonsági megoldások azonban elég foghíjasak. Az SSL/TLS és az AES-256 titkosítás ugyan rendelkezésünkre áll, azonban nincs lehetőségünk kétlépcsős azonosításra, illetve a mobilapplikációknál sem

tudunk belepési kódot megadni. A SugarSync üzleti csomagja jóval drágább a versenytársakénál; havi 55 dollárba (kb. 12 228 forintba) kerül. Ezért az árért egy terabájtnyi helyet és nonstop telefonos ügyfélszolgálatot kínál a vállalat.

Bitcasa

Meglehetősen egyedülálló a Bitcasa megoldása. A szinkronizációs szolgáltatásokkal ellentétben a Bitcasa meghajtóra másolt adatok közvetlenül a távoli szerverekre kerülnek. A szolgáltatás helyi titkosítást alkalmaz, tehát a Bitcasa dolgozói sem férnek hozzá adatainkhoz. A rendszer továbbá SSL/TLS és AES-256 kódolást használ, illetve mobilrendszereken jelszó segítségével le tudjuk korlátozni az applikációhoz történő hozzáférést is. A vállalat rendszere azonban nem teszi lehetővé a kétlépcsős azonosítást. A Bitcasa egy terabájtos prémium csomagja tízdolláros (kb. 2400 forintos) havidíjért vehető igénybe, a tízterás Pro csomag pedig havi kilencvenkilenc dollárt (kb. 24 000 forintot) kóstál.

Tresorit

Elsődleges szempont volt a Tresorit fejlesztésénél a felhasználók adatainak biztonsága, éppen ezért a vállalat szoftvere helyi szinten titkosítja a fájlokat, amelyek aztán SSL/TLS kódolással érkeznek meg a cég európai szervereire. A rendszerhez

SugarSync: kétlépcsős azonosítás nélkül

tartozó mobilapplikációkhoz történő hozzáférést jelszóval korlátozhatjuk, viszont a szolgáltatás nem rendelkezik kétlépcsős azonosítással. A száz gigabájtos prémium fiókok havi tíz euróért (kb. 3100 forintért) vásárolhatók meg, az egyterás üzleti csomagok pedig havi húsz eurótól kezdődnek.

SpiderOak

A SpiderOak megoldása a Tresorithoz hasonlóan Zero knowledge technológiát használ, tehát az adatokat csak helyi titkosítás után töltik fel. A rendszer SSL/TLS titkosítást használ a fájlok feltöltésénél, és AES kódolással ellátva tárolja a fájlokat a távoli szervereken. A cég mobilapplikációit jelszóval védhetjük, de a szolgáltatás nem képes kétlépcsős azonosításra. Az ingyenes fiókkal két gigabájtnyi tárhelyet kapunk, a száz gigabájtos Professional csomaghoz pedig havi tíz dollárért (kb. 2400 forintért) juthatunk hozzá.

Boxcryptor

Több szolgáltatás fizetős csomagja további biztonsági funkciókat kínál, és még hatékonyabb technológiákkal segíti a felhasználókat, hogy adataikat biztonságban tárolhassák. Amennyiben nem vagyunk megelégedve szolgáltatónkkal, vagy mi magunk akarjuk elvégezni a titkosítást, akkor a Boxcryptor és az ahhoz hasonló, lokális adattitkosító programok jelenthetik számunkra a megoldást. A Boxcryptor személyes felhasználásra – korlátozott képességekkel – ingyenesen elérhető, és installálás után nincs más dolgunk, mint a Windows intézőben lévő Boxcryptor meghajtón keresztül titkositani azokat a mappákat és fájlokat, amelyeket biztonságban szeretnénk tudni. Ez az egyszerűen kezelhető megoldás egyfelől biztosítja, hogy fontos adatainkhoz senki se férjen hozzá, másrészről nem korlátozza a cloud tárhelyszolgáltató rendszer képességeit sem. Adatainkat a szokásos módon megoszthatjuk és kezelhetjük, a Boxcryptor a legtöbb szolgáltatóval kompatibilis (Google Drive, Dropbox, Microsoft OneDrive, SugarSync stb.).

Box

A Box, hasonlóan a legtöbb cloud tárhelyszolgáltatóhoz, rendelkezik az alapvető biztonsági funkciókkal. Ahogy azt megszokhattuk, már az ingyenes fiókok is SSL/TLS és AES-256 kódolásban részesülnek, a mobilapplikációkat lekódolhatjuk, illetve lehetőségünk van kétlépcsős azonosítás igénybevételére is. A szoftver nem használ helyi titkosítást, ezért fájljaink láthatók és megnyithatók maradnak a vállalat dolgozói számára. Az ingyenes fióknál kétszázötven, a száz gigabájtos, hét fontot (kb. 2700 forintot) kóstáló csomagnál pedig öt gigabájtos fájlméretkorlátozással kell számolnunk.

Cubby

A LogMeIn is csatlakozott a cloud tárolók piacához a Cubbyval. A szolgáltatás SSL/TLS és AES-256 kódolást használ mappáink ás fájljaink védelmére. A Cubby mobilapplikációkban megtaláljuk a passlock funkciót, illetve a rendszert kétlépcsős azonosítás képességgel is ellátták. A száz gigabájtos Pro csomag havi négy dollárba (kb. 950 forintba) kerül. A fizetős verziókkal lehetőségünk van megkerülni a felhőt, és eszközeink között közvetlenül szinkronizálni adatainkat. A Pro csomag ezen felül tartalmazza a Cubby Locks funkciót is, amely lehetővé teszi, hogy csak az férhessen hozzá fájljainkhoz, aki tudja LogMeIn-jelszavunkat.

Horváth Máté


PCWorld
pcworld.hu