Mit szűrnek mások, és mit tehetünk mi magunk?

Linkeskedő linkek

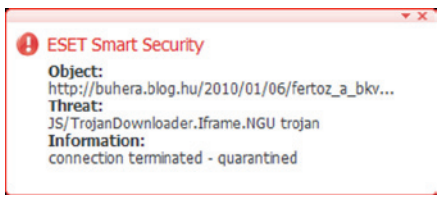
Az internet egyik nélkülözhetetlen elemeiről lesz szó sorozatunk harmincötödik részében, a linkekről. Ezek visznek minket tovább keresésünk irányába, de időnként lehetnek kártékonyak is. Kik és hogyan próbálják ezeket eltéríteni, szűrni, ellenőrizni, milyen linkek lehetnek gyanúsak, és mit lehet tenni azért, hogy megóvjuk magunkat?

Régebben ha fertőzött, gyanús linkekről beszéltünk, általában e-mail mellékletekben kapott üzenetekről és az azokban szereplő hivatkozásokról volt szó. Ezek terjesztése persze nem szűnt meg, de újabban jobbára a weben és különösen közösségi portálokon, blogokon, kommentekben, valamint a Google keresési eredmények találataiban lehet ilyenekbe beleütközni. Hogy hogyan kerülnek kártevőkre mutató linkek a különféle helyekre, azt már alaposan kitárgyaltuk a sorozatunk 26. epizódjában. Arról viszont szót ejtünk, hogy pontosan mit is tesznek ellene a különféle szolgáltatások üzemeltetői.

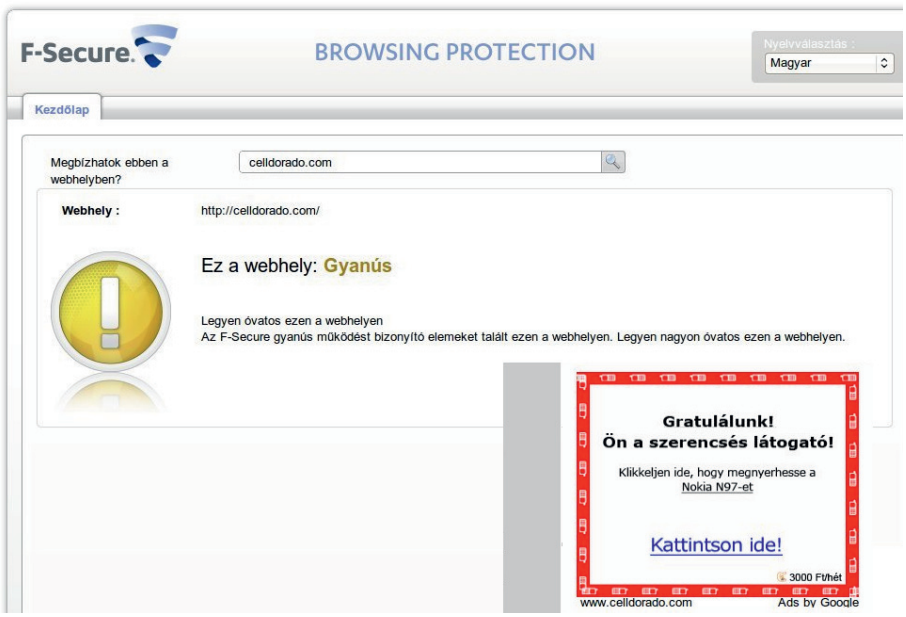
A huszonhatodik részben teljes egészében azzal a kérdéssel foglalkoztunk, hogyan keletkezik a bejelentett támadó webhely, és hogyan gyógyítsuk azt

Searching...

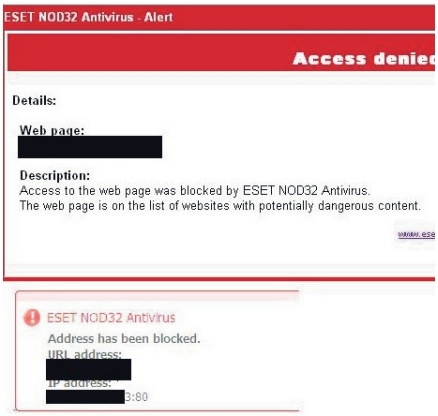
Ha keresésről van szó, szinte mindenki azonnal a Google oldalára gondol, és valljuk be, ez az egyik legjobb és legnépszerűbb eszköz, amit milliók használnak szerte a világon. A kártevőterjesztők úgy okoskodtak, hogy ha valami rendkívüli esemény történik, érdemes egy domaint regisztrálni, vagy fertőzött botnetes gépekre irányítani a keresőtalálatokat, azt remélve, hogy ezekre majd sokan fognak kattintani. Korábban csak alkalmilag, katasztrófák, híresség vélt vagy valós halálhíre, Valentin-nap, kiemelkedő sportesemények megrendezése esetén került sor tömeges linkmérgezésre, de mára ez a foglalatosság ipari méretűvé nőtt, és állandóan veszélyezteti a netezőket. A Symantec végzett egy felmérést, amelyből az derült ki, hogy szervezettebb és automatizáltabb ez a jelenség, mint azt korábban gondoltuk volna. A háttérben gyaníthatóan a hamis antivírus programok fejlesztői állhatnak, erről tanúskodik az az adat is, miszerint a webes keresők első 70 találatának körülbelül 68 százaléka vezet rendszerint kártékony oldalakra, és ezek szinte mindig az emlegetett „pánikprogramokat" tartalmazzák. Nem kell hát vulkán, nem kell Storm Worm, Eurovíziós dalfesztivál, NHL kupa, ezektől teljesen függetlenül állandó jelleggel folyik a Google Trends monitorozása, automatizált kihasználása. A vizsgálatok eredményei, amelyet a Google 2010. márciusi és áprilisi találatai alapján végeztek, azt mutatták, hogy a napi aktuális top 10 keresőszó alapján indított keresések eredményei közül mindig volt legalább három olyan, ahol kártékony linkekre mutattak a hivatkozások.



Ha kártékony kód van a weboldalon, a vírusirtó nyomban észleli. Itt még akkor is kaptunk riasztást, amikor csak egy komment tartalmazta szövegként a káros JavaScript-részletet



Nemrég indult az F-Secure Browsing Protection szolgáltatása, ahol bármilyen URL begépelése után megkapjuk annak értékelését. Ez lehet teljesen ártalmatlan vagy gyanús minősítésű, esetleg kifejezetten kártékony



Kártékony linkeket már több víruskereső megoldás is nyilvántart, ezeket pedig a szignatúraállományokhoz hasonlóan rendszeresen frissíti

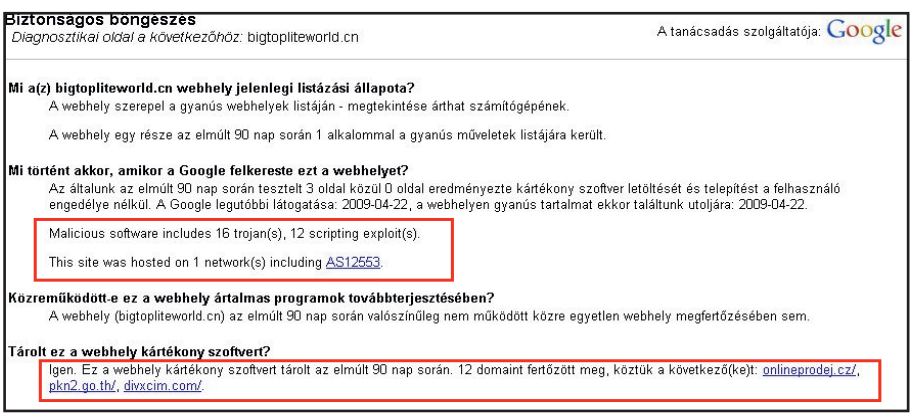
Ágnes asszony a patakban linkjeit mossa

Emiatt a Google-nél több millió oldalt vizsgálnak át naponta. Ez az elemzés a hatalmas meglévő és keletkező mennyiség miatt – a víruslaborokba ömlő napi sok ezer mintához hasonlóan – nem emberi, hanem automatikus feldolgozást jelent. Elsőként azt nézik meg, hogy egy adott URL tartalmazza-e a „bank" vagy a „login" szavakat, illetve szerepel-e benne domainnév helyett gyanakvásra okot adó IP-cím, nem szokatlanul hosszú-e az URL-sor – ezek mind gyanús jelek lehetnek. A továbbiakban aztán ellenőrzésre kerül, tartalmaz-e jelszó („password") nevű űrlapmezőt, megnézik a host szerverek területi információit stb. Utolsó lépésként pedig ellenőrzik az adott oldal esetleges adathalász-, spam-, illetve kártevőgyanús visszajelzéseit, a kétes domainhostot és hasonlókat. Ezek az összetett információk adnak aztán egy végső képet, ami alapján ha a Google szükségesnek látja, feketelistára teheti a linket. Az automatikus ítélet miatt elvétve előfordulhat hamis riasztás, de szerintük az ilyesmi pozitív esélye csekély, 1 a 10 000-hez. Nyilván az otthoni gépünknél csak egyedül erre az elemzésre támaszkodni helyi biztonsági programok helyett badarság lenne, de azokat ha némi késéssel is, de jól kiegészítheti. Persze az időfaktor is igen lényeges, valószínűleg a kártevőterjesztők sokkal gyorsabbak, és amíg a Google gépezete le is tiltja a linkek egy részét, addigra már régen újabbak vannak a nyitó oldalakon.

Addig oké, hogy van nálunk naprakészen tartott antivírus szoftver, de a Facebookon található kártevőket elsősorban nem az azt üzemeltetőknek kellene inkább kiszűrni?

Közösségi oldalak

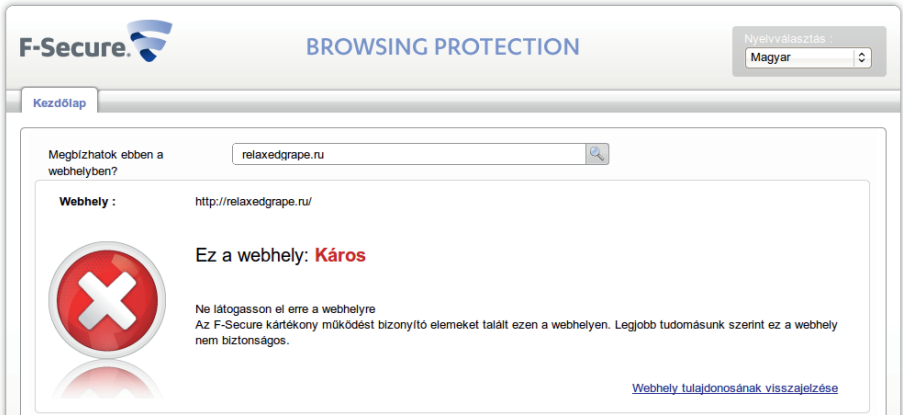
A Twitternek 75 millió tagja van, és bár az üzenetek mérete csak 140 karakteres – ezek gyakran rövidített linkeket tartalmaznak –, körülbelül 55 millió poszt keletkezik naponta. Az e-mailben küldött kéretlen linkeknél mindig is veszélyesebbnek számítottak ezek a közösségi üzenetek vagy bejegyzések, mert mindenki úgy gondolja, hogy ezek valamiért megbízhatóbbak. A rossz hír az, hogy ab ovo ez nem igaz, a jó hír, hogy a Twitter 2010. március óta már próbál tenni valamit a kártevőterjesztők ellen. Úgy gondolták, hogy mivel a felhasználók már eleve óvatlanabbak a közösségi oldalakon, legalább a linkek tekintetében próbálják megelőzni a kártékony kódok terjesztését. Ez igen hasznos lehet, hiszen rengeteg adathalász támadás indul innen, a további kártevőkről, trójaikról, kémprogramokról nem is beszélve. Előfordulhat az is, hogy hamis antivírus programra mutató linkeket küldenek Twitteren keresztül, és akinek nincs valódi védelmi programja vagy tapasztalatlan felhasználó, ebbe a csapdába is bele tud sétálni. Remélhetőleg a linkek helyzete ettől jobbra fordul, a felhasználók alapvető naivitása azonban továbbra is „kezelésre" szorul.



A Google esetében azt is részletesen lekérdezhetjük, miért lett feketelistás egy adott oldal. Ez esetben jól látható, hogy gyanús szkripteket és 16 egyértelműen azonosítható trójai programot tartalmazott a weboldal

Túlzásba vitt minőségi munka

Egy érdekes eset némileg beárnyékolja a kártékony linkek hatékony szűrését a Twitternél, de bízzunk benne, hogy azóta már minden olajozottabban működik. 2009. október 8-án *Mikko Hyppönen*, az F-Secure kutatási igazgatója meglepődve vette észre, hogy a fiókját felfüggesztették. Később kiderült, hogy ez egy eredetileg augusztus 3-i, adathalász weboldalra figyelmeztető, linket is tartalmazó bejegyzése



A különféle webes tartalmi tanácsadók (pl. Web Of Trust), maga a Google, de a weboldali ellenőrző szolgáltatások is leleplezhetik a kártékony oldalakat. Fontos lenne, hogy mindez (észlelés, bejelentés, feldolgozás, ellenőrzés, adatbázis-frissítés) minél gyorsabban történhessen meg

A figyelmeztetések platformfüggetlenül érkeznek, tehát nemcsak Windowson, hanem Macintosh vagy Linux operációs rendszer alatt is megkapjuk ezeket

miatt történt. A megoldás több kérdést is felvet. Egyrészt a linket szándékosan nem kattinthatták le a felhasználók szintaktikával írva (szóközök voltak benne). Másrészt ha ez egy olyan Twitter-szolgáltatás, amivel az ügyfeleket kívánják az üzemeltetők megvédeni, akkor miért a kéthónapos késés – vagy csúfoljuk inkább reagálási időnek? További érdekessége még a történetnek, hogy a szakembernek komoly neve van, és sokan elismerik a tevékenységét, nem kértek tőle elnézést utólag sem és a letiltott, majd visszaállított fiókja miatt a követői is jóvátehetetlenül elvesztek, mivel ezeket az adatokat az üzemeltetők végül nem voltak hajlandók számára helyreállítani.

Arcoskodjunk

A Facebook napi 570 millió látogatóval dicsekedhet, a közösségnek pedig már több mint 400 millió aktív felhasználója van a regisztrált 500 millióból. Átlagosan minden tagnak körülbelül 130 ismerőse van, a tagok pedig havonta mintegy egymilliárd képet töltenek fel. Emellett 70 százalékuk valamilyen alkalmazást, játékot is futtat az oldal kínálatából. Mindegyikük kapcsolódik 60 további oldalhoz, csoporthoz, rendezvényhez és minden hónapban körülbelül 70 új tartalmat (bejegyzés, üzenet, kép, videó) hoz létre. Tehát poszt-tok, linkek nagy számban jönnek-mennek itt is, ehhez elég csak a legutóbbi „The Sexiest Video EVER" tárgyú, látszólag ismerőseinktől jövő üzenetekre gondolni. Sajnos a kártékony linkek Twitterhez hasonló (de inkább annál sokkal jobb...) szolgáltatói szűréséről egyelőre nem tudunk.

A telepíthető Facebook-alkalmazások között is rendszeresen feltűnnek gyanús, vagy kifejezetten trójai alkalmazások, mint például a Fan Check vagy az Error Check System. A veszély szempontjából emiatt nyilván nem lehet figyelmen kívül hagyni a magyar felhasználókat sem, ők most körülbelül 1,3 milliónyian lehetnek.

Linkek fogyókúrán

A már említett, veszélyes URL-rövidítés lényege, hogy bármilyen kacifántosan hosszú linkből képes egy rövidke, akár a Twitterhez szükséges maximum 140 karakterbe beférő új hivatkozást generálni. Viszont a link nevéből – ami kattintás után ugyanúgy elvisz minket az eredeti oldalra – már nem lehet semmit sem kiolvasni. 2009 tavasza óta a spam- és kártevőterjesztők hihetetlen mértékben rákaptak erre az URL-rövidítési technikára. Jó megoldás lehet tehát egy olyan böngészőplugin, amely képes a rövidített link mögé pillantva képes megmutatni annak eredeti tartalmát. Ami a Bit.ly-t illeti Firefox alatt, szerepel a kiegészítők között a **Bit.ly Preview** (addons.mozilla.org/en-US/firefox/addon/10297/). Ez pontosan azt csinálja, amiről fentebb szóltunk, ha az egérmutatót még kattintás előtt a rövid időre a link fölé mozdítjuk. Létezik már ráadásul egy univerzális, minden linkrövidítési szolgáltatást kezelő **TheRealURL** (www.therealurl.net) nevű kiegészítő is, illetve a **Google Chrome View Thru** pluginje (hopp.pcworld.hu/7064) is ugyanezt valósítja meg.

További fegyvertársak

Ha Internet Explorert vagy Firefox webböngészőt használunk, több más forrásból is kaphatunk figyelmeztetést. Ha telepítjük a **NetCraft Toolbar** (toolbar.netcraft.com), a **Finjan Secure Browsing** (securebrowsing.finjan.com), a **Web of Trust** (www.mywot.com), **Web Security Guard** (www.websecurityguard.com) vagy a **McAfee Siteadvisor** (www.siteadvisor.com) webes tanácsadók valamelyikét – vagy mindegyikét –, akkor ezek is listázzák a felhasználók bejelentései alapján a weboldalakat, illetve rendszeresen frissített adatbázisuk alapján tudnak minket riasztani. (Az említett programok egy része Google Chrome böngészőhöz is elérhető.) Ha mindez nem lenne elég, látogassunk el az **F-Secure Browsing Protection** oldalára (browsingprotection.f-secure.com), ahol bármilyen URL vizsgálatát elvégezhetjük. Emellett több antivírus termékben működik már külön kártékony linkeket figyelő eszköz – többek közt a NOD32 is tartalmaz ilyet –, így ezek közvetlenül a böngészéskor is képesek az ismert veszedelmes oldalakra való lépést megakadályozni.

Kattintare necesse est

Az interneten keresni azonban mégis kell, mit lehet hát akkor tenni? Ebből a nagy tanulság csak az lehet, hogy a kereső találata nem szentírás, figyelmünket ekkor se kapcsolhatjuk ki, legyünk résen. Néha segíthet a találat linkjének szemrevételezése is, például nyilván nem egy kínai oldal tájékoztat majd a legautentikusabban *Michael Jackson* vagy egy más híresség valós vagy kitalált haláláról. A böngészőből érdemes a biztonságosabb változatokat (Opera, Firefox) választani, felvértezni azokat okos kiegészítőkkel (például NoScript, ShowIP). Emellett fontos egy megbízható antivírus program is, amely megfelelő beállítások mellett mind a webhozzáférést, mind pedig a MSN és egyéb üzenőprogramok mellékleteit, linkjeit képes ellenőrizni. A távoli jövő várhatóan a keresővállalatok és az antivírus gyártók valamilyen közös adatbázisán alapuló linkszűrése lehet, így biztosítható lenne a védekezéshez szükséges egyre rövidebb reakció idő, ami valljuk be, az antivírus cégeknél egyelőre nagyságrendekkel gyorsabb.

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

velemeny@pcworld.hu

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