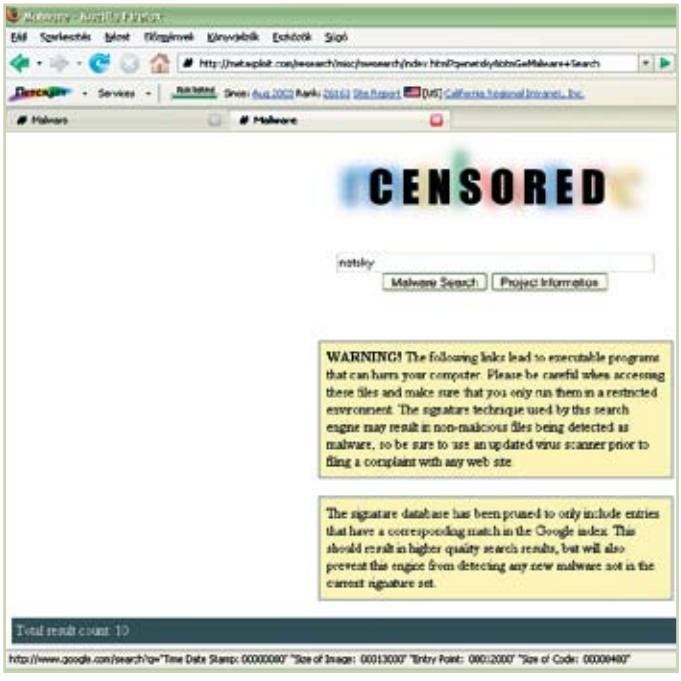
METASPLOIT MALWARE SEARCH

Víruskeresés a Google segítségével

Sorozatunk negyedik epizódjában a Google-t a szokásostól eltérően fogjuk használni: vírusokra vadászunk vele! Fény derül arra is, hogy az internetes keresők olykor olyan tartalmakat is beindexelnek – és ezzel a nagyközönség számára is láthatóvá tesznek –, amelyeket a webszerver-üzemeltetők eredetileg nem szerettek volna közkinccsé tenni.

A MetaSploit Project weboldala (**www.metasploit.com**) napjaink egyik legérdekesebb alkotása, amellyel a biztonsági szakértőknek az exploitok (biztonsági hibákat kihasználó kártevők) keresésére, tesztelésére, valamint a róluk szóló egyéb információk megszerzésére nyílik módjuk. Egyúttal ez a rosszfiúk álma is, hiszen az itt talált kódokat rendkívül egyszerűen be tudják vetni, illetve akár újakat is írhatnak az itt szerzett ismeretanyag alapján. A következőkben a Google internetes keresőjének és a MetaSploit Malware Search szolgáltatásának segítségével magunk is kártevőket terjesztő weboldalakra vadászunk.



A Metasploit Malware Search kezdőlapja

A kártevők új generációja

Az utóbbi években az ártalmas programok egyre inkább a weboldalakról leselkednek ránk. A vírusterjesztők ugyan továbbra is próbálkoznak e-mailes küldéssel, de a leggyakrabban kártékony weboldalakról vagy fertőzött zombigépekről próbálnak meg kártevőt letöltetni a gépünkre. Szintén kedvelt módszer, hogy egy online videotartalom megtekintéséhez új, kiegészítő kodek letöltését javasolja egy weboldal, amit sokan gondolkodás nélkül elfogadnak, és telepítik azt. Az így letöltött, DNS-manipulációt alkalmazó kártevő azután képes teljes mértékben eltéríteni böngészéseinket, észrevétlenül hamisított oldalakra irányít minket, és ezzel hatalmas veszélynek tesznek ki: a valós oldalhoz tartozó jelszavaink a csalóknál kötnek ki. Sajnos ez a módszer Windows alatt viszonylag gyakori, de friss hír az is, hogy egy ilyen típusú kártevőt fedeztek fel a napokban megjelent Macintosh OS X Leopard operációs rendszer alatt is.

Úgy tűnik, a jövő egyik útja az lesz, hogy a rosszfiúk tömegével fognak egyszerű, hétköznapi weboldalakat feltörni – merthogy ez könnyű –, és azok kódját láthatatlanul megmérgezve, vírusok és kémprogramok terjesztésére fogják kihasználni.

Manapság szinte mindenkinek van már a gépén valamilyen vírusirtó. Gyanús levélmelléklet esetében sokan tudnak segítséget kérni, de saját weboldaluk rendszeres ellenőrzését, megfelelő szintű technikai védelmét már sokkal kevesebben tudják ellátni – és mint máshol, a folyamatok itt is mindig a gyengébb ellenállás irányába haladnak. Természetesen emellett a nehezebb falatot jelentő, alaposabban védett, de milliókhoz eljutó közösségi és hírportálok is veszélyben lesznek. Itt a gyenge pontot az emberi lustaság, az elmulasztott vagy késve telepített biztonsági javítások, illetve a nulladik napi, még ismeretlen biztonsági hibák (exploitok) kihasználása jelenti.

Fontos a (szerver) operációs rendszer és az azon futó alkalmazói programok frissítéseinek naprakészen tartása. Ehhez jó segítség lehet a Secunia Inspector, a Microsoft Baseline Security Analyzer vagy akár a Sunbelt Network Security Inspector program. Az említett eszközök hatásosan és alaposan feltárják a gyenge, elavult komponenseket, és a frissítéshez is konkrét linkkel, útmutatóval szolgálnak.

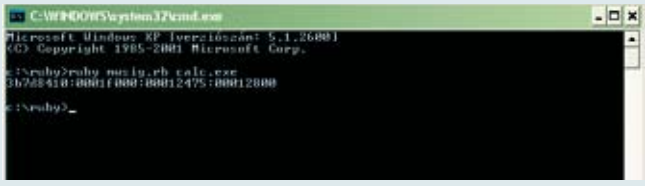
A böngészés közben terjedő kártevők miatt nemcsak az oldalak üzemeltetőinek, hanem nekünk is vigyáznunk kell, hiszen hosszabb-rövidebb ideig akár kedvenc hírportálunk, tisztának gondolt, rendszeresen látogatott weboldalaink is fertőzöttek lehetnek.

Mit tehetünk ez ellen? Az ilyen rosszindulatú oldalakat több módszerrel és helyen is igyekeznek nyilvántartani. Léteznek már beépülőmodulok (NetCraft Toolbar, Finjan SecureBrowsing, NoScript, RgGuard, Crawler Toolbar) a böngészőkliensekhez, amelyek képesek figyelmeztetni, il-

Netsky-találatok a listában

SEGÍTSÉG A KÉTKEDŐKNEK

Ha gyanús programokról gyűjtünk információt, hasznos segítség lehet egy Ruby nyelven írodott program, a Malware Signature Generator **(mwsig.rb).** Ennek segítségével bármely, a birtokunkban levő állományhoz a Metasploit által ismert „szabványos” azonosító szignatúra (ellenőrző összeget tartalmazó „ujjlenyomat”) készíthető, ennek birtokában pedig a Google-keresés is tovább árnyalható. A program kódja a Metasploit oldalán **(hopp.pcworld.hu/3855)** található, az ezt futtató Ruby interpreter pedig a **www.ruby-lang.org** címről tölthető le. (A Ruby egy ingyenes, nyílt forráskódú objektumorientált programnyelv, amelyet egyébként gyors tanulhatósága okán is érdemes megismerni.)



A Ruby nyelven íródott Malware Signature Generatorrel magunk is készíthetünk egy állományról szignatúralenyomatot

CD2/DVD
A cikkben említett programok megtalálhatók a lemezmellékleten

letve a káros tartalmakat blokkolni. A Google is elkezdte már alkalmazni saját hivatkozásminősítő figyelmeztetéseit.

A Netsky féreg nyomában

Azt, hogy valóban vannak ilyen, a kártevőket kéretlenül letöltő oldalak, már az **antivirus.blog.hu** oldal Kattintsunk-e Psycho macskára? című bejegyzésében is bemutattuk – most pedig az alábbi kísérlettel fogjuk demonstrálni.

Menjünk el a Metasploit Project kártevőkereső aloldalára, a Metasploit Malware Searchre (**hopp.pcworld.hu/3794**). Ha olyan általános hivatkozást keresünk, mint például a „worm" vagy a „backdoor", rengeteg találatot kapunk. Szűkítsük egy kicsit a kört, és keressünk egy létező vírust, esetünkben legyen ez a Netsky.

Beírjuk a Netsky szót a keresőablakba, ütünk egy Entert, és már sorakoznak is a lap alján az ezzel kapcsolatos találatok.

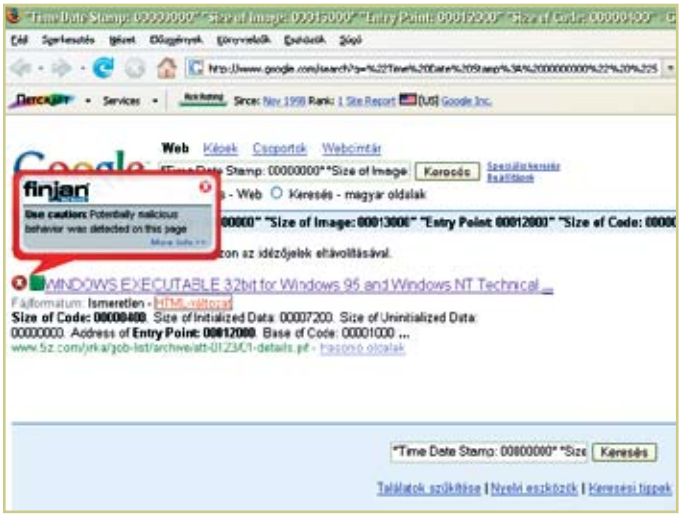
Időzzünk itt el egy kicsit! A Google ablakában lévő tanácsadó ikonok egyike jelez: a Finjan szerint ez „valószínűleg kártékony oldal". A Robot Genius RgGuard beépülője pedig már a Metasploit keresőoldalnál is pirosan világít, és egy ablakban külön figyelmeztet a veszélyes tartalomra.

Az óvatos átlagember számára az lehet a legjobb megoldás, hogy ha a kettő közül bármelyik is riaszt, a szokottnál is körültekintőbben jár el, vagy akár ki is hagyja a weboldalra való kirándulást. Mi most azonban továbblépünk, mert gépünk védelme erős és naprakész.

Gyilkos oldalak – csak biztos védelem esetén!

Válasszunk ki most egy találatot a listáról. Itt az idő, hogy elszántan ráléphessünk a linkre: az eredmény nem is marad el, kérdés nélkül egy letöltési ablak bukkan fel, és le óhajtja tölteni gépünkre a *01-details.pif* állományt, amely nem más, mint a Netsky.Q féreg egy példánya.

Megfelelő vírusvédelmi programmal (tesztgépünkön a NOD32 gyártójának, az ESET Smart Security komplett biztonsági csomagjának RC1 jelű béta-verziója volt telepítve) röptében megfoghatjuk a betolakodót, így blokkolva lesz a vírus. A böngésző még így is elhelyezhet egy példányt a webkliens ideiglenes állományai közé – ha ez bekövetkezik, a vírusirtó természetesen ezt is észleli, és megvéd bennünket: beállításainktól függően törli, vagy karanténba helyezi a kártevőt.



A Finjan SecureBrowsing beépülőmodulja kártékony oldalra figyelmeztet

A Robot Genius böngészőklienshez tartozó beépülője már magát a Metasploit-oldalt is veszélyesnek jelöli

Vétlen áldozat(?)

Félretéve a Metasploit keresőjét, a „mezei" Google keresőbe beírtuk a *01-details.pif* szót, azaz a Netsky végrehajtható állományának nevét. A találati listából kiválasztottuk a **www.5z.com** főoldalát. Az oldalt lekérve nem szembesültünk az előző problémával; semmi sem próbálkozott letöltődni, és webes tanácsadóink is csendesen hallgattak. Némi forrásolvasás után – belekukkantottunk a nyitóoldal HTML-kódjába - kiderült, hogy a lapot egy Jirka nevű illető készítette, a Google-bejegyzésből pedig már tudtuk, hogy a vírus is egy jirka nevű könyvtárban csücsül. Ez első próbálkozásunk idején ott is volt még.

Ezek után két eset lehetséges: feltörve az oldalt, valaki orvul odahelyezte a kártevőt, vagy maga az oldal gazdája volt figyelmetlen, és saját könyvtárában tárolt egy ilyen férget. Még az is elképzelhető, hogy a kritikus állományra nem is mutat hivatkozás a weboldalon, mégis szerepel a Google indexei között.

Magunk közt szólva, ha már valaki a saját webszerverét privát, nem publikus állományok tárolására használja, a .HTACCESS állomány segítségével kikapcsolhatná a hívatlan látogatók böngészési lehetőségét, egyúttal megóvhatja magát attól, hogy a fürkésző keresőrobotok kéretlenül indexeljék a másokra nem tartozó, bizalmas könyvtárakat. Emellett (vagy ehelyett) pedig jelszóval kódolt csomagoknak kellene itt szerepelni, hiszen a mappa tartalma ez esetben nem a nyilvánosságnak lett szánva – legalábbis ezt gyanítjuk.

Ha nagyon sok a szabad időnk, és pedánsak akarunk lenni, megkereshetjük az oldal gazdáját – esetünkben ezt valaki nem sokkal később már megtette –, és jelezhetjük, hogy fertőzött az oldala. Az adatokat a Domain Tools oldalán (**www.domaintools.com**) tudjuk lekérdezni, és itt, a doménfoglaló címe mellett a technikai kapcsolattartót is megtaláljuk.

***

Kicsit technikaira sikeredett ez a mai epizód – a korábbi, olvasmányosabb írásokhoz képest. Ünnepélyesen megígérjük, a következő alkalommal nem veszünk el ennyire a részletekben.

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

A kártékony programot tartalmazó weblap nyitóoldala semmilyen jelét nem mutatja a fertőzésnek

KAPCSOLÓDÓ WEBOLDALAK

ESET Smart Security: **www.eset.com/smartsecurity/**
Metasploit Malware Search: **hopp.pcworld.hu/3794**
Microsoft Baseline Security Analyser Tool: **hopp.pcworld.hu/379**
Secunia Software Inspector: **secunia.com/software_inspector/**
Finjan SecureBrowsing biztonsági beépülő: **securebrowsing.finjan.com**
Robot Genius RgGuard biztonsági beépülő: **www.robotgenius.net**
Netcraft Anti-Phishing Toolbar: **toolbar.netcraft.com**
NoScript Firefox extension: **noscript.net**
Crawler Toolbar: **www.crawler.com/products/toolbar.aspx**