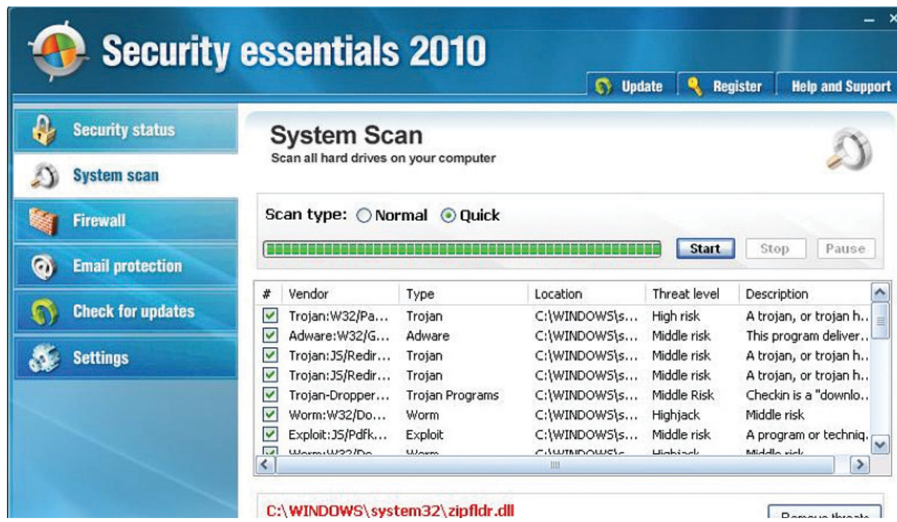
További tippek és trükkök

Csak a változás állandó

Sorozatunk negyvenedik részében kicsit folytatjuk az előző részben elkezdett, böngészéssel kapcsolatos gondolatainkat, valamint szerepelni fog egy érdekes kiegészítő is, amellyel elegánsan szüntethetjük meg a böngészési szokásaink feltérképezését, profilírozását. A továbbiakban egy adag újabb típusú átverést, csalást, kártékony programok terjesztését szolgáló trükköt is bemutatunk, valamint sort kerítünk egy olyan összefoglalóra, amely a legfontosabb védekezéshez szükséges teendőket ismerteti.

Ahogy az előző részben láttuk, résen kell lenni a linkekkel, sőt a böngészési előzményekre is muszáj vigyázni. Az Electronic Frontier Foundation tanulmánya szerint a böngészőből lekérdezhető információk segítségével a látogatások 94 százalékában megállapítható a látogató személye. Azt, hogy egy böngésző miket kérdezhet le, mit lát belőlünk, egyszerűen megnézhetjük például a www.useragentstring.com weboldalon. Vegyük észre, hogy itt mindegy, fut-e a NoScript, a használt operációs rendszert, a böngésző típusát és verzióját mindenféleképpen láthatjuk. Van lehetőség a referer adatok blokkolására – ez ugyebár az az információ, hogy milyen oldalról érkeztünk az adott URL-re. Az **Adaptive Referer Remover** (hopp.pcworld.hu/5249) kiegészítő többnyire pontosan ezt csinálja, vagyis visszatartja ezeket az adatokat. Sajnos ez a kiegészítő eléggé instabil, gyakran már a telepítésekor jégkockává fagyasztja a Firefoxot.

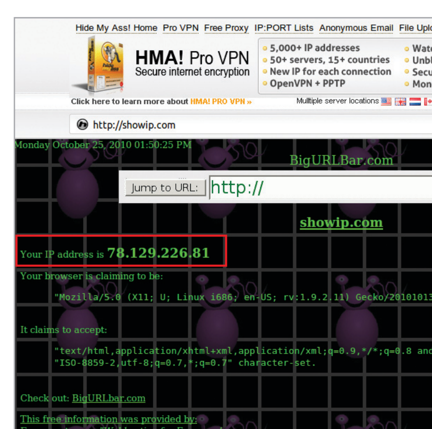
Ha emlékszünk rá, rendelkezésünkre áll egy **ShowIP** (hopp.pcworld.hu/5371) nevű Firefox-kiegészítő is, amely pedig a böngészett weboldal IP-címét mutatja meg az ablak keretén, így ellenőrizhetjük, vajon valóban az igazi OTP oldalán vagyunk-e éppen. Ha viszont a mi saját külső IP-címünket szeretnénk ellenőrizni, azt a showip.com oldalon tehetjük meg. Ekkor a földrajzi információk birtokában egy internetes hirdetést megjelenítő, mondjuk egy apróhirdetési oldal vagy ingatlanközvetítő vagy társkereső oldal képes lehet a mi falunkból, városunkból származó célzott ajánlatokat megmutatni. A proxy szerverek használata képes ezt az adatot megváltoztatni, és nyitott proxyk használatával például egy amerikai egyetemi szerver mögötti gép is láthat minket. Egyszerűen kipróbálhatjuk ezt a hidemyass.com (a pontos fordítástól ezúttal eltekintünk…) nevű honlap segítségével, ahol ha ezen keresztül érünk el egy linket, már nem a saját IP-címünk kerül bele a lekérdezésbe.



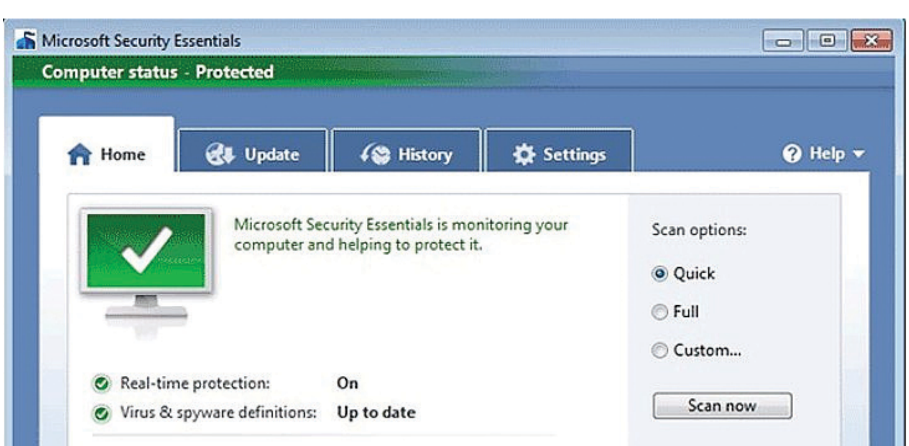
Ez a Security Essentials nem az a Security Essentials! Ráadásul míg az eredeti ingyenes, addig a csalók a hamisítványért még pénzt is kérnek

Egy beteg matróz és egy egészséges ötlet

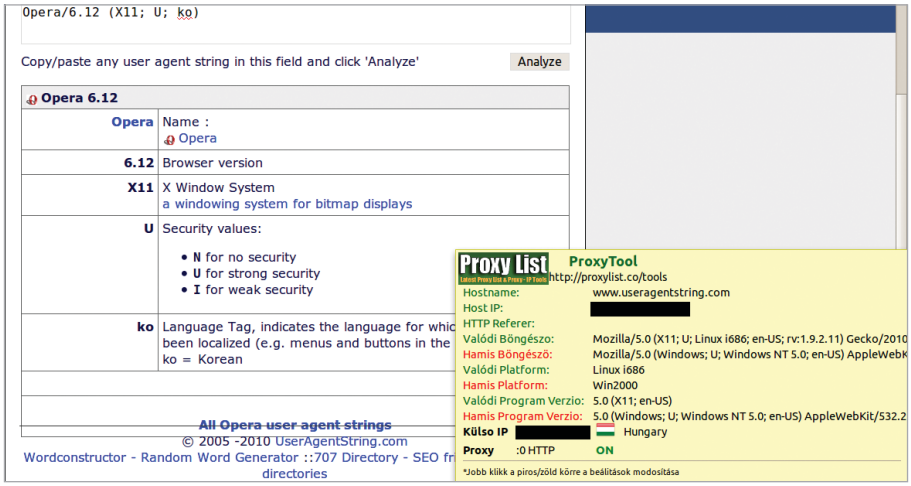
Gyúrjuk akkor mindezt össze, és képzeljük el, hogy egyetlen eszközzel, „Viribus unitis" mutatunk fityiszt ezeknek a lekérdezéseknek.



Ha az IP-címünk elfedésére van szükség – például egy adott országból nem férünk hozzá egy adott oldal tartalmához –, akkor a „hátsónk elrejtésével" könnyedén kicselezhetjük ezt a korlátozást

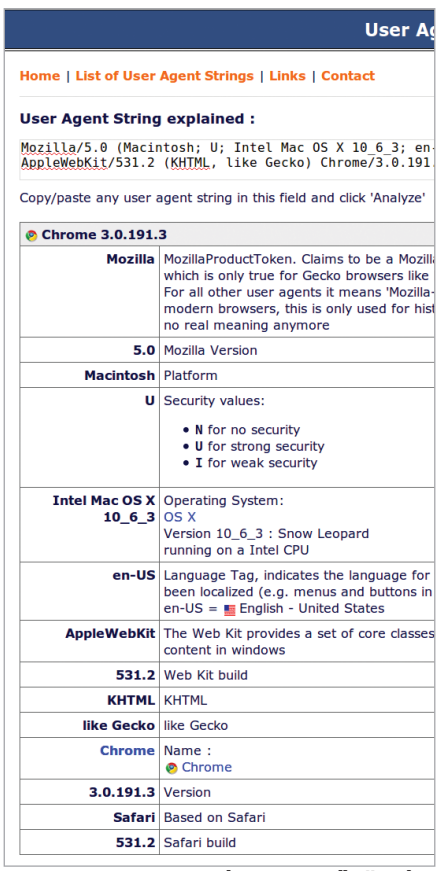


Microsoft Security Essentials, ahogy azt mindenki ismeri. A sokak számára ismerősen csengő nevet divat lett azonban egyéb csalafintaságokra is felhasználni



„Hiszem magam, aminek akarom.” A Proxy Tool egy igazán ütőképes, mindent egyben tartalmazó svájcibicska-szoftver, amely a földrajzi elhelyezkedési adatunkról árulkodó IP-cím, a böngészőből lekérdezhető OS, illetve webkliens valódi adatainak elfedésére is alkalmas

Most nyissuk ki a szemünket, és vegyük elő a **Proxy Tool** (hopp.pcworld.hu/7433) nevű Firefox-kiegészítőt. Itt tetszés szerint beállítható, milyen egyéni referert akarunk mutatni magunkból, vagy akár minden alkalommal véletlenszerűt is megadhatunk. Tetszés szerint törölgethetjük a HTML- és Flash-sütiket, ezenfelül kedvünk szerint használhatjuk az alapértelmezetten rendelkezésre álló proxyszervereket, vagy akár sajátokat is megadhatunk. Egy ilyen kiegészítővel való játszadozás tényleg felvidíthatja a napunkat, és segít privát létünk hatékony megőrzésében. Jólesően konstatálhatjuk, hogy sikerült megvalósítani a Rejtő-könyvekben szereplő alapelvet: „Semmi közöd ahhoz, ami nem tartozik rád!”



Ha a Proxy Toolban a véletlenszerű böngészőkiíratást választjuk, álmodhatunk nagyot és bármik lehetünk: Linux, Windows, Macintosh, Chrome, IE, Firefox, Opera, vadakat terelő juhász

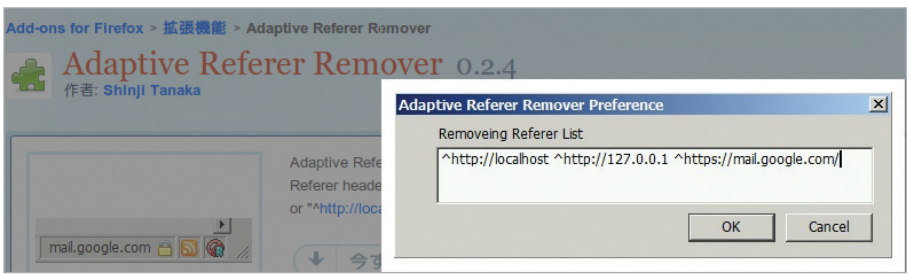
A Gellért-hegy így magas, a krokodil meg így zöld

A böngészőadatok után nézzük, milyen újabb kártevőterjesztő módszerek kerültek mostanában a felszínre. A hamis antivírus szoftverek már sokszor terítéken voltak, és egyszer azt is megemlítettük, hogy ezek kinézete, valamint a hamis ablakokban szereplő kártevők elnevezése is többnyire valódi vírusirtókról származnak. Egy újabb módszer szerint az ál-antivírus termékek elnevezése is előtérbe került, olyan valóban létező, a félinformációkkal rendelkező tömegek számára ismerősnek tűnő neveket választanak, amelyek segíthetik az elegendően nagy számú kattintást, letöltést. Egy ilyen vonal a Microsoft Security Essentials csomagjával való manipulálás.

A korábbi trükköket ezúttal megfejelték még egy érdekességgel. Aki még emlékszik a 23., *Kártevőelemzés házilag* című epizódunkra, annak ismerős lehet a **Jotti** (virusscan.jotti.org) weboldal. Ez a sokkal ismertebb VirusTotal.com oldalhoz hasonlóan szintén egy csomó antivírus motort tartalmaz, és a feltöltött gyanús állományok online vizsgálatát végzi (amikor például a VirusTotal nagyon leterhelt, akkor jó alternatívát jelenthet). Ha megvizsgálunk egy állományt és az ottani riport kinézetére koncentrálunk, rögtön ismerős lehet az a trükk, amit az újabb ál-Essentials mutat. Itt is sok motor keresési eredményét összefoglaló képet kapunk, ám érdekes módon az ismert antivírus termékek közé olyan neveket is beillesztettek, mint az AntiSpySafeguard, Major Defense Kit, Peak Protection, Pest Detector vagy a Red Cross. Ha valaki sosem hallott ezekről, az ne szomorkodjon, ezek egytől egyig hamis vírusirtók. Ami viszont még ennél is viccesebb, az az, hogy míg például az F-Secure, Kaspersky, McAfee, NOD32 és Symantec termékek nem detektálnak semmit, az előbbi új nevek mindegyike felismeri ezeket az állítólagos csúnya gonosz „kártevőket”, sőt gálánsan linket is biztosít a „mentesítéshez”.

Nem vazelin, Vaszilij!

A netezők többsége már jól ismeri a Bejelentett Támadó Webhely szindrómát. Ezt egyszerű felhasználóként is láthattuk, amikor böngésztünk, de elszenvedhettük úgy is, mint aggódó weboldal-tulajdonos. Ennek elhárításakor azonnali feladatunk a kártékony JavaScript-kód kigyomlálása az összes HTM, HTML, PHP állományunkból, haladéktalan FTP-jelszócsere, és irány a Google Webmaster Tools, ahol bejelentjük, hogy immár tiszta az oldalunk, és türelmesen várjuk a webhely visszaminősítését. Pontosan itt jön a képbe a jó érzékű csaló, aki visszaélve ezzel a már jól ismert üzenettel, elkészíti a hamis „Reported Attack Page!” feliratú oldalt. Ha feltesz-



Közöd? – kérdezhetnénk a weboldalaktól, amelyek arra kíváncsiak a HTTP Referer fejlécben, hogy honnan is kattintottunk oda. Az Adaptive Referer Remover segít nekünk ebben: jó titkos ügynökhöz hasonlatosan nem hagyjuk kikérdezni magunkat, nem szivárogtatunk

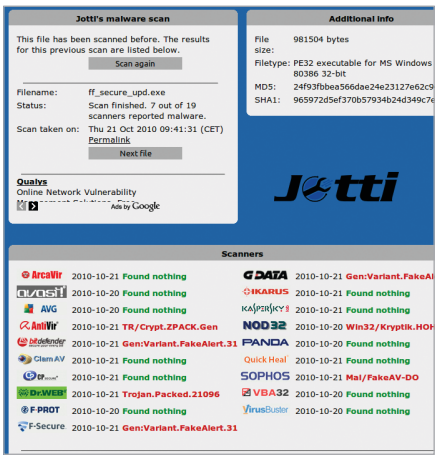
szük a kérdést, hogy vajon miben is különbözik az eredeti és a preparált oldal, akkor jól látható, hogy a különbség a letölthető frissítési (**Download Updates**) gomb, amelyre kattintva egy kártevő próbál meg a számítógépünkre települni.

Nyilas Misi pakkot kapott

Egyik korábbi cikkünkben már kalapot emeltünk az előtt a trükk előtt, amikor is az elkövetők az autók szélvédőjére tettek csali értesítő cetlit azzal a szöveggel, hogy állítólag lefotózták és megbüntették az autónkat szabálytalan parkolás miatt, és a mellékelt linken megtekinthetjük az inkriminált képet. A büntetőcédulák persze hamisak voltak, a weboldal pedig kártékony szoftvereket próbált telepíteni az áldozatok számítógépére. Egy újabb trükk ezúttal a DHL és UPS csomagküldő szolgálat nevével él vissza – a készítők egy kéretlen levélben arról tájékoztatnak bennünket, hogy a nekünk szánt csomag kézbesítése a címzés sajnálatos hibája miatt nem sikerült, de a levélhez mellékelt űrlapot kinyomtatva, kitöltve és személyesen bemutatva átvehetjük a küldeményünket a postán vagy az irodában. Természetesen a mellékelt ZIP kiterjesztésű állomány kártevőt tartalmaz, de ez a kinyomtatósdis beugratás azért tényleg zseniális. (Forrás: **hopp.pcworld.hu/7434**)

Érdemesebb online bűnözni, mint bankot rabolni

Nem véletlen, hogy a különféle fenti módszerek, trükkök gombamód szaporodnak: már 2007-ben megállapítást nyert, hogy az USA-ban a számítógépes bűncselekmények több pénzt hoztak a szervezett bűnözők konyhájára, mint a drogkereskedelem. A rendőri erők is úgy értékelik, hogy teljes mértékben átalakult a hagyományos bűnözés. Régebben, ha a kábítószerfutárok elvesztették az árut, bankot raboltak, hogy megtérítsék a kárt a főnökeik felé. Ma már tudnak egyszerűbb verziót: például inkább bérlik vagy megvásárolják ukrán szerzők kártékony programjait, és ezek segítségével csapolják meg tömegesen hétköznapi felhasználók vagy cégek számláit. A hamis álláshirdetéssel toborzott szamarak (angolul az öszvér – mule – szót használják rájuk) pedig egy kevés jutalékért elvégzik a piszkos munkát, vagyis átutalják a pénzt a lopott számlákról a bűnözőknek. Mindezt szinte lebukásmentesen, hiszen ha nagy ritkán el is kapnak a balekok közül valakit, az semmit sem fog tudni részleteiben a szervezet nagy egészéről.

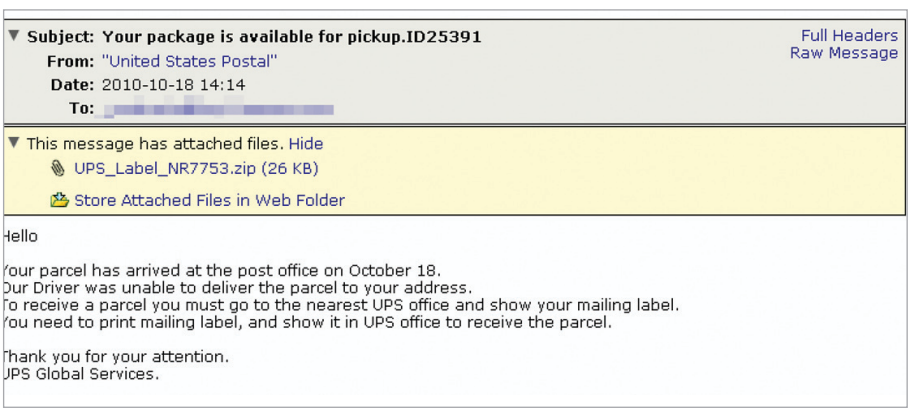


A Jotti Malware Search kinézete, ahogy azt mindenki ismeri. Egy új ál-vírusirtó ezt is igyekszik kiaknázni és megtévesztésre felhasználni

Vajon milyen súlyos fertőzés lehet az, amit a nevesincs AntiSpySafeguard, Major Defense Kit, Peak Protection, Pest Detector és Red Cross előzékenyen felismer, míg az F-Secure, Kaspersky, McAfee, NOD32 és a Symantec szoftverei nem detektálnak?

És mi, belgák, hogyan védekezzünk?

A két fő fertőzési ok, ami miatt gépünket mostanában támadhatják – vagy amiatt, hogy egy botnet részévé kívánják tenni, vagy pedig személyes adatainkat szeretnék ellopni, kikémlelni. Melyek azok a lépések, döntések, teendők, amelyek segíthetik vagy megkönnyíthetik a védekezést? Ha vírusvédelmi terméket választunk, érdemes olyan programot használni, amely erős proaktív védelemmel rendelkezik. A valós idejű heurisztikus, viselkedésalapú elemzés – mint például a ThreatSense – segíthet minden olyan új kockázat időben való felismerésében, amely a vírusismereti szignatúra-adatbázis segítségével még nem észlelhető. Jelentősen csökkenthetjük a szükséges döntési helyzetek számát, és persze egyúttal a kockázatokat úgy is, ha minden olyan levelet, amelynek a feladója ismeretlen, olvasatlanul törlünk. Amikor pedig állományokat vagy telepítendő programokat töltünk le, legyünk elővigyázatosak. Csak ismert, ellenőrzött, megbízható helyről installáljunk szoftvereket, illetve minden újdonságnak alaposan nézzünk utána az interneten. Ha már sokan panaszkodnak egy-egy ilyen alkalmazásra, inkább kerüljük el a felesleges kockázatokat. Érdemes az operációs rendszerünket és minden használt alkalmazást naprakészen tartani a biztonsági frissítésekkel. Amint ezek közül új jelenik meg, haladéktalanul futtassuk le, bezárva ezzel a már kijavított sebezhetőségeket. Ha a gépünkön Microsoft Windows fut, kapcsoljuk be a frissítések automatikus telepítése opciót. Ha pedig NOD32 vagy ESET Smart Security programot használunk, érdemes tudni, hogy ezek is képesek figyelmeztetni, jelezni a Tálcaikon narancsszínre váltásával, ha még telepítetlen biztonsági frissítések állnak a rendelkezésünkre.



Elvileg UPS csomagunk érkezett, ehhez mindössze a ZIP mellékletben lévő űrlapot kellene megnyitni, kicsomagolni, kinyomtatni és kitölteni. Ehelyett ténylegesen egy kártevő lapul a csatolmányban

***

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