SZÜKSÉGES-E VÍRUSVÉDELEM, VAGY ELÉG AZ ÓVATOSSÁG?

Homokba dugott fej

Sorozatunk huszonkettedik epizódjában körüljárjuk a két ellentétes oldal érveit. A piros sarokban úgy gondolják, hogy ha óvatosan neteznek, nem eshet bántódásuk antivírus szoftver és profi tűzfal nélkül sem. A kék sarok ezt azért másképp látja: óvatosságra természetesen szükség van, de ettől még nem nélkülözhetőek a biztonsági programok.

Aki már olvasott különböző számítástechnikai fórumokat, az biztosan megtapasztalta, milyen erős indulatok tudnak időnként elszabadulni. Egy-egy Linux kontra Windows, Norton vs. Kaspersky, vagy éppen a „vírusirtót csak az idióták használnak" témájú topikba akár ezernyi hozzászólás is érkezhet, de nem biztos, hogy igaz érvek csapnak össze a hitviták-ban. Most meghallgatjuk a két fél érvelését, aztán megpróbálunk igazságot tenni.

Piros sarok: zavaró és felesleges ballaszt annak, aki ésszel netezik

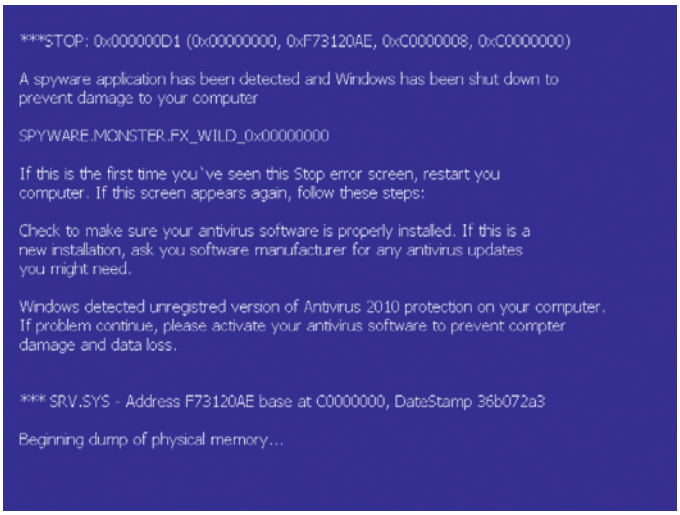
Vajon mi vezet arra valakit, ha már ért a géphez valamicskét, hogy olyan kijelentésre ragadtassa magát, mint például, hogy az antivírus program tolakodó, zavaró és felesleges? Ez az oldal azt állítja, nem használ semmilyen antivírus szoftvert, de nem az ára miatt, vagyis ingyenes verziót sem telepítenek fel. Így aztán nincs is semmifajta teljesítménycsökkenés, vakriasztás, biztonsági programok esetleges összeakadása. A koncepció lényege az, hogy kizárólag a Windows beépített eszközeire támaszkodnak és ehhez társul még néhány kialakult szabály.

Az első védelmi vonalat a tűzfal jelenti, és ebből akár több is működhet náluk egyszerre, ugyanis a legtöbb router tartalmaz ilyet, és emellett a Windows alapkészletébe is beletartozik a szoftveres tűzfal.

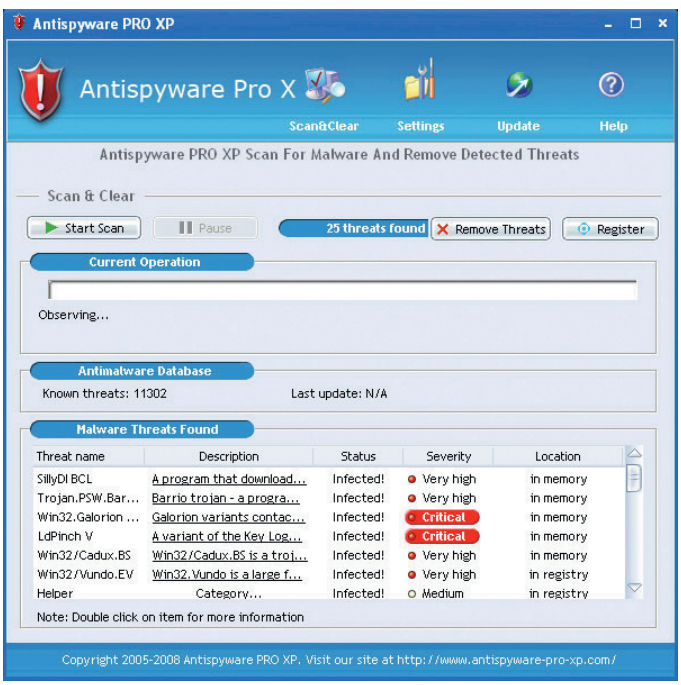
Természetesen az útválasztó önmagában nem tudja megállítani a vírusokat, kémprogramokat, adathalász támadásokat. Viszont ha valaki például Gmailt használ, akkor a spamszűrő modul elég hatékonyan képes kiszűrni a kéretlen levélszemeteket, és ezek közt sok a kártevő-terjesztő oldalak linkjeire mutató üzenet. Mint tudatos felhasználó, természetesen nem is kattint mindenfajta levélre vagy levélmellékletre, hiszen jól tudja, mivel járhat ez.

Bemutatkozik a fegyverarzenál

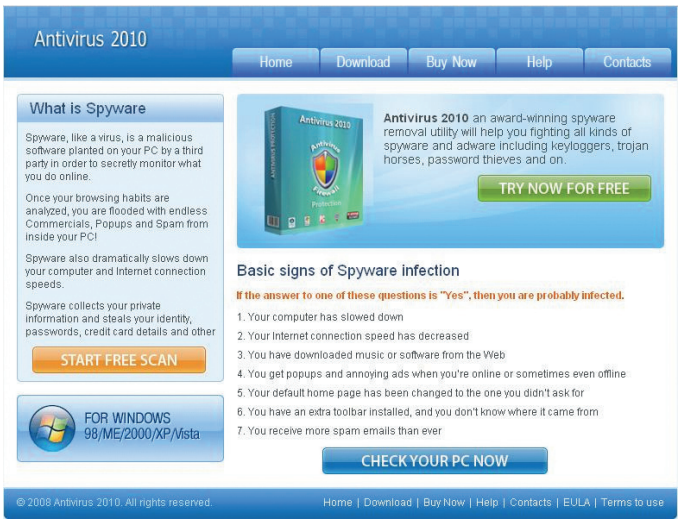
A tudatos böngészés ismét csak felvet eszközbeli, valamint viselkedésbeli kívánalmakat. Ez a csoport nagy ívben kerüli a régebbi kiadású Internet Explorer használatát, és jobbára az új IE 8, de még inkább a Mozilla



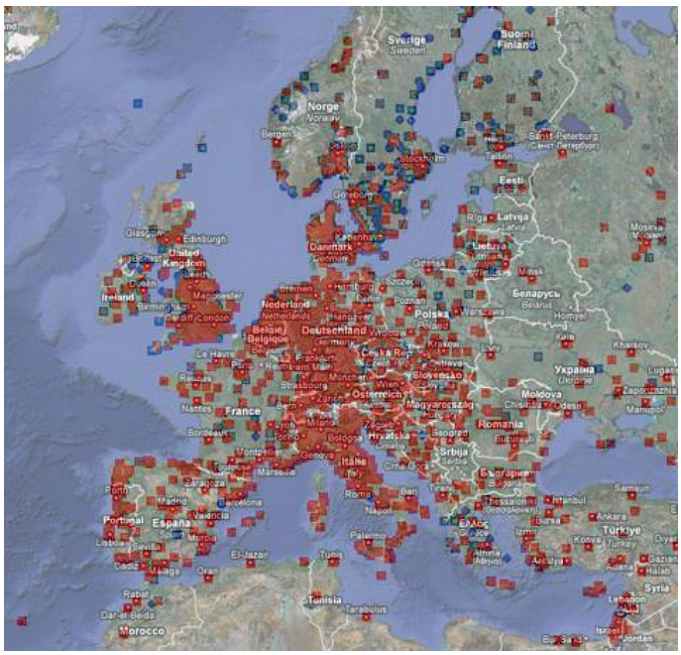
A kék halált nem szeretjük, sőt kimondottan utáljuk. Ez valójában csak egy trükkös kép, amikor nem igazi lefagyás történt, hanem a hamis antivírus akarja velünk elhitetni, hogy baj van a gépünkkel.



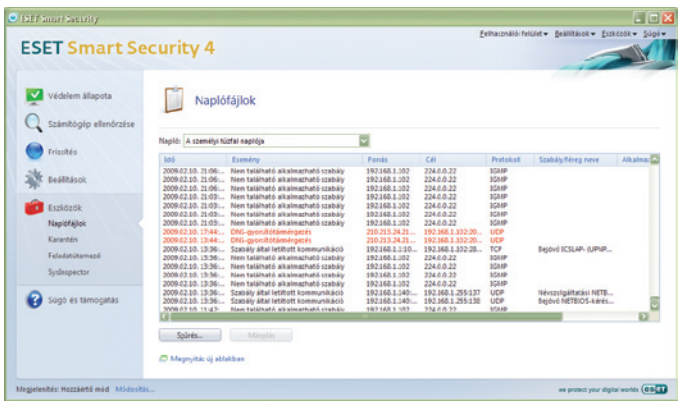
Tudjuk, hogy egy hamis kémprogramirtó minden esetben jelez, még újonnan telepített tiszta gépen is. Egy igazi védelmi programnak is lehetnek vakriasztásai, ennek ellenére érdemes használni



Kevés olyan szoftvert ismerünk, amely egyaránt kompatibilis a Windows 98-tól kezdve az XP-n át egészen a Vistáig. Már ennél a pontnál is elkezdhetnénk kételkedni erre az „olcsó", valójában hamis védelmi programra



A klub, ahova nem szeretnénk tartozni. A térképen Európa Conficker féreg által fertőzött botnetes gépei láthatóak. Ők is úgy gondolták, nincs szükségük védelemre



Amire a Windows beépített tűzfala nem képes: mind a kimenő, mind a bejövő adatforgalom ellenőrzése, szofisztikált szabályrendszer alkotása, részletes beállítási lehetőségek garmadája

Firefox mellett teszi le a voksát. Mindezekben van valamilyenfajta phishing-szűrési opció, amely tippet, tanácsot ad, ha olyan weboldalra látogatnánk, ami szerinte egyértelműen vagy gyaníthatóan csalárd. Mindkét böngészőkliens fejlesztői sokat dolgoztak azon, hogy minél több biztonsági megoldás kerüljön bele a programba.

Ez igen: naprakész és legális

A piros sarokban emellett gondosan beállítják mind a Windows operációs rendszer, mind pedig az összes fontosabb felhasználói alkalmazás frissítéseinek automatikus fogadását. Ezzel állításuk szerint elkerülik a problémákat, hiszen a kártevők sokszor használnak ki olyan exploit kódokat, amelyeket a tudatlan vagy lusta felhasználók nem frissítenek. Ezek között nemcsak néhány hónapos, de akár többéves is szerepel, és valóban az ember szinte nem is érti, miért nem futtatják a felhasználók a kész javításokat ennyi idő eltelte után sem.

És a végső „érv": kerülnek mindenfajta kétes weboldalt, mindenfajta nem megbízható hírű vagy ismeretlen állomány letöltését. Nem járnak pornó-, warez-, szerencsejáték- és hasonló, a kártevők terjesztésében élenjáró weblapokra. Sőt, nem használnak warez vagy illegális szoftvert sem, csak legális vagy ingyenes programokat futtatnak a gépükön.

Kék sarok: szép-szép, de azért árnyaljuk csak kissé ezt a képet!

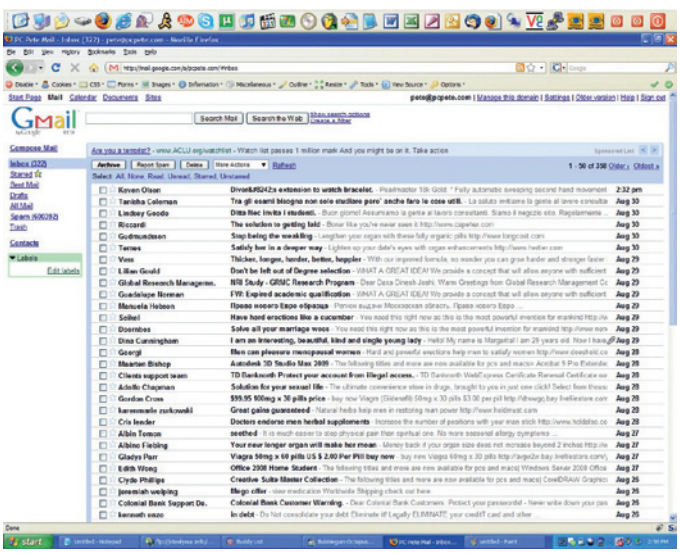
Biztosan annak is van egy kis *Robin Hood*-feelingje, ha valaki évi pár-ezer forintot igyekszik megspórolni, dacolva a biztonsági szoftveriparral. Látni kell azonban, hogy az elmúlt húsz év eseményei egyre gyorsabb iramban arról szóltak, hogyan lehet alkalmazásokat és szolgáltatásokat másként használni, hogyan lehet hibákat széleskörűen kihasználni. Mivel a kártevők bűnözők által történő terjesztése és célba juttatása már egy tudatos és iparszerű folyamat, nem igen boldogulnánk segítő-védő alkalmazások nélkül. A piros sarokban felsorolt óvatossági intézkedéseket matematikaprofesszorosan „szükséges, de nem elégséges" lépeseknek értékeljük. Hiszen nagy hangon mondhatja bárki, hogy neki nincs szüksége szánalmas ajtózárra, a zár- és lakatművek tőle nem lát egy fillért sem, majd ő megvédi magát, lakását, házát a nuncsakujával. Ami az esetek jelentős részében talán működik is, de mi van, ha a lakástulajdonos éppen alszik, WC-re megy, fürdik, esetleg el kell mennie otthonról, netán a kopogás nélkül érkező „látogatók" fizikai erőben, felfegyverzettségben és létszámban is fölényben vannak?

A konstruktív ellenzék dicsér is, ha van mit

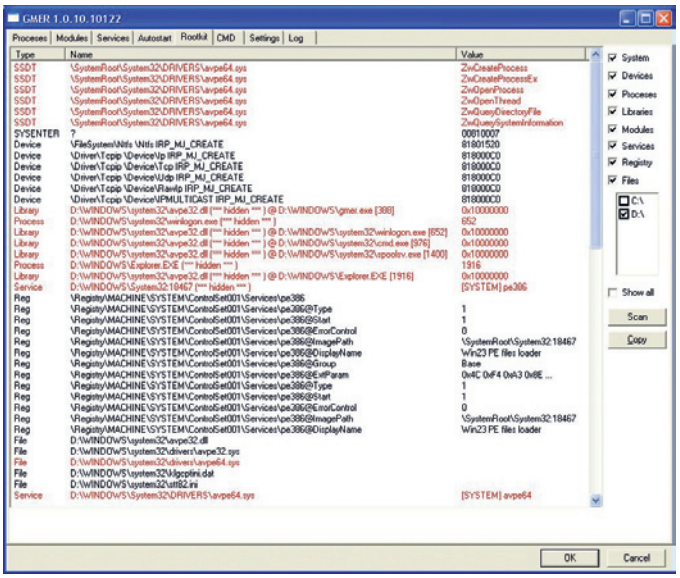
Természetesen találunk azért részben pozitív üzenetet a külső fejlesztésű biztonsági szoftverek ellenzőinek szavaiban. Tekintve, hogy hajlandóak egy keveset tanulni, kiemelt odafigyelést tanúsítanak az internet- és számítógép-használat közben. Ezek jó dolgok, de valójában inkább kiegészítik a számítógépes biztonsági programok védelmét, semmint kiváltanák, vagy helyettesítenék azokat. A gyanakvó hozzáállás szintén sokat segíthet a gyakran alkalmazott emberi megtévesztésen alapuló (social engineering) csalási, fertőzési incidensek elhárításánál.

A böngészők, és az ezekbe épített adathalász, illetve egyéb kiegészítő figyelmeztetési lehetőségek valóban hasznosak, de ne feledjük, amíg egy ilyen listára felkerül egy potenciálisan káros URL, addig több óra vagy még ennél hosszabb idő is eltelhet.

Napjainkban számos olyan fertőző weboldal létezik, ahol a támadók az FTP-jelszavakat eltulajdonítva titokban belépnek a weboldalakra, és ott minden HTM, HTML, PHP állományba beszúrnak egy IFRAME taget, amely kártékony kódot tartalmazó linkre mutat. Néhány vírusvédelmi program – köztük a NOD32 is – böngészés közben azonnal észleli az ilyen gyanús IFRAME szekciót, és annak tartalmától függetlenül egy általános figyelmeztetéssel riaszt. Emellett ha esetleg mégis meglátó-



A Gmail spamszűrője kifejezett jó hatásfokkal válogatja szét a hasznos és haszontalan küldeményeket. Képünkön egy terhelési kísérlet eredménye látható, 600 ezer kéretlen tesztlevéllel



Fertőzés esetén még aktív vírusvédelem esetén is kerülhetünk olyan helyzetbe, hogy az antivírus mellett még külön segédprogramot (GMER, www.gmer.net) is igénybe kell venni némely nehezebben eltávolítható kártevő esetében. A feketével jelzett „fertőzések" nem biztos, hogy kórokozót jeleznek – csak a szakembereknek adnak információt –, ezeket ne próbáljuk eltávolítani!

gatjuk ezt a fertőzött oldalt, akkor pedig magára a kártevőre kapunk egy másik, az adott kórokozó kódjára jellemző konkrét riasztást.

Lyukak a falban

Azt mindenkinek tudnia kell, hogy a Windows beépített tűzfala a többi szoftveres tűzfallal összehasonlítva igencsak gyengének számít. Az első probléma mindjárt az, hogy magától csak és kizárólag a bejövő forgalmat szűri, a kimenőt egyáltalán nem. Hatékonyság területén sem képes felvenni a versenyt a külső gyártók által fejlesztett versenytársakkal, a legtöbb teszten minimális vagy éppen nulla pontszámot képes csak összeszedni, és emellett a beállítási lehetőségei is jócskán elmaradnak a többi programéhoz képest.

Egy tűzfal alapos beállítása nem egyszerű feladat, és sok olyan kommunikáció zajlik közben, amely olyan döntés elé állítja a felhasználót, hogy engedélyezzen vagy tiltson-e valamit. Például ha valaki a Microsoft Office programcsomagot használja, az akkor is megkísérli a kommunikációt a SharePoint szerverrel, ha ez az opció nincs is az otthoni gépen telepítve. Egy jó tűzfalprogram tehát fel kell legyen készítve a kifelé menő forgalom minősítésére, és ha ismeretlen dolgot talál, akkor minimum figyelmeztet, de még inkább kérdez.

Tényleg észlelhető minden csak megérzéssel?

Bár a közelmúltban komoly figyelmeztetések láttak napvilágot például a Conficker féreg kapcsán, sokan valóban úgy gondolják, őket nem érheti baj. Úgy véljük, számos esetben még a sok tapasztalattal és „megérzéssel" rendelkező óvatos felhasználót is meg lehet fertőzni. Ismeretlen eredetű program telepítésekor pedig szinte nélkülözhetetlen, hogy a régi és új kártevők detektálása is megtörténjen. A Windows is tartalmaz ugyan egy kártevőellenes programot, amelyet havonta egyszer frissítenek. A ritka frissítés, és a piaci versenytársakkal nem összemérhető funkcionalitása ellenére néha használ vehetjük, de semmiképpen sem pótolhatja egy komoly professzionális antivírus és kémirtó alkalmazás tudását. Az csak egy dolog, hogy egy modern biztonsági program például már tartalmaz heurisztikát az új kórokozók viselkedésbeli tulajdonságai alapján történő korai felismeréséhez, de sok esetben a rejtőzködő, Windows API-függvényeket eltérítő és ezért hagyományos eszközökkel nem észlelhető „láthatatlan" rootkiteket is detektálni tudja.

Kicsit még kapcsolódva a Conficker-hez, azt láthatjuk, hogy sokan nem fordítanak elég figyelmet a Windows és alkalmazásaik rendszeres biztonsági frissítéseire. Az antivírus-mentes oldalnál azonban örvendetesen azt tapasztalhatjuk, hogy erre kiemelt figyelmet fordítanak. Ebből érdemes lenne azoknak is profitálni, akik viszont használnak ugyan vírusirtót, de ezt a részt viszont teljességgel elhanyagolják. Ezt eltanulhatnák tőlük, és például egy Secunia Software Inspectorral (**secunia.com/vulnerability_scanning/**) igen kényelmesen frissíthetőek az olyan nagy exploitveszélynek kitett alkalmazások, mint az Adobe Reader, az SWF Flash, az Office állományok vagy éppen az Apple Quick Time. Egyet viszont mindenképpen meg kell jegyezni: léteznek emellett nulladik napi sebezhetőségek is, amelyekre még nem is léteznek biztonsági javítások, és az ezek elleni védekezés még védelmi program esetén sem megoldott.

A heurisztika feladata az új kórokozók viselkedésbeli tulajdonságaik alapján történő korai felismerése. Akkor szeretjük, ha mindent észrevesz, de közben nem produkál vakriasztásokat. Az AntiStealth modul pedig a rejtőzködő rootkitek ellen hasznos, nélküle esélyünk sincs a leleplezésre

Internet Security nélkül mit érek én?

Máté Péter már sajnos nem énekelhet a fenti címmel slágert, mi viszont jól tesszük, ha nem „énekeljük ki" a személyes és banki adatainkat, jelszavainkat. Bár néhányan úgy gondolják, hogy az antivírus programok üzletága csupán olyan biznisz, ahol a fejlesztő cégek azon gazdagszanak meg, hogy saját maguk írják a vírusokat – ez távolról sem igaz. Szinte mindegyik fejlesztő csapat kicsiben kezdte, megbízható és rendkívül felkészült szakemberekkel folyamatosan küzdenek a néha szinte reménytelen mennyiségben keletkező kártevők áradata ellen, és várhatóan a helyzet évről évre keményebb próbatétel elé állítja őket, ahogy minket felhasználókat is. Nem lehet elégszer hangsúlyozni, hogy 100 százalékos védelem nem létezik, így esetleg még az is megfertőződhet, aki naprakész védelmi programokat használ. Már csak emiatt sem érdemes szándékosan tárva-nyitva hagyni az ajtót, hiszen ezzel ennek esélyét emeljük nagyságrendekkel.

***

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**
Windows Sysinternals programok: **www.sysinternals.com**
GMER rootkit detektor és eltávolító: **www.gmer.net**