HAMIS ANTIVÍRUS PROGRAMOK

Egészpályás letámadás vírusirtóra hangszerelve

Sorozatunk tizenötödik epizódjában egy sajnos igen elterjedt ál-antivírus programcsaláddal fogunk foglalkozni. Ez XP Antivirus 2008, 2009 és hasonló neveken érkezik, és kész rémálom, ha egyszer a gépre kerül. Természetesen nem hagyományos vírusirtóról, hanem egy kártékony, az embereket becsapó és gépeinket megfertőző programról van szó, amely – nem mellékesen – még a pénztárcánkat is megcsapolhatja.

Bárhogyan is nevezzék az ál-antivírus programot, egyben mindegyik azonos: nem létező kártevőkre, fertőzésekre figyelmeztet és pénzt akar

A hétköznapi ember számára megtévesztő, hogy egy csaló program még a *PC World* magazin legjobb vételeként hirdeti magát, de nem kevésbé vérlázító a Softpedia kártevőmentességet hirdető tanúsítványának odahamisítása sem

Ha a Windows rendszer alatt valamilyen programot kívánunk telepíteni, zömmel egy setup folyamatot indítunk el, amely aztán nemcsak egy „bitkolbászt” húz el szemünk láttára 1-től 100%-ig, hanem telepíti is a program szükséges komponenseit, könyvtárakat készít ezek számára, útvonal- és indító bejegyzést hoz létre, és még egy fontos momentum: megjegyzi és eltárolja a későbbi esetleges uninstallálási folyamathoz szükséges információkat. Általában, ha a továbbiakban el akarunk távolítani egy alkalmazást, az alábbi esetek többsége, vagy akár mindegyike rendelkezésünkre áll.

Ha a fejlesztők alaposak és gálánsak voltak, rendelkezésre bocsátanak egy külön kiválasztható menüpontot is az uninstall indítására.

A másik nagy és sima út, ha a *Start* menün belül a *Beállítások → Vezérlőpult → Programok telepítése és törlése* menüpontot választjuk, ez is hivatalos és szabályos módszernek számít. Ehhez persze az is szükséges, hogy a listában szerepeljen az eltávolítandó program.

Ha ezek valamelyike nem működik, még mindig meg lehet szabadulni a nem kívánt alkalmazástól az Easy Uninstallerrel vagy egy ehhez hasonló segédprogrammal. Ez még mindig biztosabb és kényelmesebb, mint a végső megoldás: kézzel törölgetni az állományokat és Registry-bejegyzéseket.

A normál ügymenet áttekintése után nézzük, milyen akadályokat igyekezhetnek az utunkba állítani. Például egyáltalán nincs uninstall, és sok esetben szembesülünk azzal, hogy a program törlése utáni gépindításnál mégis visszakerül valahogyan a nem kívánt alkalmazás. Lehet aztán olyan „vicces” és kilométer hosszú, apróbetűs licencszerződés, amelyen nem a szokásos „elfogad” és „elutasít” gombok szerepelnek, hanem csak egyetlen választási lehetőségünk van: elfogadni, sőt az ablak felső sarkából még az X, azaz bezár funkció is hiányzik, hogy kész helyzet elé állítsanak minket. Ha pedig pont egy biztonsági program műveli ezt velünk, az körülbelül az a kategória, mintha a pap rontaná meg a gyermekünket, az orvos ölné meg a beteget vagy a rendőr törne be hozzánk – mélységes és váratlan ilyenkor a csalódás.

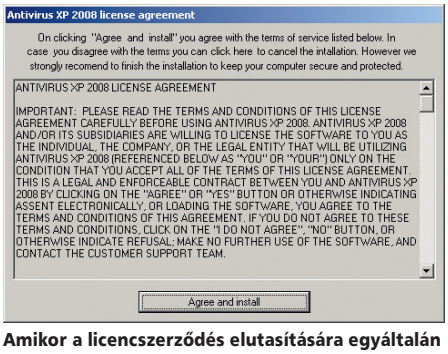
Induljon a banzáj

Ha valaki figyelmetlenségből feltelepít egy ilyen programot, valószínűleg hamarosan visszasírja az írógépes korszakot. Igen sokféle néven találkozhatunk ál-vírus-, illetve kémprogramirtóval, felsorolunk néhány közismert nevet: **AntiMalware 2009, AntiMalware-Suite, AntivirusProtection, Antispyware 2008 XP, AntiSpyware Pro XP, Antivirus Lab 2009, Antivirus Security, Antivirus XP 2008, ConfidentSurf, ContraVirus, DataHealer, eAntivirus Pro, MalwareScanner, Master Antivirus 2009, Micro Antivirus 2009, Perfect Cleaner, PersonalAntiSpy, Smart Antivirus 2009, Spyware Guard 2008, System Optimizer 2008, Virtual PCGuard, VirusGuard Plus, VirusResponse Lab 2009, Vitae Antivirus 2008, Windows Antivirus, XP Protector 2009, Zinaps Anti-Spyware**. Nem mindennapi sorozat ez, és számuk sajnos napról-napra folyamatosan növekszik.

Agybaj a gépben

Akár véletlenül, akár tévedésből kerül a számítógépre, onnantól folyamatosan ijesztgeti a felhasználót. Esetenként olyan hamis BMP állományokkal is manipulál, melyen a lefagyást jelző kékhalál (BSOD, Blue Screen Of Death) vagy egy kémprogramfertőzésre figyelmeztető ablakot ábrázol.

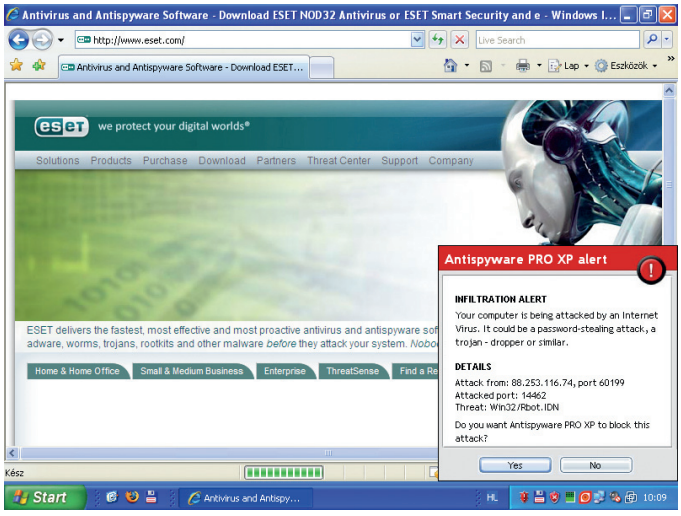
A cikkíráshoz szándékosan töltöttünk le egy Antispyware Pro XP programot, és ami a nagy érdekesség volt: maga a telepítő teljesen tiszta volt, sőt a **VirusTotal.com** oldalon vizsgálva mind a 37 biztonsági program néma maradt. A megoldás az, hogy a csalók egy üres, később külön oldalakról letöltögető vázat készítettek, amely az install közben kezdi el a kártékony kódokat telepítgetni különböző webcímekről. Ha „normális” vírusvédelmi program van a gépünkön, az azonnal képes megóvni minket a megpróbáltatásoktól. Itt különösen azok



Amikor a licencszerződés elutasítására egyáltalán nincs lehetőség. Vegyük észre, hogy nemcsak az a baj, hogy mindössze az OK gombot választhatjuk, de az ablak bezárására való X ikon is hiányzik

Az Antivirus XP 2008 egyik érdekessége, hogy a weboldalán olyan hamis Top 10 víruslistát közöl, amely a NOD32 programot készítő ESET laboratórium elnevezési metódusát használja

Mostanában a kémprogramirtók is a reneszánszukat élik, logikusnak látszik tehát, hogy ebből is készül hamisítvány. Ha végiggondoljuk, hány tájékozatlan átlagfelhasználó eshet áldozatul naponta, megértjük, mi motiválja ezeket az embereket: újabb regruták bővítik a pénzt hozó botneteket



A fertőzött gépen rendszeres időközönként megjelenik valamilyen támadásra figyelmeztető ablak. Ha kicsit viccesebbek lettek volna a készítők, jelezhettek volna támadást a nem létező 71546 portról is ☺

a felhasználók vannak a veszélyben, akik semmilyen, vagy nagyon elavult vírusirtót használnak.

Vigyázó szemetek Windowsra vessétek!

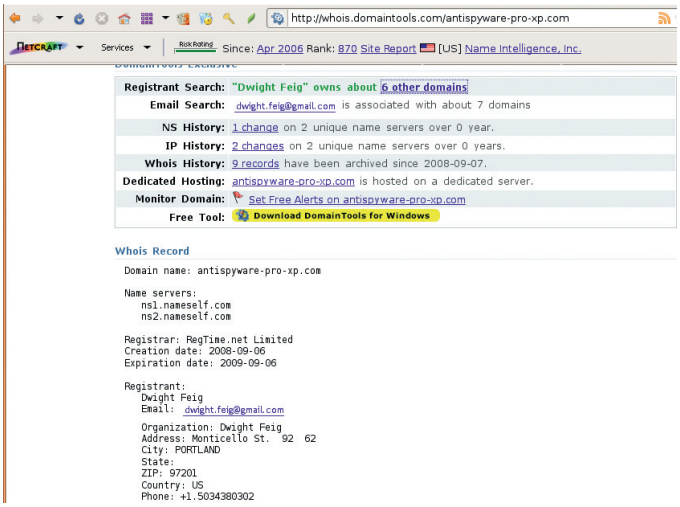
Ha már a gépen van, indul a színjáték. Sok esetben a számítógép ellenőrzése csak egy animáció, és mindig talál a végén fertőzést. Kifinomultabb esetben (a Spyware Pro XP is ilyen) végigpörgeti gépünk könyvtárait és csak utána jelez fertőzést, hogy hihetőbb legyen a dolog. Lényeg a lényeg, ettől kezdve bármit teszünk is, rendszeres időközönként felbukkannak ablakok, amelyek különféle nem létező vírusok, férgek és kémprogramok fertőzéseire figyelmeztetnek. Külön „vicc”, hogy a figyelmeztető ablakok kinézetét más kereskedelmi forgalomban is kapható vírusirtókból mintázták, így például Panda-szerű és NOD32-típusú figyelmeztető ablakot is láttunk már.

Jönnek a kéretlen felugró reklámok

A program ezt az ajtót is kinyitja, ettől kezdve kéretlenül érkeznek a különféle, hazai és külföldi oldalakról származó reklámok. Ebben talán a hazai lehet az igazi meglepetés, hiszen ez már valamiféle együttműködést is feltételez a résztvevő felek között.

Hamarabb utolérni, mint a sánta kutyát

Külön érdemes megemlíteni, hogy hazudós barátaink még külön supportot, azaz terméktámogatást is ígérnek, és ehhez a weblapjukon külön űrlap is felfedezhető. Bár a program bőszen hivatkozik a szinte sztahanovista 24/7 munkarendre, a weblapon nem találunk semmilyen elérhetőséget, felelős kapcsolattartót, telefont vagy e-mail címet, csupán egy egyirányú kapcsolatfelvételre alkalmas űrlapot, amelyen üzenni lehet, s amelyben megemlítik, hogy ha 12 óra múltán sem kapnánk választ, ismételjük meg a kérdést.



Ön vakon megbízna egy olyan biztonsági programban, amelynek weboldalát csak pár napja jegyezték be egy semmitmondó gmailes címről? Ahogy Virág elvtárs mondta: „az óvatosság nem bizalmatlanság!”

Megvenni nem érdemes

„Ha majom néz a tükörbe, nem nézhet vissza prófétá” – szól a mondás. Ennek fényében kár lenne arra várni, hogy egy (különben nem működő) adatbázis-frissítés, vagy a program fizetős változatának megvásárlása ránta-ná ki szekerünket a bajból. Bár a program fő célja, hogy vásárlásra serkentsen, hiszen a mentesítés sem működik, a gombra való kattintással csupán a terméket árusító oldalra jutunk. Talán egy mondattal összefoglalhatjuk a lényeget: ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google összes találata „How to remove...” szófordulattal kezdődik. Ennek olyan bölcsességgé kellene válnia fejünkben, mint annak, hogy az „okos pilóta alagútban nem katapultál”. Ha meg akarjuk óvni számítógépünket és személyes adatainkat, nem maradhatunk életünk végéig tudatlanok, naivak és potenciális áldozatok.

Cui prodest – kinek az érdeke?

Hogy mire megy itt a játék, egyszerű belátni: pénzkeresés felsőfokon. A többfrontos támadásnál sokféle veszítenivalónk lehet. Vagy kártevővel fertőződünk meg, és akkor nem a sok felbukanó ablak lesz a legnagyobb bajunk, hanem hogy a gépünk már egy zombihadsereg tagjaként spamlevelek terjesztésében és weboldalak elleni támadásokban vesz részt – tudtunkon kívül. Egy komolyabb méretű bothálózat (botnet) erejét tetemes összegért adják bérbe bűnözők. Emellett keresnek még rajtunk a kéretlenül megjelenített reklámok megjelenítéséért kapott pénzen. A support és a megrendelést feldolgozó modul egyben e-mail cím- és identitásgyűjtő is, ezek a személyes adatok külön, még banki adatok nélkül is eladható árucikkek. És végül, de nem utolsósorban, aki van olyan óvatlan, és megadja a hitelkártya-adatait a hamis vírusirtó vagy kémprogramirtó „vásárlásakor”, az egyben tálcán kínálja fel banki adatait a csalóknak és maradék pénzének is búcsút mondhat. Ez van, így működnek a dolgok, sajnos nem olyan naiv történet ez, mint egy Pöttyös Könyv vagy a Kisvakond meséje, hanem kőkemény érdekek vezérelte üzleti folyamat, ahol mindig résen kell lennünk.

***

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

www.eset.hu/virus
www.spywarewarrior.com/rogue_anti-spyware.htm
www.bleepingcomputer.com/malware-removal/rogue-programs
www.2-spyware.com/remove-antispyware-pro-xp.html