Adatlopás

Hitelkártyaszámok, bankszámlaszámok, e-mail postafiókok – semmilyen bizalmas adat sincs biztonságban a spyware-ek előtt. Tesztünkből kiderül, vajon melyik **ANTISPYWARE ESZKÖZ** véd ellenük.

Kinek mi jut eszébe az ilyen szoftverek nevei hallatán: XP Anti-Spyware 2009, AntiSpyCheck vagy Malware Alarm? Főleg, ha netezés közben találjuk meg őket? Valószínűleg az, hogy megint itt van három olyan program, amely az internet egyik rákfenéje, a spyware ellen nyújt védelmet. Csakhogy a valóság éppen ennek ellenkezője! Ezek a programok nemhogy megvédenének a kémprogramok ellen, éppen, hogy ők maguk azok. A készítők a valós programok nevei alapján nevezték el kártékony szoftvereiket, hogy a gyanútlan felhasználók telepítsék őket. Az első ilyesfajta szoftver 2003-ban jelent meg, azóta ez a technika a hackerek egyik kedvelt eszközévé vált. Manapság programok százai tettetik magukat vírusirtónak, vagy éppen kémprogramok ellen védelmet nyújtó alkalmazásnak, s kérik az azonnali telepítést a gépen lévő hamis vírusokra hivatkozva.

A szoftverek ezután kérik, hogy a kártevő végleges eltávolításához vásároljuk meg a program teljes verzióját. Nyilvánvaló, hogy aki beleesik a csapdába, az pénzéért nem egy jól működő szoftvert, hanem egy mindenre használhatatlan alkalmazást vásárol meg, és ez még a jobbik eset. Az is előfordulhat ugyanis, hogy a „vírusirtó" egy kémprogramot telepít fel gépünkre, hogy aztán érzékeny adatainkat a készítője számára eljuttassa.

Kémtechnikák

Azt egészen biztosan leszögezhetjük, hogy a hackerek nem a böngészési szokásainkra kíváncsiak. Ami őket igazán érdekli, azok a következők: hitelkártyaszámok, online banking adatok, felhasználói nevek, jelszavak, e-mail fiókok belépési adatai. Ezeket általában nem felhasználják, hanem eladják, de így is komoly pénzekre tehetnek szert. Felmérések szerint a feketepiacon akár 1000 dollárt is fizetnek egy bankszámla adataiért, míg a hitelkártyaszámok, e-mail fiókok belépési adatai 25–40 dollárt érnek. Nem csoda tehát, hogy manapság virágzik az online szervezett bűnözés, s a rengeteg klasszikus spyware, amelyek csak a felhasználók szokásait jelentették, már a múlté. Helyettük folyamatosan hirdetések ugrálnak fel, amelyek elsősorban a figyelemfelkeltést szolgálják, s ha rájuk kattintunk, akkor jutunk el a valódi kémprogramot tartalmazó oldalra.

Néha még arra sincsen szükség, hogy bármire is rákattintsunk, a letöltés és a telepítés automatikusan elindul a háttérben. Ezek nagyon ravasz dolgok, mert amellett, hogy a telepítés a felhasználó tudta nélkül indul el, akkor sem nagyon lehet ellene tenni, ha valahogyan észrevesszük, hogy mi folyik a „színfalak mögött". A spyware programok innentől kezdve beépülnek a rendszerbe, a Windows következő indításakor már automatikusan elindulnak – ráadásul az indító kód a registryben tárolódik, így nehéz megtalálni. A kártevő gyakran nem is egy, hanem több folyamatot indít el, amelyek egymást monitorozzák. Ha a felhasználó bármelyiket leállítja, a másik azonnal újraindítja az alkalmazást, illetve ezek a szálak figyelik a registry-bejegyzéseket is, és szükség esetén pótolják a törölteket. Így az eltávolítás gyakorlatilag megoldhatatlan feladat elé állítja a felhasználókat.

De nemcsak az eltávolítás, hanem a kémprogramok felismerése is egyre nehezebb. A hackerek ugyanis előszeretettel kombinálják a spyware és rootkit alkalmazásokat – utóbbi elterelésként funkcionál, meg persze remekül el tudja rejteni a valóban ártalmas folyamatokat, minden nyomukkal, még a registry-bejegyzésekkel együtt is. A rootkit előszeretettel bújik meg a kernelben, ahonnan remek rálátással van az egész rendszer működésére. A kernel felügyeli többek között a CPU-időt, a memória-hozzáféréseket, a hozzáférési jogosultságokat stb. És ez az, ami különösen ellenállóvá teszi őket.

Rootkit: elrejti a spyware-t

A hackerek a támadásoknál előszeretettel használják fel a kernel objektumokat. Az operációs rendszer ezeket adminisztrátori és ellenőrző funkciókra használja fel, például az aktív feladatok rendszerbe történő regisztrálásakor. A feladatkezelő hozzáfér az ehhez használatos protokollhoz, így könnyedén ki tudja listázni az éppen futó alkalmazásokat. Ha azonban a rootkit meg tudja változtatni →

TÉNYEK

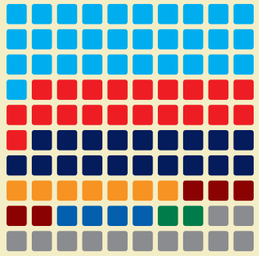
Christian Funk, a Kaspersky Lab Central Europe elemzője

Növekvő fenyegetettség

Amíg a klasszikus vírusok száma alig növekszik, a spyware alkalmazások száma egyetlen év alatt megnégyszereződött. És a növekedésnek addig valószínűleg nem is lesz vége, amíg van esély ily módon mások számláját használni. A legfontosabb dolog, amit a felhasználók tehetnek, hogy nem becsülik le a bűnözés e formáját.

ADATCSERE A FEKETEPIACON

A hackerek csak megszerzik és eladják az adatokat. A vevők azok, akik a számlák tényleges kiürítését végzik.

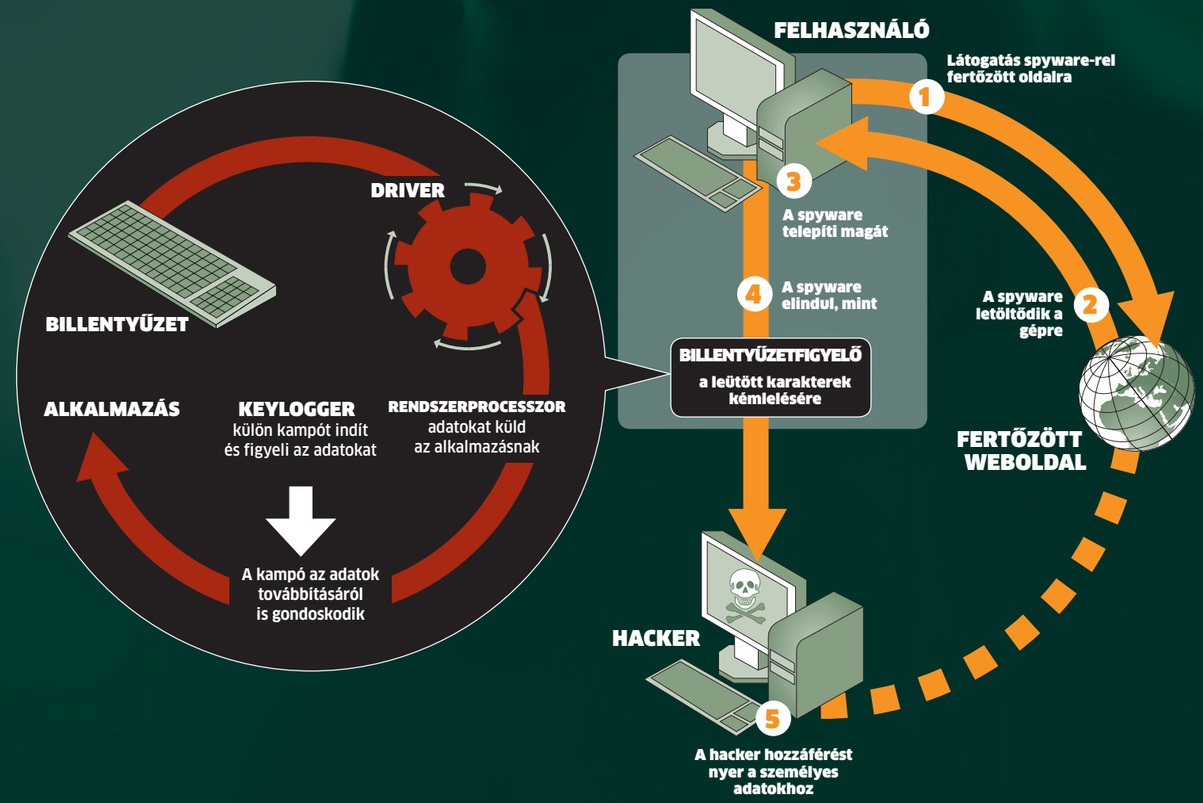


FORRÁS: SYMANTEC

31 % HITELKÁRTYA-ADAT
20 % BANKSZÁMLAADAT
19 % E-MAIL CÍM
7 % SZEMÉLYES INFORMÁCIÓ
5 % SZERVERHOZZÁFÉRÉS
4 % HACKELT PC
2 % ROSSZINDULATÚ KÓD
12 % EGYÉB

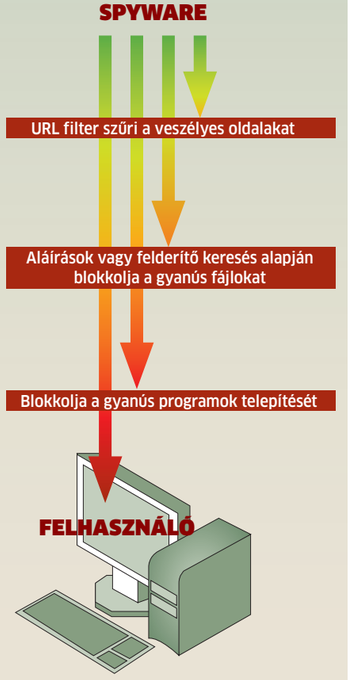
spyware-rel

Így működnek a spyware programok



Háromszintes védelem

Egy jó AV program egyszerre több szinten is figyel, hogy már a kártevők PC-re jutását is meg tudja akadályozni. Figyel internetezésnél, a webes fájlok letöltésénél és a programok telepítésénél is.



LEMEZMELLÉKLETEN

Spyware-védelem

AVG Anti Virus Free ►ajándék vírusirtó

DriveImage XXL ►HDD adatokat archiválja

Eset Smart Security 3.0 ►komplett csomag kiváló vírusirtóval

Gmer ►felderíti és törli a rootkit programokat

HijackThis ►átnézi a regisztryt rosszindulatú kódokat keresve

Recuva ►törölt adatokat állít vissza

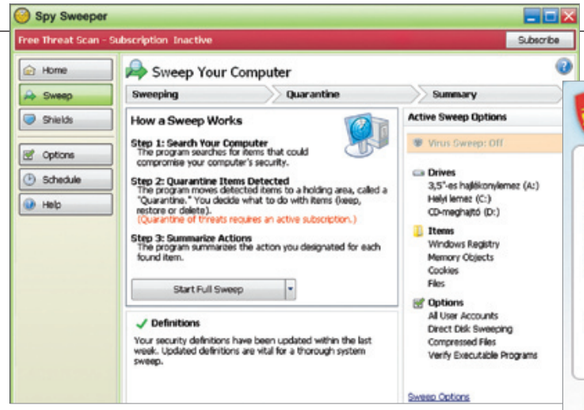
Sandboxie ►szoftvereket biztonságos környezetben futtat

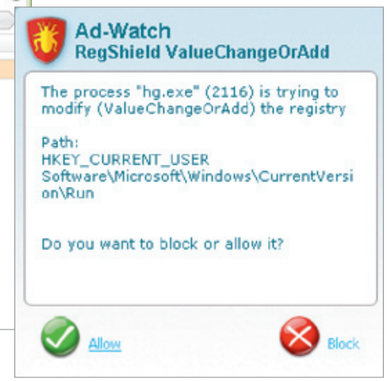
SpyBot Search & Destroy ►ingyenes kémprogramok elleni védelem

VirtualKeyboard ►virtuális billentyűzet billentyűzetfigyelők ellen

A CD/DVD-N: Minden programot megtalál a SPYWARE TESZT menüpontban.

Ál-antispyware Igazi átverés: a program vírusra figyelmeztet, és kéri a felhasználót, hogy vegye meg a vírusirtó teljes verzióját. Aki ezt megteszi, pénzt dob ki az ablakon, de rosszabb esetben spyware-t is letölthet





Tesztgyőztes A Spy Sweeper a legtöbb kategóriában az élen végzett, azonban ez sem elég arra, hogy egy vírusirtó nélkül tökéletesen megvédje gépünket a spyware alkalmazásoktól

Mit tegyünk? Számos antispyware alkalmazás ehhez hasonló figyelmeztetésekkel elbizonytalanítja a felhasználókat, amikor a felhasználó kezébe adják a döntést, ahelyett, hogy azonnal blokkolnák a gyanús programot

a kernelhez kapcsolódó információkat, ezt természetesen meg is teszi, oly módon, hogy a kémprogramokra vonatkozó infók eltűnjenek. Azaz, ha valaki spyware után kutakodna, semmit nem fog találni.

A kernelbe való beépülésnek azonban van még egy további „előnye" is. A Windows a rendszerfejlesztők számára engedélyezi, hogy egyes meghajtókhoz további szűrőket illesszenek, annak érdekében, hogy az illesztőprogramok funkcionalitását növelni lehessen, a driver újraprogramozása nélkül. Ez viszont egy biztonsági rés, hiszen a driverek nemcsak a hardverekhez és szoftverekhez való hozzáférésre jogosultak, hanem egyes rendszerfájlokhoz is hozzányúlhatnak. Ez egyfelől a valódi biztonsági programoknak ad lehetőséget gyanús aláírások, gyanús programok keresésére, másfelől viszont a rootkitek is „élvezhetik" a plusz jogokat: például, és ez nagyon fontos, kommunikációs csatornát nyithatnak a szoftver gazdája, a hacker felé. E szempontból a Vista sokkal biztonságosabb, a kernelhez például csak az aláírt és a felhasználó által hitelesített folyamatok férhetnek hozzá.

Ha azonban a spyware mégis a gépre került, az adatok biztonságát semmi nem garantálhatja. A billentyűzetfigyelők a legveszélyesebb programok közé tartoznak – a háttérben figyelnek, és minden leütést, sőt, időnként képernyőképeket is küldenek a gazdájuk felé. Ezen kívül rögzítik a látogatott weboldalakat, és azt is, hogy a felhasználó mely alkalmazásokat indította el. A keylogger dolga ezután már csak annyi, hogy akár a megnyitott csatornán, akár e-mailen keresztül elküldje az adatokat a hackernek.

A spyware-vadász

A spyware alkalmazások egyre kifinomultabb és ravaszabb működése a kémprogramok elleni szoftverek fejlesztőitől is hasonló megoldásokat követelnek. Tesztlaborunkban hat biztonsági csomagot vizsgáltunk meg. Elsősorban arra voltunk kíváncsiak, hogy menynyit fejlődött a helyzet az elmúlt időszakban, illetve nagy kérdés volt az is, hogy az antivírus alkalmazások jó eredménnyel veszik-e fel a harcot a spyware alkalmazásokkal szemben. Vagy esetleg szükség van külön erre szakosodott program használatára is?

Speciális tesztünkben az alkalmazásokat egy többszintes „tesztpálya" segítségével vizsgáltuk meg, amely a hatékonyságuk mellett az erőforrásigényt és a sebességet is mérte.

Felismerés: spyware-vadászat

Egy jó antivírus program kétféle módon is ki tudja szűrni a spyware alkalmazásokat, megelőzve ezzel azt, hogy a kártevő felkerüljön gépünkre. Az egyik egy URL-ekből összeállított feketelista, amely tartalmazza azokat a weboldalakat, ahonnan – felhasználók jelentései és saját vizsgálatok alapján – kártékony kód kerülhet a gépünkre. A lista alapján az AV program blokkolja a kérdéses weboldalakat, így azok egyáltalán nem töltődnek be.

A másik dolog a fájlrendszer figyelése: a különféle aláírások alapján a vírusok és más kártevők abban a pillanatban észlelhetők, amint a telepítő létre akarja hozni a fájlt. Tesztgépünkkel, amelyre Windows XP SP3-at telepítettünk, 200 olyan oldalt próbáltunk megnyitni, amelyek titokban spyware szoftvert akarnak gépünkre felcsempészni. Mivel URL listája csak a Spy Sweepernek van, ez a szoftver a többiekkel szemben előnyt élvezett. 24 olyan oldalt is blokkolt, ahol az aláírások alapján nem lehetett következtetni a spyware program jelenlétére. A többiek pusztán az adatbázisuk alapján dolgoztak, és kiábrándító eredményt produkáltak: egyikük sem blokkolta még csak a kártékony weboldalak felét sem. Leggyengébben a Spyware Doctor és a SpyBot teljesített, e két szoftver a fenyegetések kevesebb mint egy tizedét tudták kiszűrni. Még egyszer: ezek a szoftverek csak az aláírások és más egyéb működési jellegzetességek figyelése alapján dolgoztak, viszont azt így megállapíthatjuk, hogy a kártevők viselkedése alapján egyiküket sem tudja megbízhatóan kiszűrni a kémprogramokat.

Miután a kártevő a gépre került, elindul egy telepítési folyamat. Legalább ennek felderítése nem okozott komolyabb gondot – általában. A SpyBot valamennyi kísérletet blokkolta, a Windows Defender viszont alig néhányat – ez az oka annak, hogy a szoftver az utolsó helyre került a rangsorban.

A felderítés azonban még csak a kezdet, az alkalmazásoknak tudniuk kell blokkolni a folyamatot, és persze eltávolítani a kártevőt, kártevőket. E szempontból ismételten a Spy Sweeper mutatkozott a legjobbnak, de néhány hátránya ennek az alkalmazásnak is volt. A többiek esetében nagy hibának tartjuk, hogy túlságosan gyakran igényeltek felhasználói beavatkozást, rengeteg esetben a felhasználónak kell eldöntenie, hogy kémprogrammal áll-e szemben. Ráadásul, ha ilyenkor csak a telepítés megszakítását kérhetjük, az EXE fájl a gépen marad, így később még probléma forrása lehet.

Gyakran kaphatunk téves riasztást is – ennek tesztelésére tíz népszerű programot telepítettünk, köztük a Deamon Tools, Microsoft Office 2007, Adobe Reader és iTunes alkalmazásokat is. A Windows Defender és a Spyware Sweeper csont nélkül vette az akadályt, míg az Ad-Aware tízből hétszer riasztott. A Spy Sweeper megszakította az Adobe Reader és a Skype telepítését, az AntiSpyWare 2 pedig kifagyott az iTunes telepítése során.

Kártevők kiirtása: csupa csalódás

Rengeteg felhasználó csak akkor kap észbe, és kutat spyware-irtó alkalmazás után, amikor gépét már ellepték a kémprogramok. Éppen ezért a tesztben résztvevő alkalmazásokat próbára tettük tíz „előre telepített" kémprogrammal is – köztük néhány olyannal, amelyik registry-módosításokat is végzett.

Megdöbbentő és egyben csalódást keltő eredmény született: teljesen egyik résztvevő sem tudta megtisztítani a rendszert. Még a legjobban teljesítők is csak a kártevők felét tudták eltávolítani, számos indítható fájl, több registry-bejegyzés is a gépen maradt.

Tesztünk végkövetkeztetése ezzel teljesen egyértelmű: a vírusirtó alkalmazások jobb munkát végeznek, mint a külön kémprogramok eltávolítására specializálódott szoftverek. Bár ez mindenképpen csalódást keltő eredmény, annyi pozitívum azért van a dologban, hogy egy korszerű antivírus program mellé, úgy tűnik, nem szükséges kémprogram-eltávolítót telepíteni.

De vigyázzunk, az egyszerűbb programváltozatok, jellemzően az ingyenes verziók és a különféle hardverekhez mellékelt szoftververziók nem tartalmazzák azt a modult, amelyik a kémprogramok eltávolítását végzi! Esetükben a „kevés is több, mint a semmi" elvet követve erősen ajánlott a kémprogram-eltávolító használata.

Antispyware-teszt: Víruskeresővel jobban járunk, mint a speciális programokkal

	1. HELY	2. HELY	3. HELY	4. HELY	5. HELY	6. HELY
Termék	Spy Sweeper 5.8	Ad-Aware 2008 Plus	Spyware Doctor 6	SpyBot Search & Destroy	AntiSpyWare 2	Windows Defender
Fejlesztő	www.webroot.com	www.lavasoft.com	www.pctools.com	www.spybot.info	www.ashampoo.com	www.microsoft.hu
Tájékoztató ár	9000 Ft	7500 Ft	9000 Ft	ingyenes	9000 Ft	ingyenes
Értékelés	67	56	56	52	50	48
Felderítés letöltés közben (URL szűrő/aláírás alapján)	**20%/48%**	0%/19%	0%/10%	**0%/6%**	0%/29%	0%/38%
Felderítés telepítés közben (viselkedés/aláírás/egyéb alapján)	0%/80%/10%	0%/40%/30%	0%/80%/10%	**0%/10%/90%**	0%/10%/70%	**0%/20%/0%**
Felderített/blokkolt/törölt program telepítés során	**90%/60%/30%**	90%/40%/30%	90%/50%/20%	100%/60%/10%	80%/40%/0%	**20%/20%/0%**
Téves riasztás (figyelmeztetés/blokkolás)	30%/20%	**70%/0%**	**0%/0%**	50%/0%	50%/10%	**0%/0%**
Kártevők letiltása utólagos telepítésnél (teljes/részleges)	**50%/30%**	50%/20%	30%/30%	**20%/30%**	30%/30%	60%/0%

Csúcskategória (100–90) Felső kategória (89–75)
Középkategória (74–45) Nem ajánlott (44–0)
Értékelés pontszámokkal (max. 100)