



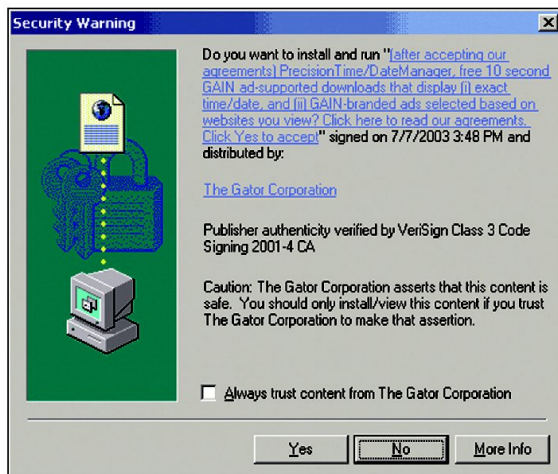
KÉRETLEN REKLÁMPROGRAMOK

Az nem lehet, hogy valami nem sörnyítő!

Sorozatunk nyolcadik epizódjában a kérértlen reklámprogramokról lesz szó. Azt már tudjuk, hogy ezek nem vírusok, és nem is férgek, sőt még kártevőnek sem szabad nevezni őket, mert különben vaskos pereket veszünk a nyakunkba. Jó lenne tudni, mennyire veszélyesek, hogyan kerülnek gépünkre, és főképp: miként szabadulhatunk meg tőlük? A cikk végére minden kiderül.

Nemcsak a vírusok, férgek és trójai programok veszélyeztetik mindennapjainkat, hanem kérértlen reklámprogramok és a számítógépes szokásainkat fűrkésző kémprogramok is lesben állnak. Létezik egy érdekes kategória, a greyware szoftverek. Ez a szürke

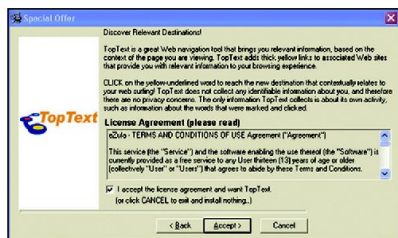
zóna: ide a legalitás és illegális peremén egyensúlyozó alkalmazások tartoznak. Ezek a veszélytelen szoftverek és a kifejezetten rosszul elgondolt kártevők közé esnek, és fajtájukat tekintve mint reklámprogramok (adware), kémprogramok (spyware) vagy nyomkövető programok



A Win32/Adware.Gator az egyik legrégebbi versenyző a kérértlen reklámprogramok mezőnyében

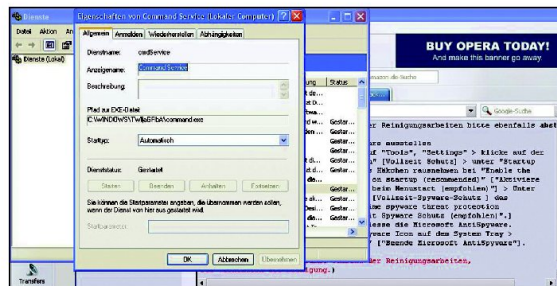


Ha kiválasztottuk a veszélyes alkalmazások keresése opciót, a Mr. és Mrs. Smith videofilmet védő Settec Alpha rootkit is felkoppán a NOD32 védelmén



(trackware) jelennek meg egyre nagyobb számban az interneten. Némely vírusvédelmi kereskedő óvatossággal hívja őket: PUP (Potentially Unwanted Programs) – magyarul valószínűleg felesleges vagy kérértlen programok. Ez az új kategória azért nyerhetett létjogosultságot, hogy elkerülhetők legyenek az olyan törvényes bonyodalmak, ahol a gyártók azt vitathatják, törvényes-e a szoftverük,

Amikor a felhasználó maga egyezik bele figyelmetlenül – íme az Ezula licen szerződése



A Command Service sem egy átlagos szereplő: megpróbál eltávolítani minden más reklámprogramot gépünkől (eddig örülnék) azért, hogy aztán egyedül terpszkedhessen rajta, és jelenítsen meg hirdetéseket (mégsem lesz a barátunk)

vagy sem; illetve törvényes-e, hogy a vírusvédelmi alkalmazások kártevőnek jelölik meg az ő kétes programjukat. Néhány esetben ráadásul legális szoftverekben is előfordulhat ilyen szoftver-„csatolmány”. Ezek legális vagy rosszindulatú mi voltuk szintén a rejtőzködés mértékétől függhet. Amíg a jelenlétük néha egészen nyilvánvaló, például jönnek a felugró (pop-up) ablakok, váratlan helyekre irányít bennünket a webböngésző, és így tovább – szinte mindig komoly figyelmet fordítanak arra, hogy megakadályozzák tényleges állományaik észlelését és eltávolítását. Némelyek ezt úgy kommentálják, hogy ezen a terepen lehet a rootkit vagy rootkitjellegű technológiát legális célokkal is használni, és így módon valóban legyőzhetők az operációs rendszerek hiányosságai, amikor az adatok elrejtéséről van szó.

„Jóindulatú” reklámprogramok

Vitatható a védelmi cégeknél ez a különbségtétel a reklám- és a kémprogramok között, ha az ember a törvényesség határán egyensúlyoz. Ujraalkotva a „greyware” fogalmát, és általánosabb magyarázattal élve a megkülönböztetés kihangsúlyozására, a NOD32 lényegesen részletesebb irányítási lehetőséget adott a felhasználók kezébe már a korábbi verzióktól kezdődően, és még pontosabban írja le ezt az egyre homályosabb területet.

Néhány reklám- és felhasználói aktivitást követő vállalat arról panaszkodik, hogy a felismerők szoftverüket reklám- vagy kémprogram-

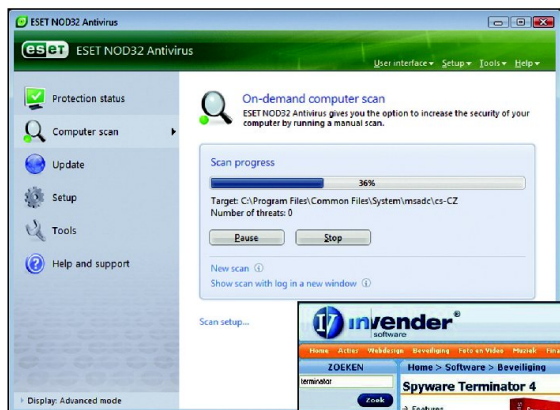
ként azonosítják. A NOD32 már a 2.7-es változatában bevezetett egy új felismerési kategóriát Kérértlen alkalmazások (Potentially Unwanted Applications) néven. Ide tartozik minden reklámjellegű alkalmazás, amely nem szükségképpen rosszindulatú; működésüket egy felhasználói licen szerződés (EULA) figyelemmel elofogadásakor mi magunk engedélyeztük, létezik hozzá uninstall lehetőség és így tovább. Bár nem mindig rosszindulatú, az adware általában feleslegesen terheli a számítógépek tároló- és memóriakapacitását, ami hátrányosan hat annak teljesítményére, megbízhatóságára és stabilitására. Ezzel még nem okoz biztonsági kockázatot, de önmagában is rendkívül felhasználó számára.

Vitatható adware-technikák

Rádásul néhány állítólagos reklámprogram esetében erősen megkérdőjelezhető módszereket használnak mind a felhasználók tájékoztatásakor, mind pedig a program telepítésekor. Az ilyen reklámprogramok hosszú (kinyomtatva akár több tucat oldalas) és bonyolult megfogalmazású felhasználói licen szerződést tartalmaznak. Olyan összetevőket is magukban foglalhatnak, amelyek a működési környezetben jogosultságot változtatásokat visznek véghez, csendesen telepítik magukat, sőt felügyelhetik az



A cikkben jelzett ingyenes programok megtalálhatók a lemez mellékletben



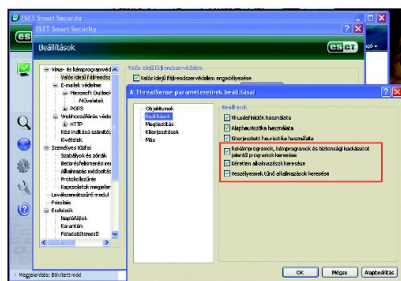
Gyanú esetén ne sajnáljuk az időt, illetve a fáradságot, és végezzünk egy teljes vírus- és kémprogram-ellenőrzést, minden opciót bekapcsolva

esetleges eltávolítási kísérleteket is – ekkor észrevétel nélkül újratelepíthetnek, vagy pedig egyáltalán nem, vagy csak alig működő uninstallálási lehetőséget nyújtanak.

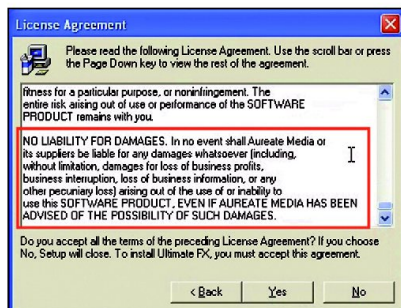
Biztonságos?

A NOD32 ezekre is már egy átkeresztelt kategóriát alkalmaz, a korábbi Valószínűleg veszélyes alkalmazás (Potentially Dangerous Applications) helyett a Valószínűleg nem biztonságos alkalmazás (Potentially Unsafe Applications) elnevezés szerepel. Ez a kategória tartalmaz minden ke-

reskedelmi forgalomban megjelent billentyűűtés-naplózót (keylogger), távoli adminisztrációt lehetővé tevő alkalmazást (remote administration tools), IRC-csevegőkliens programokat és minden olyan eszközt, amelyet eredeti rendeltetésüktől eltérően rosszindulatú célra is használhat-



A NOD32 és a Smart Security is képes szűrni a különböző kártevő alkalmazási kategóriákat – ezt az opciót viszont nekünk kell bekapcsolni!



Mintha Hamupipőkének kellene kiválogatni a lencsét a hamuból. Aki a sokoldalú szerződésben észreveszi a gyanús kitételt – ahelyett hogy automatikusan rákattintana a NEXT gombra –, annak észinté elismerésünk

alkalmazást: példánkban ez most az Ultimate FX Painter rajzprogram lesz.

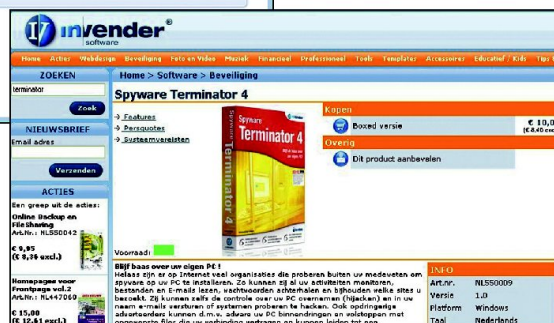
Természetesen gépünkön fut vírus-irtó, naprakész adatállományokkal. Mint azt korábban már említettük, a NOD32 lényegesen részletesebb irányítási lehetőséget ad a felhasználó kezébe a törvényesség határára egyensúlyozó kétes reklám- és kémprogramok esetén, így mód nyílik a veszélyes alkalmazások, a kértlen alkalmazások és külön a reklám- és

mazások keresése opció szintén hasznos lehet, különösen rootkites védelmek esetében – annak idején a Mr. és Mrs. Smith videofilmnél azonnal felismerte a kártevőt. Alig, hogy elindítjuk a második telepítést, azonnal kapjuk a riasztási ablakot, sőt többit is, hiszen az Adware Aurate minden komponensét azonosítja.

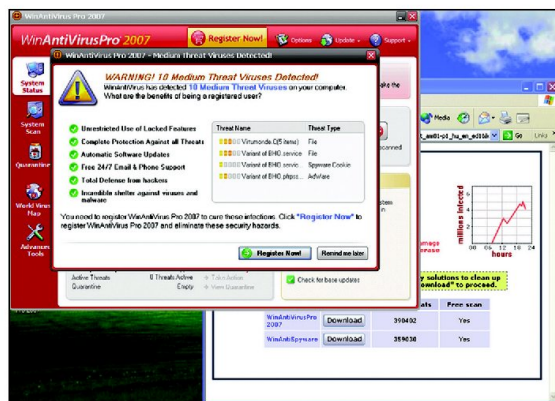
A reklámprogramok irtása, illetve törlése után két eset lehetséges. Az eredeti program működőképes marad, de az is elképzelhető, hogy a reklámprogramok épségét figyelve megtagadja az üzemszerű működést. Most szerencsénk volt: a rajzprogram a mentés után tökéletesen működik, és a nemkívánatos reklámprogramoktól is sikeresen megszabadultunk.

Összefoglalás

Az adware és az ehhez hasonló programokat tehát a NOD32 nem nevezi kártevőnek, nehogy jogi problémákba ütközzön, de azért képes hatékony védelmet nyújtani ellenük. Mindamellett nem árt tudni, hogy számos legálisnak mondott szoftver



Ez a Spyware Terminator nem az, amit mindenki ismer. A csupán hasonló nevű holland termék egy család alkalmazás, amely ráadásul még kémkedik is utánunk



A Virtumonde trójai futása közben különféle kértlen felnyíló ablakokat jelenít meg, és megkísérel néhány további kártevő komponens letölteni

kémprogramok keresésére is. A kísérlet első részében az állandó védelem beállításánál a reklám- és kémprogramok elleni védelmet nem kapcsoljuk be. Indulhat a telepítés, és itt már is egy fontos momentumhoz érkezünk: tíz emberből kilenc nem szokta alaposan végigolvasni a felhasználói licencszerződést, pedig sokszor már itt is le van írva, hogy az ingyenesséért cserébe reklámok megjelenítését kell elviselnünk. Így esetünkben sem titokban települ a kértlen reklámkomponens, az Aurate, hanem a felhasználó jóváhagyására, még ha az figyelmen kívül volt.

Szedjük le tehát a programot, majd telepítsük újra, ezúttal azonban a valós idejű védelemmel választjuk ki a reklám- és kémprogramok elleni modult is. Érdemes megjegyezni, hogy az úgynevezett veszélyes alkal-

is képes jelentős sebezhetőségeket okozni egy PC-n.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemen@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivirus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Az ESET honlapja: www.eset.eu
A NOD32 magyar honlapja: www.nod32.hu
Az „adware” a Wikipédián: en.wikipedia.org/wiki/Adware