Számítógép kártevők - védekezés

MalWare = Malicious Software

Kártevők típusai

A kártevő olyan szoftver, amely **a felhasználó tudta nélkül megpróbál bejutni a rendszerbe**, és felhasználja azt saját maga **továbbterjesztésére**, miközben egyéb **kártékony** tevékenységet is végrehajt.

- **Vírusok**
  Végrehajtható file-hoz kapcsolódó önreprodukáló program
- **Makró vírusok**
  A Word és Excel ***dokumentumokba úgy nevezett makrokat***, - Basic nyelven írt ***futtatható (akár káros) program elemeket - lehet betenni***, melyek a dokumentum megnyitásakor aktivizálódhatnak. ***A makro akkor vírus, ha káros a működése.***
- **Férgek**
  A számítógépes féreg olyan ***kártevő kódot tartalmazó program***, amely hálózatba kötött számítógépeket támad meg, és a ***hálózaton terjed***. A vírus és a féreg között az az alapvető különbség, hogy a férgek ***önállóan képesek replikálódni és terjedni***.
- **Trójaiak**
  Hasznosnak látszó – a felhasználó számára kívánatos funkciókat tartalmazó ***program, amely mást is csinál, mint amit eredetileg magáról állít. Rombolja a gép szoftver erőforrásait.***
- **Rootkitek**
  A Rootkit ***olyan szoftver eszközök együttese, melyet a rendszer irányításának átvétele után arra használnak, hogy a rendszer működésébe avatkozzanak***. A támadónak hozzáférést biztosítanak a rendszerhez, miközben jelenlétüket elrejtik.
- **Spam**
  Kéretlen levelek, melyek „levélszeméttel“ telítik a levelező rendszert.
- **Reklámprogramok**
  Az olvasandó web lap információt gyakran kitakaró reklám célú programok.
- **Kémprogramok (SpyWare)**
  A spyware programok információkat gyűjtenek a felhasználó tudta nélkül és a gép irányításába akarnak bekapcsolódni. (Pl. billentyű leütés figyelő, jelszó lopó stb.)
- **Veszélyes alkalmazások.**
  Olyan hasznos programok melyek rossz kezekben bűnös célokat szolgálhatnak. (Pl. a távoli hozzáférést biztosító eszközök)

Számítógép vírusok (szűkebb értelemben)

A vírus önreprodukáló program, amely saját másolatait egy másik végrehajtható file-ba vagy dokumentumba helyezi be, azt fertőzi meg. Terjedését tekintve hasonlít a biológiai vírushoz, amelyik élő sejtbe települ be, így szaporítja magát. A vírus betelepedhet a felhasználói programokba, rendszerprogramokba, pendrive-ok boot szektorába, vagy dokumentum file-okba makróként.

A végrehajtható programba települt vírus akkor fut, ha a programot elindítják, a boot vírus a gép indulásakor, a makro vírus akkor, ha a dokumentumot megnyitják.

A vírus lehet szándékosan káros, vagy csak bosszantó. Manapság a vírusokat legtöbb esetben haszonszerzési céllal készítik (pl. zsaroló vírus), az ezzel foglalkozó bűnözői csoport megbízásából.

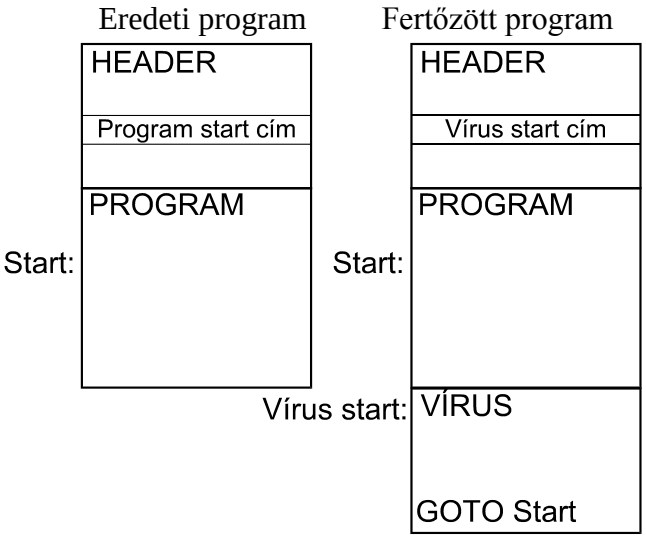
A vírus gyakran késleltetett hatású, működése valamilyen dátumhoz, vagy cselekményhez kötődhet, például akkor jelez, ha a fertőzés egy adott szintet elér. Az ilyen vírust időzített, illetve logikai bombának nevezik.

A vírus egyrészt megfertőzi azt a gépet, melybe belejut, másrészt programok átadásával terjed. A program vírus és a boot vírus a DOS-os korszak jellemző kártevője.

Az első PC vírus 1986-ban jelent meg, boot vírus volt, neve Brain, két pakisztáni fivér hozta létre.

Nem rezidens vírusok

Végrehajtható programokhoz kapcsolódnak:



A vírus program feladatai:

- végrehajtható file-ok keresése
- annak vizsgálata, hogy a file már fertőzött-e
- a megtalált file fertőzése a fent vázolt módon (start címke mentése, módosítása, vírus program hozzáfűzése az eredetihez, benne ugrás az eredeti start címkére).
- valamilyen akció végrehajtása (például péntek 13-án egy üzenet kiírása).

Védekezés a vírus ellen:

- vírus program mintájának felismerése
- a program hosszának figyelése – gyors, minden gép indításkor végrehajtható
- a program tartalmának figyelése valamilyen ellenőrző szám segítségével (pl. a program kód összes byte összeadása és összehasonlítása a vírus mentes esettel.)

Támadás a védekezés ellen:

- a vírus nem a program végére települ, hanem beépül a program file ki nem töltött részeire (ilyenek a nem iniciált adat területek), így a program hossza nem változik
- a vírus változtatja mintázatát, azaz magát a vírus programot. Ennek lehetőségei:
  - egyszerű változtatás: egyes feladatok elvégzésére több eljárás van, és fertőzéskor ezek hívása variálódik
  - a program kód átkódolása véletlenszerűen változó kulccsal. Futás előtt a vírus visszaállítja a kódot. A dekódoló programrész azonosítható

- a polimorfikus vírusban a dekódoló modul is fertőzésenként változik, így a minta alapján nem azonosítható
- a metamorfikus vírus fertőzéskor teljesen újra írja saját magát. Ezek nagyon bonyolult kódok, például a W32/Simile vírus program 14000 forrás sorból áll (ez kb. 280 oldal).

A polimorfikus vírusok ellen u.n. heurisztikus víruskereséssel védekeznek, azaz rá akarnak jönni, hogy egy program résznek a kód átalakítása-e a célja. Elő szokott fordulni mellétalálat, azaz hasznos programot minősítenek vírusnak.

Internetes kártevők

Az interneten keresztül hivatalból kaphatunk a saját gépünkön futó programokat:

- ***Egy HTML dokumentumban gyakran van futó kód*** (tipikusan valamilyen effekt). De a kód akár káros is lehet. ***Ezért egy ismeretlen weblap megnyitása is veszélyes lehet***.
- ***Az e-mail melléklete is lehet futó kód, amely az e-mail megnyitásakor automatikusan elindul***, például egy születésnapi üdvözlet zenét kezd játszani.

Ezekben a programokban lehetnek kártékony komponensek, melyek saját gépünk erőforrásait akarják rombolni. Ezek elleni ***védekezések***:

- meg lehet tiltani az interneten érkező programok futását. Ennek több szintje lehet (soha ne fusson, csak bizonyos programok futhassanak, csak engedélyezés után fusson...)

- meg kell védeni a gép saját erőforrásait az interneten érkező kártevőktől. Ez alapesetben elvileg megy, hiszen a korszerű operációs rendszerekben a felhasználói taszkok a többi taszktól izolálva futnak, és a rendszert elvileg nem tehetik tönkre. ***A kártevők az u.n. biztonsági hézagokon keresztül törnek be a gépbe*** (ld. JPEG vírus).

Ezeket a biztonsági hézagokat folyamatosan dokumentálják és javítják. Ezért is kell a ***Windows rendszerekben az egyébként automatikusan végrehajtható frissítéseket rendszeresen el kell elvégezni.***

JPEG vírus (2006)

JPEG file-ban is el lehet rejteni vírust, amit a vírus figyelők nem vesznek észre, mert nem is feltételezik, hogy ez előfordulhat.

A vírus azt használja ki, hogy egy JPEG file-ba megjegyzést lehet beszúrni. Az üzenet elején az üzenet hossza + 2 van (2 byte-on az üzenet hossza, utána az üzenet). Ha üzenet hosszként 0 vagy 1 van megadva, akkor a JPEG olvasó program a tényleges üzenethosszat -2-nek vagy -1-nek veszi, majd ezt 32 bites előjel nélküli számmá konvertálja, így kb. 4GByte-os üzenetet próbál olvasni, amitől elszáll, de közben már beolvasta az üzenetben lévő kódot, ami futó kód is lehet. Ez a biztonsági rés Windows frissítéssel könnyen javítható, de újabb tanulsággal szolgál: ne nézegessünk ismeretlen dokumentumokat.

Nehéz védekezni a gép kezelője által szándékosan betöltött kártevők ellen. Bármilyen program, amit a gépre telepítünk, tartalmazhat kártevőket, hiszen a programot azért telepítjük, hogy az a gép erőforrásait kezelje, így a programban lévő káros komponens is tud működni.

Trójai

Hasznosnak látszó – a felhasználó számára kívánatos funkciókat tartalmazó ***program, amely mást is csinál, mint amit eredetileg magáról állít. Rombolja a gép szoftver erőforrásait.*** Végtelen sokféle képzelhető el, a lényeg az, hogy egy ***spam-ben (kéretlen üzenet) kínált programot nagy gyanakvással kell fogadni***.

Féreg (worm)

A vírushoz hasonlóan **önreprodukáló program**, de **nem másik programhoz kapcsolódik**, hanem **önállóan tud szaporodni. Egy hálózaton keresztül képes továbbküldeni magát, így már ezzel árt a hálózatnak, mert *fogyasztja a sávszélességet***. A féreg persze **a vírushoz hasonlóan rombolást is végez**.

Makró vírusok

Az 1990-es évek közepétől a makro vírusok váltak általánossá. A **Word és Excel dokumentumokba Basic nyelven írt futtatható (akár káros) program elemeket lehet betenni**, melyek a dokumentum megnyitásakor aktivizálódhatnak. A makro értelme kétféle lehet:

- a megnyitáskor meginduló program valamilyen effektet generál
- bővül a Word vagy Excel eredeti utasításkészlete, például új parancsgombok jelenhetnek meg, így a dokumentum működő programmá válik, amely parancsa különböző műveleteket hajt végre, mondjuk egy szövegben talált szóhoz egy szótárból kikeres egy másik szót, és az eredetit helyettesíti.

A Microsoft windows-os rendszerekben szinte bármi berakható a makrókba, így a számítógépre káros működés is, ami anélkül indul el, hogy erről tudnánk.

Fő terjedésük: e-mailek csatolt állományaival.

A makró vírus elleni legegyszerűbb védekezés, hogy egy file megnyitása előtt az Excel vagy Word megkérdezi, hogy az abban lévő makróval vagy anélkül nyissa-e meg a file-t. A használati utasítás: soha ne engedélyezzünk nem garantáltan biztonságos makrókat, még egyszerűbben: a másoktól kapott dokumentumot csak makró nélkül nyissuk meg.

Kémprogramok (SpyWare)

A spyware programok **a gépre felkerülve információkat gyűjtenek a felhasználó tudta nélkül és a gép irányításába akarnak bekapcsolódni.**

A cél általában az, hogy ez a beavatkozás más számára előnyöket adjon, például:

- kémkedés, a gép futásáról, a benne lévő erőforrásokról információ kiküldése. A hétköznapi felhasználó számára legveszélyesebbnek hangzó az, amely **a képernyő állapotát és a billentyűzet kezelést kémleli**, hiszen így rossz esetben pénzügyi tranzakciók, **jelszavak figyelhetők** meg, és utána hamis tranzakciók indíthatók máshonnan. (Ez ellen banki rendszerben használt védekezés: a bank SMS üzenetet küld a felhasználó mobiltelefonjára, amire szükség van a pénzügyi tranzakciókhoz.)
- pop-up hirdetések küldése
- Web-böngészés monitorozása kereskedelmi célból
- a gép rávevése arra, hogy spam-eket küldjön
- http kérések küldése hirdetési oldalakra, azért hogy a hirdetési oldal forgalma látszólag nőjön.

Természetesen a gépen lévő *file-ok ellopása* is okozhat gondot (*bizalmas dokumentumok, fényképek*), de inkább csak „fontos” embereknél, vagy cégeknél.

A spyware programok jelenleg az egyik legnagyobb károkozónak számítanak. Az eddig felsorolt hatásokon túlmenően nagyon lelassíthatják a gépet, akár kezelhetetlenné téve azt.

Mérések szerint a PC-k kb. 70%-a fertőzött spyware-rel.

Anti-spyware programok: felderítik és kiirtják a gépen futó spyware-t. Például: SpyBot.

Rootkit

A Rootkit olyan szoftver eszközök együttese, melyet a rendszer irányításának átvétele után (ld. Spyware) arra használnak, hogy a rendszer működésébe avatkozzanak.

A rootkitek olyan a számítógépünkön megbúvó kis programocskák, melyek a tudtunk nélkül általában káros tevékenységet folytatnak, miközben mi gyanútlanul a szokásos módon használjuk a gépünket.
A rootkitek gyakran az operációs rendszer szokványos programjainak működését utánozva, annak helyébe lépve dolgoznak, el is végzik annak feladatait, de közben csinálnak még valami mást is, például adatokat szolgáltatnak ki gépünkről, vagy éppen hátsó ajtót nyitnak valaki más számára, hogy észrevétlenül kutakodjon.
Előfordulhat az is, hogy gépünk egy rootkit segítségével részévé válik egy spam- vagy vírusküldő hálózatnak, vagy más számítógépes bűncselekmény elkövetésére használják fel.

Spam

Mesterségesen gerjesztett nagy mennyiségű forgalom az interneten. Leggyakoribb formája az e-mail spam: a kéretlenül megjelenő hirdetések. Mostanában két leggyakoribb formája: olcsó szoftver vagy áru hirdetése. A hasznos levélforgalom 10-szerese is lehet. Spam címkeresési technikák:

- nyilvános honlapokon e-mail címeket kereső programok. ***Akinek címe hozzáférhető az interneten, biztos lehet benne, hogy elárasztják szeméttel*** (ilyen például egy egyetemi oktató).
- címlisták kiolvasása (ez ilyenkor spyware).

A spam küldésnél figyelhetik a címzett szokásait a WEB böngészést monitorozva.

Lánclevél (ez is spam)

„Ezt az üzenetet küldd tovább…” vagy „A Moszkva téren sebességmérő radarokat helyeztek üzembe…” tartalmú e-mail-ek, melyeket az olvasók általában továbbküldenek. Kétféleképpen okoz kárt:

- forgalmat gerjeszt
- munkaidőt vesz el. Legyen egy vállalatban csak 60 PC, mindenki csak fél percig foglalkozik a levéllel. Ez kb. 2000-4000 Ft kár.

DOS támadás

(DOS = Denial of service = Kiszolgálás visszautasítása)

A DOS támadás megakadályozza, hogy egy szolgáltató a hozzá érkező kérésekre reagálni tudjon.

Leggyakoribb formája az, **hogy a WEB oldalt elárasztják fals kérésekkel**, így eltömődik, és a normális kérésekre sem tud reagálni. Ez nagy anyagi kárt okozhat a Web oldal üzemeltetőjének. A támadás általában Zombi gépeken keresztül történik: fertőzött gépek küldik a nagy mennyiségű e-mailt.

DOS előfordulhat a népszerűség nem várt növekedése miatt is, például valamilyen szenzációs hírhez megadják azt a címet, ahol részletes információ található.

Másik lehetőség, hogy a egy rossz formátumú üzenettel lefagyasztják a gép operációs rendszerét. Például a Nuke támadás olyan hibás formátumú vagy rosszul tördelt csomagot, általában ICMP-t (Internet Control Message Protocol) küld, amely bug-ot (poloska=számítógép program hibás működése) idéz elő a megcélzott számítógépben, és tönkreteszi annak futását.

Tűzfal

[Windows 7 súgó]

A tűzfal **olyan szoftver vagy hardver, amely ellenőrzi az internetről vagy hálózatról érkező információkat, és a tűzfal beállításaitól függően blokkolja vagy továbbengedi őket** a számítógépre.

A tűzfal segít megakadályozni, hogy a támadók vagy rosszindulatú programok (például férgek) hozzáférjenek a számítógéphez a hálózaton vagy az interneten keresztül. A tűzfal megakadályozza azt is, hogy a számítógép rosszindulatú szoftvereket küldjön más számítógépekre.

[Windows XP súgó]

A tűzfalak a számítógép biztonságának növelésében segítenek. Korlátozzák a más számítógépekről érkező adatokat, így szabályozhatóvá teszik az adatok elérését, továbbá védelmet nyújtanak azon személyek és programok (például vírusok és férgek) ellen, akik és amelyek jogosulatlanul próbálnak a számítógéphez hozzáférni.

A tűzfal felfogható egyfajta határállomásként, amely ellenőrzi az internet vagy a hálózat felől bejövő adatokat (azaz *forgalmat*), és beállításaitól függően bizonyos adatokat visszafordít, másokat továbbenged a számítógép felé.

A Microsoft Windows XP Service Pack 2 (SP2) rendszerben a Windows tűzfal alapértelmezés szerint bekapcsolt állapotban van. (A számítógépgyártók és a hálózati rendszergazdák azonban kikapcsolhatják.) Nem feltétlenül kell a Windows tűzfalat használnia, tetszőleges tűzfalat telepíthet és futtathat. Mérlegelje a különféle tűzfalak által nyújtott szolgáltatásokat, és állapítsa meg, hogy igényeinek melyik termék felel meg leginkább. Ha úgy dönt, hogy másik tűzfalat telepít és futtat, kapcsolja ki a Windows tűzfalat.

A szolgáltatás működése

Ha valaki az internet vagy a hálózat felől megkísérel csatlakozni a számítógéphez, ezt a kísérletet „kéretlen kapcsolatnak” nevezzük. Ha a Windows tűzfal ilyen kéretlen kapcsolatra tett kísérletet észlel, blokkolja a kapcsolatot.
Ha olyan programot futtat, amelynek működéséhez adatok fogadására van szükség az internet vagy az intranet felől (ilyen programok például az azonnali üzenetküldő szolgáltatások vagy a többszereplős hálózati játékok**), a tűzfal megkérdezi, hogy engedélyezi, vagy blokkolja a kapcsolatot**. Ha az engedélyezés (azaz a blokkolás feloldása) mellett dönt, a Windows tűzfal *kivételt* hoz létre, hogy a program a továbbiakban zavartalanul fogadhasson bejövő adatokat.

Ha például azonnali üzenetküldési kapcsolatban áll valakivel, aki egy fájlt (például egy fényképet) szeretne küldeni, a Windows tűzfal megkérdezi, hogy feloldja-e a kapcsolat blokkolását, és engedélyezi-e a fénykép megérkezését a számítógépre. Vagy ha ismerőseivel többszereplős hálózati játékban szeretne részt venni az interneten keresztül, a játékot kivételként definiálhatja, hogy a tűzfal engedélyezze a játékkal kapcsolatos adatok fogadását a számítógépen.

Jóllehet a Windows tűzfal bizonyos internetes vagy hálózati kapcsolatok esetén kikapcsolható, ez növeli a kockázatát annak, hogy a számítógép biztonsága esetleg sérülhet.

Amire a Windows tűzfal alkalmas, és amire nem

Amire alkalmas:	Amire nem alkalmas:
Segít megakadályozni azt, hogy vírusok és férgek kerüljenek a számítógépre.	**Nem észleli és nem tiltja le a vírusokat és a férgeket,** ha már elérték a számítógépet. E célból víruskereső szoftvert kell telepíteni és rendszeresen frissíteni; a víruskereső megakadályozza, hogy vírusok, férgek és a biztonságot fenyegető egyéb tényezők kárt tegyenek a számítógépben, vagy a számítógépet vírusok terjesztésére felhasználják.
A felhasználó engedélyét kéri bizonyos csatlakozási kérések blokkolásához vagy engedélyezéséhez.	**Nem akadályozza meg veszélyes mellékletet tartalmazó e-mailek megnyitását.** Ne nyisson meg ismeretlen forrásból érkező e-mail mellékleteket. Akkor is legyen elővigyázatos, ha ismeri az e-mail küldőjét, és megbízik benne. Ha ismerőse küld Önnek e-mail mellékletet, megnyitása előtt vizsgálja meg a tárgy sorát. Ha a tárgy értelmetlen, kérdezze meg a feladót.
Kérésre létrehoz egy rekordot (biztonsági naplót), amelyben rögzíti a számítógéphez érkező sikeres és sikertelen csatlakozási kéréseket. A napló segítséget nyújt a hibaelhárításhoz.	**Nem blokkolja a szemétlevelek vagy kéretlen e-mailek** beérkezését a számítógépre. Ehhez egyes levelezőprogramok nyújtanak segítséget. További információkért olvassa el a levelezőprogram dokumentációját.

ESET NOD32 Antivirus program HELP részletek (olvasmány)

Kártevők típusai

A kártevő egy olyan szoftver, amely a felhasználó tudta nélkül megpróbál bejutni a rendszerbe, és felhasználja azt saját maga továbbterjesztésére, miközben egyéb kártékony tevékenységet is végrehajt.

Vírusok

A számítógépes vírus olyan fertőzés, amely fájlokat rongál meg a számítógépen. A vírusok a biológiai vírusokról kapták a nevüket, mert hozzájuk hasonló technikákkal terjednek egyik számítógépről a másikra.
Elsősorban alkalmazásokat és dokumentumokat támadnak meg. Úgy replikálódnak, hogy „törzsüket" hozzáfűzik a célfájl végéhez. A vírusok működése dióhéjban a következő: a fertőzött fájl betöltése után a vírus (még az eredeti alkalmazás előtt) aktiválódik, és elvégzi meghatározott feladatát. Az eredeti alkalmazás csak ez után indul el. A vírus csak akkor képes megfertőzni a számítógépet, ha a felhasználó (véletlenül vagy szándékosan) futtatja vagy megnyitja a kártékony programot.

A számítógépes vírusok tevékenységüket és súlyosságukat tekintve igen változatosak. Némelyikük rendkívül veszélyes, mert képes szándékosan fájlokat törölni a merevlemezről. Ugyanakkor vannak vírusok, amelyek nem okoznak valódi károkat, egyetlen céljuk, hogy bosszantsák a felhasználót, vagy fitogtassák szerzőjük műszaki jártasságát.

Fontos megjegyezni, hogy a vírusok (a trójaiakkal vagy a kémprogramokkal összehasonlítva) egyre inkább a ritkaság kategóriájába tartoznak, mert anyagilag nem jelentenek vonzerőt a kártevő szoftverek szerzőinek. Magát a „vírus" kifejezést pedig az összes kártevő megjelölésére is szokták – gyakran tévesen – alkalmazni. Ebben az értelemben azonban fokozatosan egy új, pontosabb terminus, a „kártevő" (angolul „malware" - malicious software, vagyis kártékony szoftver szavak összevonása) kezdi kiszorítani a használatát.
Ha a számítógépet vírus fertőzi meg, a fájlokat vissza kell állítani eredeti állapotukba, azaz egy vírusvédelmi programmal meg kell tisztítani őket.

Vírusok például a következők: OneHalf, Tenga és Yankee Doodle.

Férgek

A számítógépes féreg olyan kártevő kódot tartalmazó program, amely **hálózatba kötött számítógépeket támad meg, és a hálózaton terjed**. A vírus és a féreg között az az alapvető különbség, hogy **a férgek önállóan képesek replikálódni és terjedni.** Ehhez nincs szükségük gazdafájlokra (vagy rendszertöltő szektorokra).
A férgek e-mailben vagy hálózati csomagokban terjednek. E tekintetben az alábbi két kategóriába sorolhatók:

E-mailben terjedő férgek – Olyan férgek, amelyek elküldik magukat a felhasználó névjegyalbumában lévő e-mail címekre.

Hálózati csomagokban terjedő férgek – Olyan férgek, amelyek különböző alkalmazások biztonsági réseit aknázzák ki.

A férgek tehát sokkal életképesebbek, mint a vírusok. Az internet hozzáférhetősége miatt kibocsátásuk után néhány órával – esetenként néhány perccel – már az egész világon felbukkanhatnak. Az önálló és gyors replikációra való képességük más kártevő szoftvereknél (például a vírusoknál) lényegesen veszélyesebbé teszi őket.
A rendszerben aktiválódott féreg számos kellemetlenséget okozhat: fájlokat törölhet, ronthatja

a rendszer teljesítményét, sőt akár kikapcsolhat egyes programokat. Természetéből adódóan alkalmas más típusú kártevő kódok szállítására is.
Ha számítógépe féreggel fertőződik meg, ajánlatos törölni a fertőzött fájlokat, mivel azok nagy valószínűséggel ártalmas kódot tartalmaznak.

Jól ismert férgek például a következők: Lovsan/Blaster, Stration/Warezov, Bagle és Netsky.

Trójaiak

Történelmi szemszögből a számítógépes trójaiak olyan kártevő kódok, amelyek hasznos programokként tüntetik fel magukat, és csalárd módon ráveszik a felhasználót a futtatásukra. Fontos azonban megjegyezni, hogy ez a régebbi trójaiakra volt igaz, az újabbak már nem tartanak igényt az álcázásra. Kizárólagos céljuk, hogy a lehető legegyszerűbben bejussanak a rendszerbe, és kifejtsék kártékony tevékenységüket. A „trójai" olyan gyűjtőfogalommá vált, amely a más kategóriákba nem sorolható kártevő szoftvereket jelöli.
Tág fogalomról lévén szó, gyakran különböző alkategóriákra osztják. A legismertebbek:

- Letöltő – Olyan kártékony program, amely képes más fertőző kódokat letölteni az internetről.
- Vírushordozó – Olyan trójai, amelynek rendeltetése, hogy más típusú kártékony szoftvereket telepítsen a fertőzött számítógépekre.
- Hátsó kapu – Olyan alkalmazás, amely távoli támadókkal kommunikál, lehetővé téve számukra a rendszerbe való behatolást és irányításának átvételét.
- Billentyűzetfigyelő – Olyan program, amely rögzíti, hogy a felhasználó milyen billentyűket üt le, és ezt az információt elküldi a távoli támadóknak.
- Tárcsázó – Olyan program, amelyet emelt díjas telefonszámok tárcsázására terveztek. Szinte lehetetlen észrevenni, amikor egy ilyen program új kapcsolatot létesít. A tárcsázók csak faxmodemek révén tudnak kárt okozni, ezek azonban már egyre ritkábbak.

A trójaiak általában .exe kiterjesztésű alkalmazások. Ha a számítógép valamelyik fájljáról kiderül, hogy trójai, ajánlatos törölni, mivel nagy valószínűséggel kártevő kódot tartalmaz.

Jól ismert trójaiak például a következők: NetBus, Trojandownloader.Small.ZL, Slapper

Rootkitek

A rootkitek olyan kártevő programok, amelyek a támadónak hozzáférést biztosítanak a rendszerhez, miközben jelenlétüket elrejtik. Miután bejutnak a rendszerbe (általában annak biztonsági rését kihasználva), a rootkitek az operációs rendszer funkcióinak használatával igyekeznek észrevétlenek maradni a vírusvédelmi szoftverek előtt: folyamatokat, fájlokat és Windows regisztrációs adatbázisbeli adatokat rejtenek el. Emiatt a szokványos vizsgálati technikákkal szinte lehetetlen felderíteni őket.
Ha meg szeretné előzni a rootkitek okozta fertőzést, gondoljon arra, hogy az észlelés két szinten működik:

1. Az első szint az, amikor ezek a szoftverek megpróbálnak bejutni a rendszerbe. Még nincsenek jelen, ezért inaktívak. A legtöbb vírusvédelmi rendszer ezen a szinten képes a rootkitek elhárítására (feltéve, hogy egyáltalán fertőzöttként felismerik az ilyen fájlokat).

2. A második szint az, amikor a szokványos ellenőrzés elől elrejtőznek. Az ESET vírusvédelmi rendszer felhasználói élvezhetik az aktív rootkitek észlelésére és elhárítására képes Anti-Stealth technológia előnyeit.

Reklámprogramok

A reklámprogram olyan szoftver, amelynek rendeltetése hirdetések terjesztése. Ebbe a kategóriába a reklámanyagokat megjelenítő programok tartoznak. A reklámprogramok gyakran automatikusan megnyitnak egy reklámot tartalmazó előugró ablakot a böngészőben, vagy módosítják a kezdőlapot. Gyakran szabadszoftverekkel („freeware" programokkal) vannak egybecsomagolva, mert ezek fejlesztői így próbálják meg csökkenteni az (általában hasznos) alkalmazásaik költségeit.
A reklámprogram önmagában nem veszélyes, de a hirdetések zavarhatják a felhasználót. A veszélyt az jelenti, hogy az ilyen programok (a kémprogramokhoz hasonlóan) nyomkövetést is végezhetnek.
Ha freeware szoftver használata mellett dönt, szenteljen különleges figyelmet a telepítőprogramnak. A legtöbb telepítő értesíti a felhasználót a reklámprogramok telepítéséről. Gyakran lehetőség van a szoftver reklámprogram nélküli telepítésére. Egyes esetekben azonban a szoftver nem telepíthető reklámprogram nélkül, vagy csak korlátozottan használható. Ez azt jelenti, hogy a reklámprogram „legálisan" fér hozzá a rendszerhez, mert a felhasználó erre engedélyt adott neki. A biztonságot részesítse azonban előnyben, hiszen jobb félni, mint megijedni.
Ha a számítógép valamelyik fájljáról kiderül, hogy reklámprogram, ajánlatos törölni, mivel nagy valószínűséggel kártevő kódot tartalmaz.

Kémprogramok

Ebbe a kategóriába tartoznak mindazon alkalmazások, amelyek magánjellegű információkat továbbítanak a felhasználó tudta vagy hozzájárulása nélkül. Nyomkövető funkciók révén különböző statisztikai adatokat küldhetnek, például a meglátogatott webhelyek listáját, a felhasználó névjegyalbumában lévő e-mail címeket vagy a leütött billentyűk felsorolását.

A kémprogramok szerzői azt állítják, hogy ezek az eljárások a felhasználók igényeinek és érdeklődési körének feltérképezésére, így hatékonyabban célzott reklámok létrehozására szolgálnak. A probléma azonban az, hogy nincs világos határvonal a hasznos és a kártékony alkalmazások között, és senki sem lehet biztos abban, hogy az összegyűjtött információkkal nem élnek-e vissza. A kémprogramokkal megszerzett adatok lehetnek biztonsági kódok, PIN kódok, bankszámlaszámok és így tovább. A kémprogramokat szerzőik gyakran ingyenes programverziókkal csomagolják egybe, hogy jövedelemre tegyenek szert, vagy szoftverük megvásárlására csábítsanak. Gyakran előfordul, hogy egy program a telepítéskor tájékoztatja a felhasználót a kémprogram jelenlétéről, amivel arra igyekszik rávenni őt, hogy frissítsen a szoftver kémprogrammentes verziójára.

Az egyenrangú (P2P) hálózatok ügyfélalkalmazásai például olyan ingyenes („freeware") termékek, amelyekről tudott, hogy kémprogrammal egybecsomagolva jelennek meg. A Spyfalcon vagy a Spy Sheriff (és sok más) szoftver külön alkategóriába tartozik – ezek kémprogram védelmi alkalmazásoknak tüntetik fel magukat, ám valójában maguk is kémprogramok.
Ha a számítógép valamelyik fájljáról kiderül, hogy kémprogram, ajánlatos törölni, mivel nagy valószínűséggel kártevő kódot tartalmaz.

Veszélyes alkalmazások

Számtalan törvényesen használható alkalmazás létezik, amely a hálózati számítógépek adminisztrációjának egyszerűsítését célozza. Az ilyen programok azonban rossz kezekben bűnös célokat szolgálhatnak. Az ESET ezért állította fel ezt a különleges kategóriát. Ügyfeleink most megadhatják, hogy a vírusvédelmi rendszer észlelje-e vagy sem az ilyesfajta fenyegetéseket.
A „veszélyes alkalmazások” csoportjába a kereskedelemben kapható, törvényes szoftverek tartoznak, mint például a távoli hozzáférést biztosító eszközök, a jelszófeltörő alkalmazások, valamint a billentyűzetfigyelők (a felhasználó minden billentyűleütését rögzítő programok).
Ha észreveszi, hogy egy veszélyes alkalmazás van jelen a számítógépen és fut (de nem Ön telepítette), kérjen tanácsot a hálózati rendszergazdától, vagy távolítsa el az alkalmazást.

Kéretlen alkalmazások

A kéretlen alkalmazások nem feltétlenül kártevők, de hátrányosan befolyásolhatják a számítógép teljesítményét. Ezek az alkalmazások általában engedélyt kérnek a telepítésükhöz. Miután a számítógépre kerülnek, a rendszer a telepítésük előtti állapotához képest eltérően kezd viselkedni. A lényegesebb változások a következők:

- Korábban nem látott új ablakok nyílnak meg.
- Rejtett alkalmazások aktiválódnak és futnak.
- Megnő a rendszererőforrások használata.
- Módosulnak a keresési eredmények.
- Az alkalmazások távoli szerverekkel kommunikálnak.