SZÁMÍTÓGÉPES KÁRTEVŐK (MALWARE)

Számítógépes kártevők

- A rosszindulatú számítógépes programokat összefoglalóan kártevőknek (angolul malware, ejtsd melver) nevezzük.
- A kártevők típusai:
  - Vírusok
  - Férgek
  - Kémprogramok és kéretlen reklámok
  - Trójai programok, rootkitek, botnetek

1. Számítógépes vírusok

- A vírus egy rövid, különleges program, mely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban (képes szaporodni).
- A vírus csupán egyike a rosszindulatú szoftverek *(malware)* számos típusának.
- Valamilyen esemény hatására aktivizálódik
- Tönkretehet fájlokat, hardvert vagy az egész számítógépes rendszert

A vírusok jellemzői:

- Valamilyen futtatható programkódhoz csatlakoznak.
- A program elindulásakor a vírus kódja lefut, és másolatait újabb programokhoz fűzi. Így szaporodik.
- nagyon kicsi a méretük, rejtetten működnek
- legtöbbjük a Microsoft Windows operációs rendszereken okoz gondokat
- futtatható állományokat is képesek megfertőzni
- általában ártó szándékkal készítették őket
- Különböző adathordozókon (pl. pendrájv, CD, stb..) vagy internetről letöltött programokkal, és futtatható kódot tartalmazó adatfájlokkal terjednek.

Védekezés a vírusfertőzéssel szemben

- Legfontosabb a megelőzés:
  - Ellenőrizzük a letöltött programokat és fájlokat
  - Csak legális programot használjunk
  - Telepítsünk a számítógépünkre vírusirtó programot

Boot szektor vírusok

- A lemezek boot szektorát fertőzik meg.
- Fertőzéskor a vírus a lemez egy nem használt részére elmenti a lemez eredeti boot szektorát, azután saját kódját helyezi a boot szektorba.
- Ilyen módon a vírus már a lemezzel való első műveletkor, minden más előtt bemásolódik a memóriába, innen pedig már képes más lemezekre terjedni.
- Abban az esetben, ha egy lemez írásvédett, a boot vírus nem képes fertőzni.

Trójai vírusok

- Nevüket viselkedésük miatt kapták a trójai faló nyomán: ezek a vírusok jól működő programok álcája mögé bújnak.
- Nem sokszorosítják magukat, inkább időzített bombaként foghatjuk fel őket: a trójai program egy darabig jól ellát valamilyen feladatot, aztán egyszer csak nekilát, és végzetes károkat okoz (pl. tönkreteszi a merevlemezen tárolt adatokat, hálózati támadáshoz használja gépünket, stb).

Makróvírusok

- A programozható irodai alkalmazások megjelenésével jöttek létre és terjedtek el
- az Office eszközökkel készült dokumentumainkban tehetnek kárt.
- Irtása többnyire könnyű!

E-mail vírusok

- Az Internet rohamos terjedésével jelentek meg az **e-mail-vírusok**, melyek a levelezőszerverek tömeges e-mail-küldéssel való leterhelése mellett adatvesztést, adatok kiszivárgását okozhatják.

MR vírusok

- Memóriába fészkeli be magát a vírus. (memória-rezidens)
- Irtása: tiszta boot- lemezről való gépindítással lehetséges.

2.Férgek (worm ejtsd: vörm)

- Egy **számítógépes féreg** (*worm*) a számítógépes vírushoz hasonló önsokszorosító számítógépes program.
- Nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket.
- Gyakran a számítógép-hálózatokat használják fel terjedésükhöz.

2.Férgek (worm ejtsd: vörm)

- Az első férget 1978-ban készítette el két kutató.
- Az első széles körben is ismertté vált féreg a Morris-féreg volt. (1990. január 22-én 3 év szabadságvesztésre és 400 óra közmunkára ítélték, valamint 10 000 dolláros bírságot szabtak ki az alkotóra.

3.Kémprogramok (spyware)

- **Kémprogramnak** (angolul spyware) nevezzük az olyan, főleg az interneten terjedő számítógépes programok összességét, amelyek célja, hogy törvénytelen úton megszerezzék a megfertőzött számítógép felhasználójának személyes adatait.
- Feltelepülése általában észrevétlenül történik.
- A megszerzett információkat bűncselekmények (hitelkártya számok, online szolgáltatások jelszavai) elkövetésére vagy böngészési szokásaink, érdeklődésünk, ízlésünk megfigyelésére használják fel.

4.Agresszív reklámprogramok (adware)

- **Reklámprogram**nak nevezzük az olyan, interneten terjedő számítógépes programok összességét, amelyek célja, hogy egy terméket, számítógépes programot, annak készítőjét vagy egy céget reklámozzanak.
- Reklámprogramokat nagyon sok programmal együtt telepíthetünk (licencszerződés ezt előírja, nem figyelünk a beállításoknál. A megszerzett információkat üzleti célokra (pl. célzott reklámok létrehozása, felhasználói statisztikák, profilok készítése stb.), vagy akár nem törvényes (kéretlen reklámlevelek, lásd spam) módon használják fel.

5.Rootkitek

- **Rootkit** alatt bizonyos szoftvereszközöket értünk, melyek segítségével egy hacker könnyen visszatérhet a "tett színhelyére", ha már korábban beférkőzött a rendszerbe, hogy bizalmas adatokat gyűjtsön a fertőzött számítógépről.
- A rendszerfájlokat fertőzik meg, amik továbbra is ellátják feladataikat, de már bennük van az ártó kód.
- A hackereket az anyagi haszonszerzés vezérli, a védtelen vagy nem megfelelően védett számítógépek pedig jó lehetőség számukra.

Védekezés a kártékony programok ellen

- Megelőzés
- Korai felismerés
- Védelem
- Gyógyítás

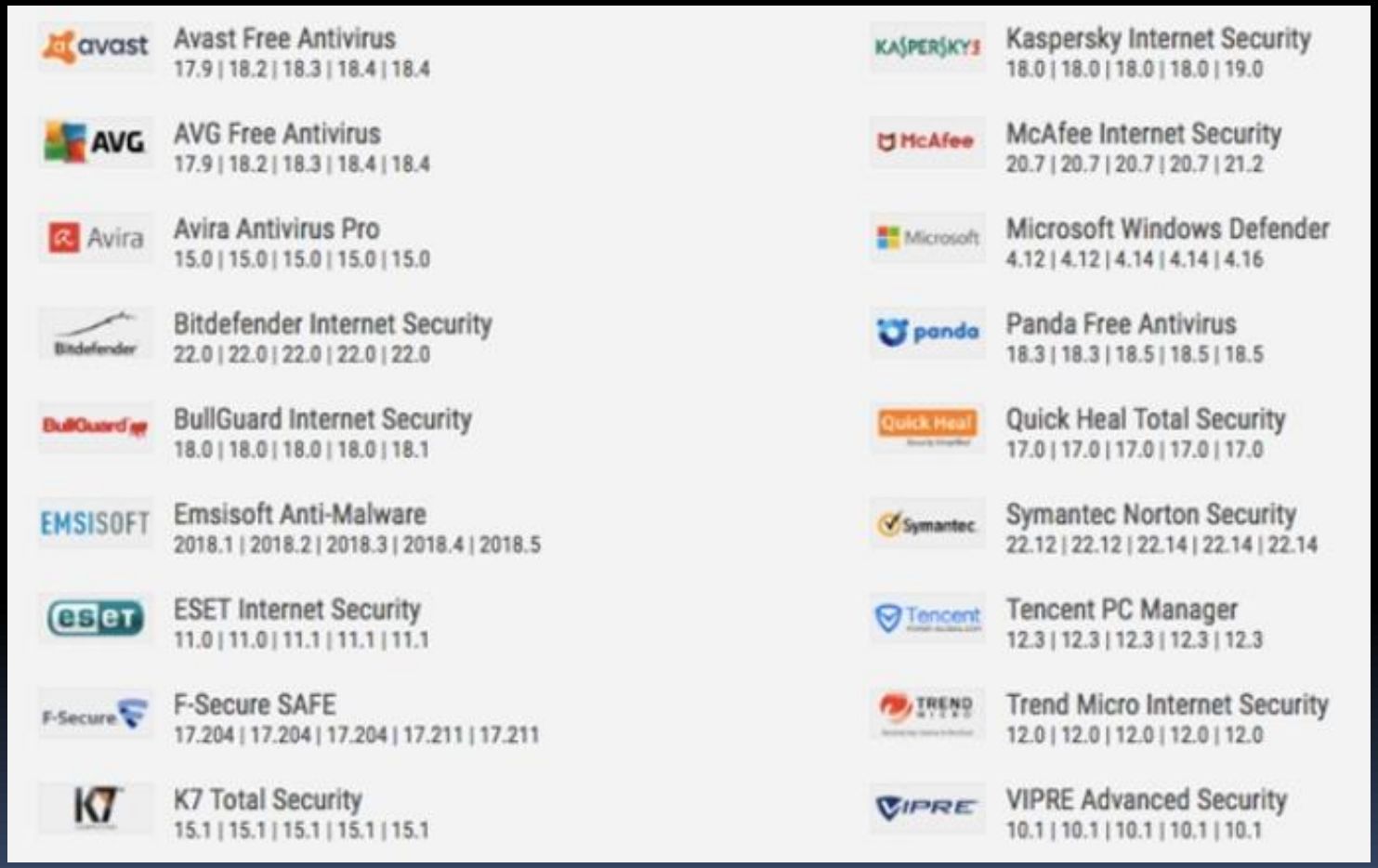
A védekezés formái a vírusok ellen

- A számítógépre telepített vírusirtó programmal (antivírus program), mely állandóan figyeli a rendszert.
- Tűzfallal, mely megvédheti a rendszerünket az illetéktelen betörési kísérletektől illetve a vírusok hálózati fertőzését is megakadályozhatja.

A többi malware ellen

- A spyware ellen: kereső szoftverek segítenek
- Adware ellen: összetett biztonsági programokkal, felderítőprogramokkal
- Férgek ellen: antivírus programokkal, tűzfallal
- Rootkitek ellen: antivírus programokkal, tűzfallal

Jelenleg legnépszerűbb kiberbiztonsági programok



Kép forrása: https://hvg.hu/tudomany/20180717_legjobb_ingyenes_virusirto_2018_legjobb_antivirus_program_letoltes

Tűzfalak

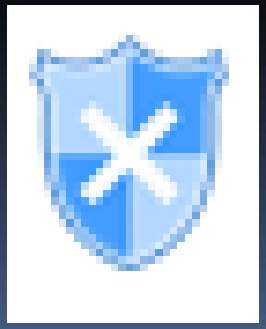
- Olyan szoftveres és/vagy hardveres technika, amellyel az intézmények helyi hálózatukat megvédhetik a külső hálózatról (jellemzően az internetről) érkező betörések ellen, a bejövő és kimenő adatforgalom figyelésével, megszűrésével és korlátozásával.

Kémprogram-eltávolítók:

- Ad-Aware SE (ingyenes, magyarul)

- SpyBot (ingyenes)

- Spyware Terminator Free (ingyenes, magyarul)



A vírusírtó programok működése

- A kártevők felismerésére és eltávolítására szolgálnak.
- A memóriában tartózkodnak, minden fájlműveletet ellenőriznek.
- Az ismert vírusok jellegzetes kódrészleteit keresik, vagy olyan műveleteket figyelnek, amelyek a vírusokra jellemzőek.

Mit kell tenni a vírusok elleni hatékony védelem céljából?

- Rendszeresen fel kell frissíteni a vírusölő programot
- Más felhasználó adatállományának a használata előtt feltétlenül ellenőrizni kell az adatállomány vírusmentességét
- Kerülni kell a hálózoton az ismeretlen helyekről származó állományok letöltését
- Kerülni kell a hálózoton az ismeretlenekkel való adatcserét
- Nem kell kinyitni az ismeretlen személyektől kapott elektronikus levél melékletét