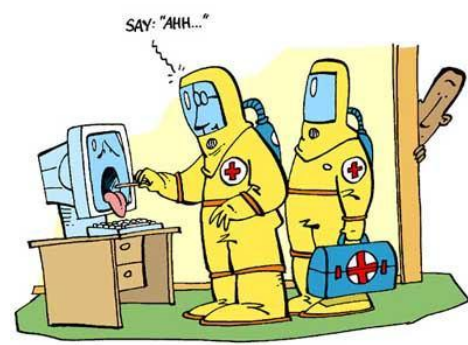


Számítógépes vírusok



Fogalma:

A vírus önmaga sokszorozására és terjesztésére képes kisméretű számítógépes szoftver, a felhasználók számára nem láthatók. Információ szerzés, kártétel, vagy esetleg teljen ártalmatlan üzenet küldése a céljuk.

Típusai:

a. Boot vírusok

A lemezegységek bootszektorában tanyáznak, és amennyiben erről a lemezről történik a bootolás, beköltözik a memóriába, és a továbbiakban minden elérhető lemez boot szektorát megfertőzi, bemásolja magát.

b. File vírusok

A futtatható állományokhoz (exe, com kiterjesztésűek) fűzi hozzá magát. Amennyiben elindítjuk ezt az állományt, bekerül a memóriába, és minden továbbiakban elindított állományt megfertőz.

c. Makro vírusok

Az Office csomag állományait képes fertőzni, Word, Excel, Powerpoint és Acces adatállományokba írja be magát, az úgynevezett makróutasítások segítségével. Az utóbbi évben a felfedezett vírusok 90 %-a makrovírus volt.

d. E-mail vírusok

Léteznek olyan vírusok, amelyek e-mail útján terjednek, vagy a csatolt állományon keresztül, vagy újabban elég a levelet elolvasni

e. Férgék

önállóan, önmaga igen sok példányban történő sokszorozásával terjed. Legsikeresebb férgek e-mail-ben csatolt állományként ill. különböző rendszerek sebezhetőségeit kihasználva fertőznek és terjednek.

Működésük időszakai:

1. Szaporodás

A vírusprogram képes önmagát másolni, reprodukálni. (Kivéve a trójai faló típusú vírusok.)
A vírusokat elhelyezkedésük, szaporodásuk szerint csoportosítjuk.

2. Lappangás

A vírusok egy meghatározott feltételig rejtve maradnak, hogy sor számítógépen el tudjanak szaporodni. A lappangási időszakban csak szaporodnak.

3. Aktivizálódás

Egy bizonyos feltétel teljesülése esetén a vírus aktivizálódik, ami lehet egy bizonyos számú másolat, vagy az év bizonyos napja, speciális billetyűkombináció, vagy 1001 egyéb feltétel. Ekkor a vírus vagy jóindulatú, vagy nem. Ha jóindulatú, akkor csak felhívja magára a figyelmet, de nem töröl semmilyen adatot a lemezekről, ha rosszindulatú, akkor általában törli, vagy elérhetlenné teszi winchesterek tartalmát.

Védekezés a vírusokkal szemben:

- Használjunk vírusellenőrző és -irtó programokat. Rendszeresen (hetente) frissítsük a vírusirtó program vírus-adatbázisát, hogy a legújabb támadási formákkal szemben is védettek maradjunk.
- Óvakodjunk az idegen számítógépből származó vagy kétes eredetű programoktól, melyek általában mágneslemezen vagy más adathordozón bekerülhetnek saját gépünkbe, ezek futtatásától.
- Csak megbízható forrásból származó szoftvereket használjunk.