7. óra Vírusok2

BLZS©

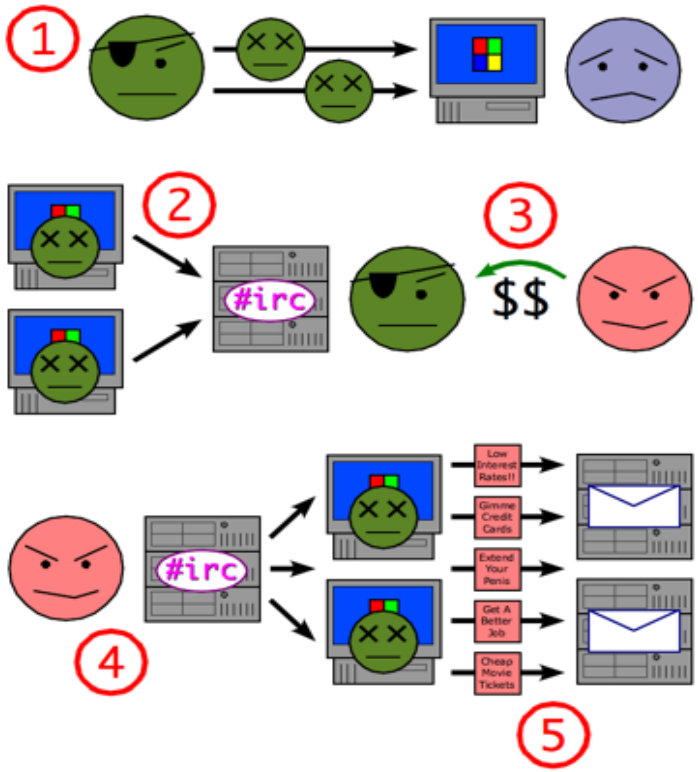
Keylogger programok:

- Rögzíti a billentyűleütéseket és csevegéseket, eltárolja a számítógép képernyőjének minden változását is (képernyőfelvételek naplója).
- Elment minden, a vágólapra helyezett szöveget.
- Emellett rögzíti minden meglátogatott honlap címét, valamint a futtatott alkalmazásokat.
- Működése teljesen észrevétlen és láthatatlan marad.
- Legális célra is használható

Botnet

BLZS©

- Zombigépek alkotta hálózat: ezeken a gépeken – valamilyen vírus segítségével, távolról átveszik az erőforrások feletti vezérlést részben vagy egészben és azt valamilyen cél érdekében használják fel levelezőszerver elleni tömeg támadás.



Rootkit

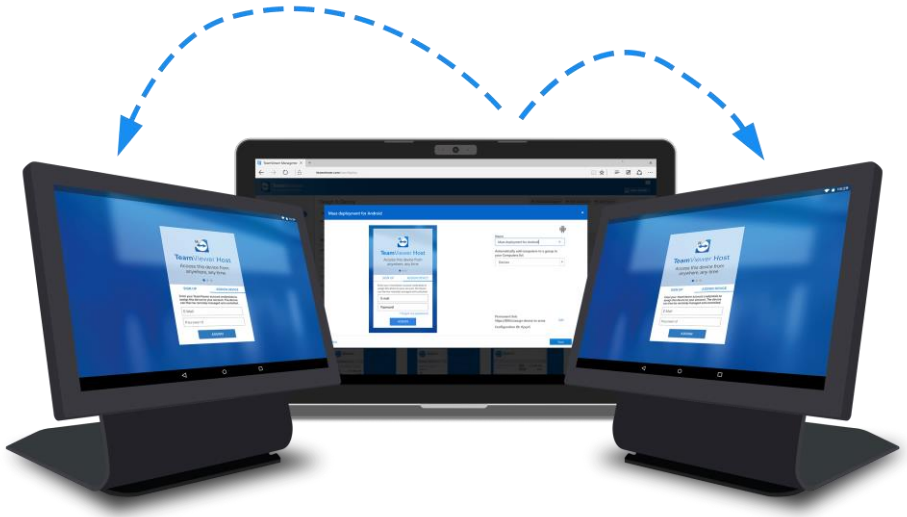
- Olyan programok, amelyek illetéktelen behatolók (cracker) megfertőzött rendszerekbe való visszatérését segítik elő.
- Igyekeznek elrejteni magukat és akár más károkozókat is az operációs rendszer illetve a víruskereső alkalmazások elől.

BLZS©

Spyware, kémprogramok

•Adatokat gyűjtenek a felhasználó internetezési és egyéb szokásairól, esetleg további személyes információkat is, amit akár továbbítanak is külső állomáshoz kereskedelmi vagy illegális felhasználási célokra.

•Legális célokra is használhatók ilyen programok: TeamViewer; tanterem felügyeleti programok



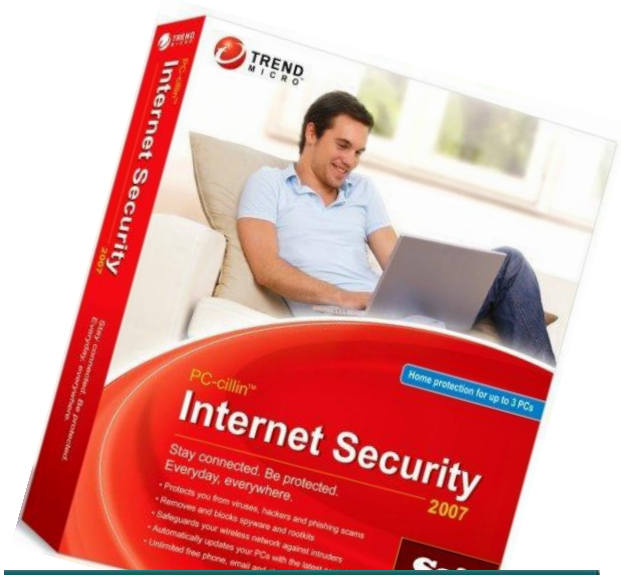
Védekezés a vírusok ellen:

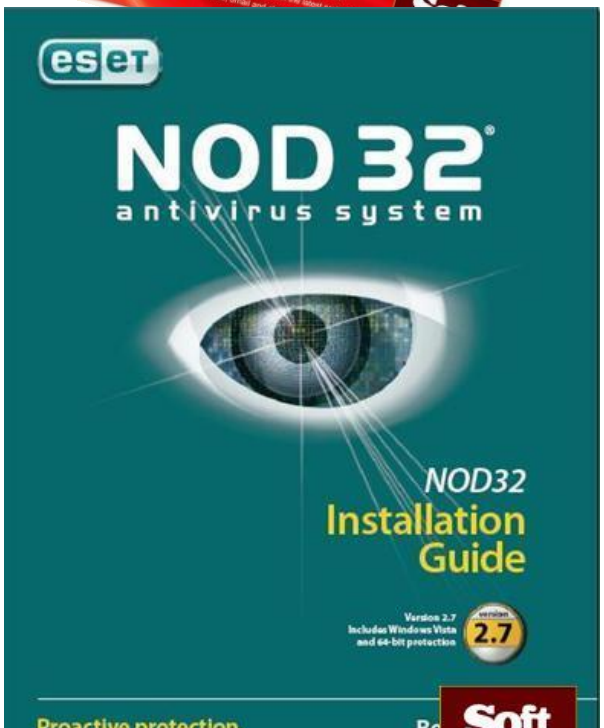
BLZS©

- Rendszeresen futtassunk vírusellenőrző programokat.
- Vizsgáljuk meg a kölcsön kapott adathordozókat és programokat mielőtt elindítanánk.
- A tömörített programokat kibontás után ellenőrizzük.
- Rendszeresen archiváljunk.
- Régen fontos volt hogy legyen készenlétben indító lemez.

Vírusirtó programok

BLZS©





-Dr Solomon's AntiVirus Toolkit
-F-Prot Professional
-IBM AntiVirus
-McAfee VirusScan
-Norton AntiVirus
-ThunderByte Anti-Virus Utilities
-VirusBuster
-VirOverseer
-AVG
-NOD 32
-VirWare
-UVE
-Panda Antiv

Vírusirtó programok

BLZS©

Vírusirtó programok

BLZS©

Szinte mindegyik vírusirtó program felismeri a vírusokat de irtani csak néhány képes. Nagyrészük nem tesz mást csak rejtőzködik, de vannak vírusok amelyek tönkreteszik állományainkat, leformázzák a merevlemezünket, vagy nem engedik, hogy újraindítsuk a szg.-et, esetenkénk tönkreteszi a BIOS beállításunkat. Heurisztikus keresés: Fridrik Skulason alkalmazta először az általa fejlesztett F-Protban. A módszer lényege, hogy a keresés során megvizsgált file-okról oly módon legyen eldönthető, hogy vírusosak-e, vagy sem, hogy sem a vírusról, sem pedig az eredeti programfile-okról nincs információ.

Vírusirtó program iránti elvárások!

BLZS©

Naplózás:

vírus keresés és irtás során a műveleteket naplózza a program, bejegyzések a vírustalálatról, hibákról

Karantén:

írhatatlan, javíthatatlan fájlok helye tovább nem fertőz!

Állandó védelem:

A vírusirtó program állandóan figyelje a fájl műveleteket.

Programfrissítés:

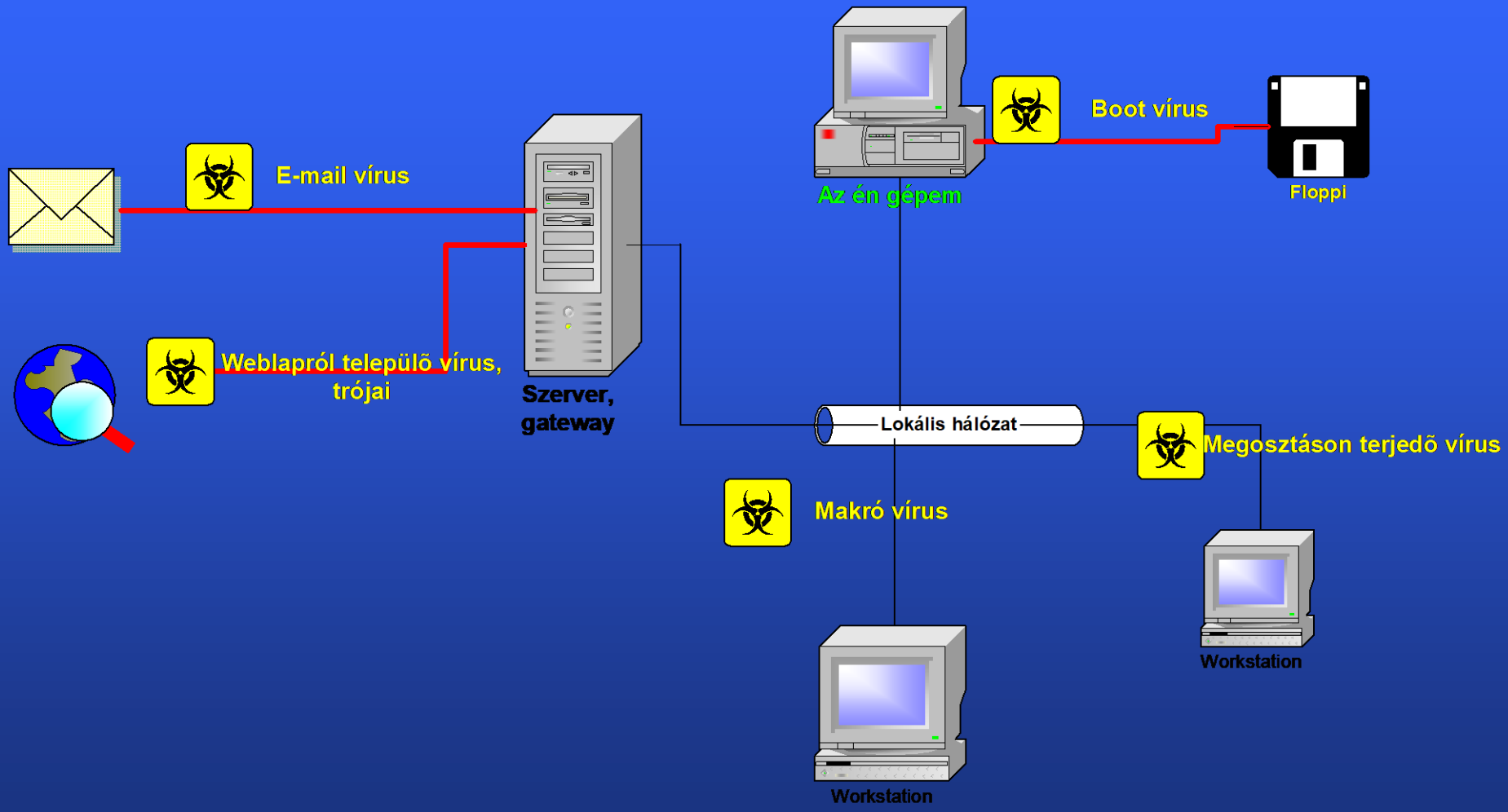
Követelmény, hogy a frissítőfájlok naponta vagy kétnaponta letölthető legyen automatikusan.

Hatékonyság:

Ne csak felismerje a vírusos fájlokat, hanem javítsa is ki!

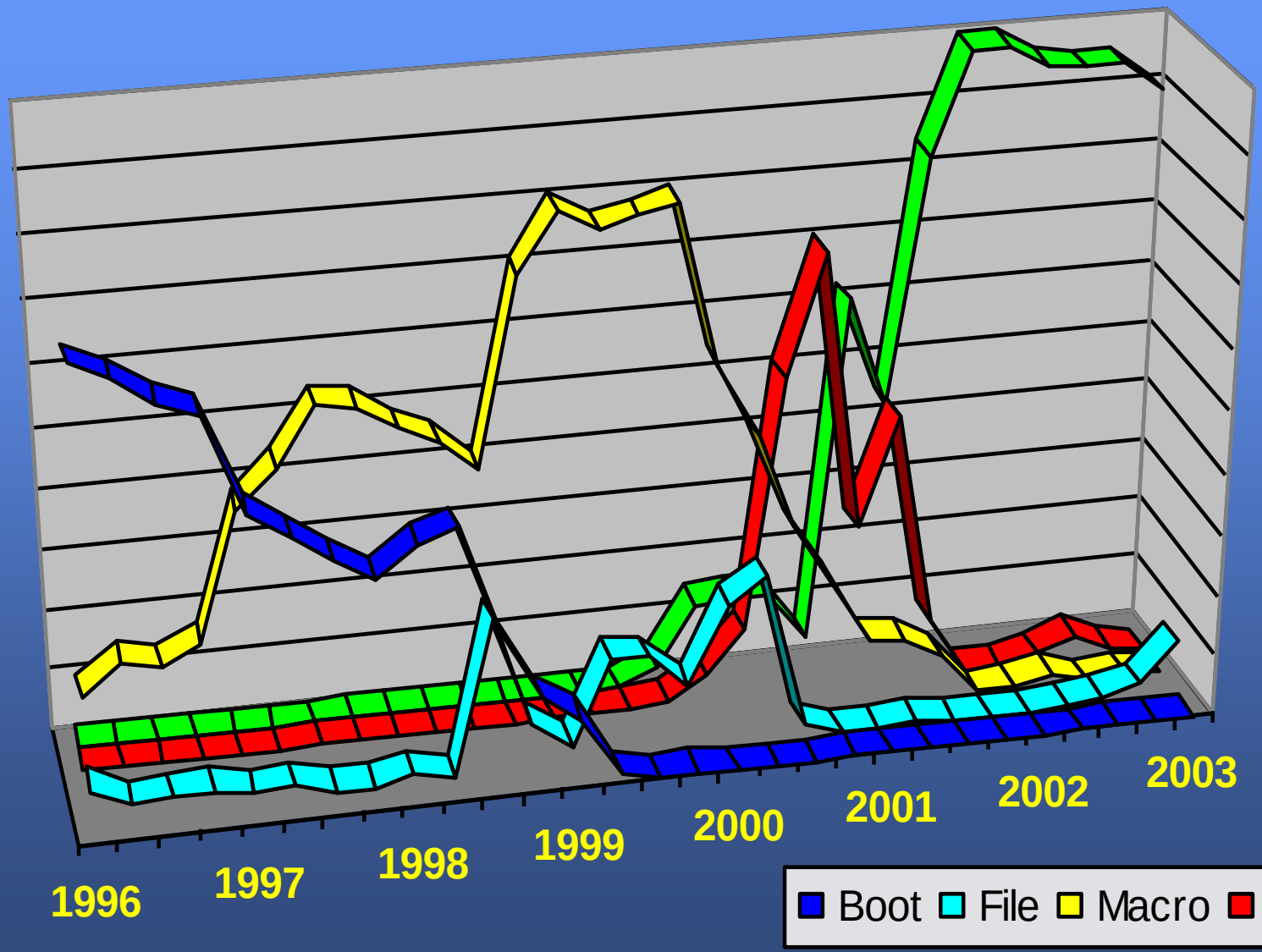
Vírus terjedési pontok!

BLZS©



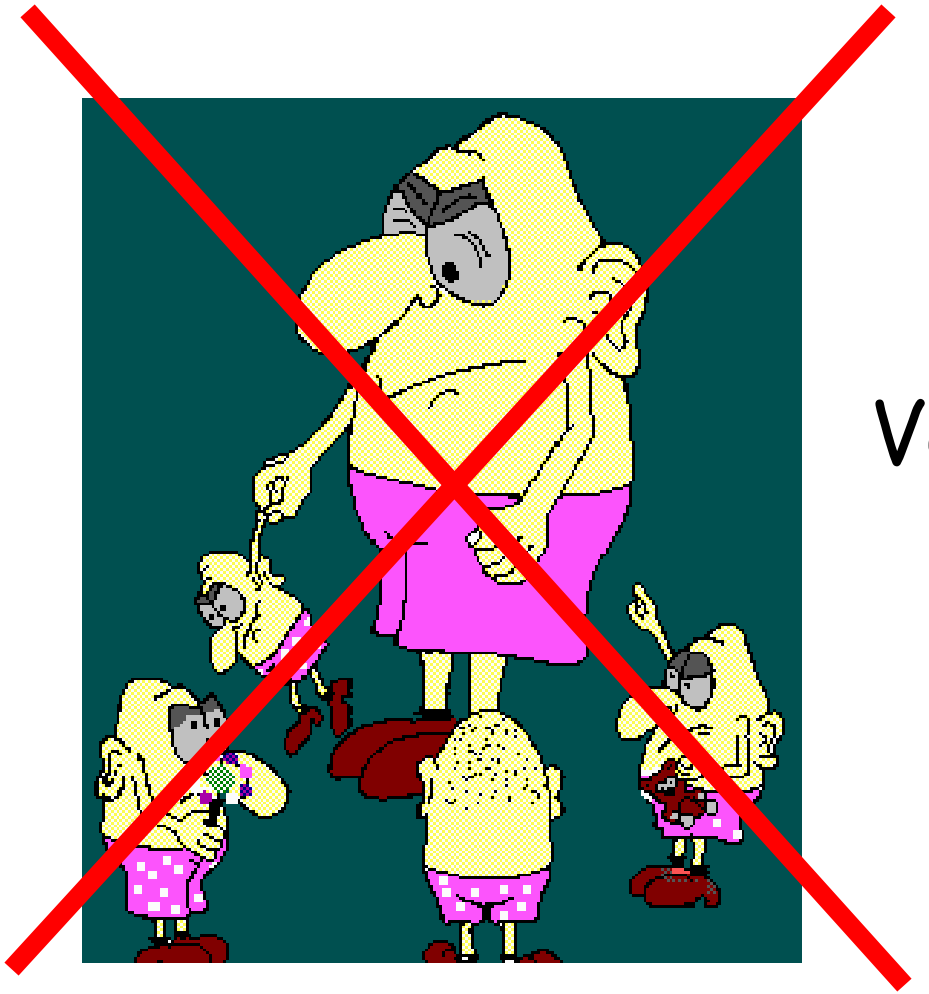
A vírusok fajtáinak alakulása!

BLZS©



BLZS©

Vírusmentes környezetet kívánok!



Vesszenek a vírusok!