13. Vírusok és egyéb szoftveres károkozók (3.1)

- Vírus fogalma, csoportosítása, terjedése
- Fertőzésre utaló jelek
- Passzív védekezés módszerei
- Aktív védekezés módszerei

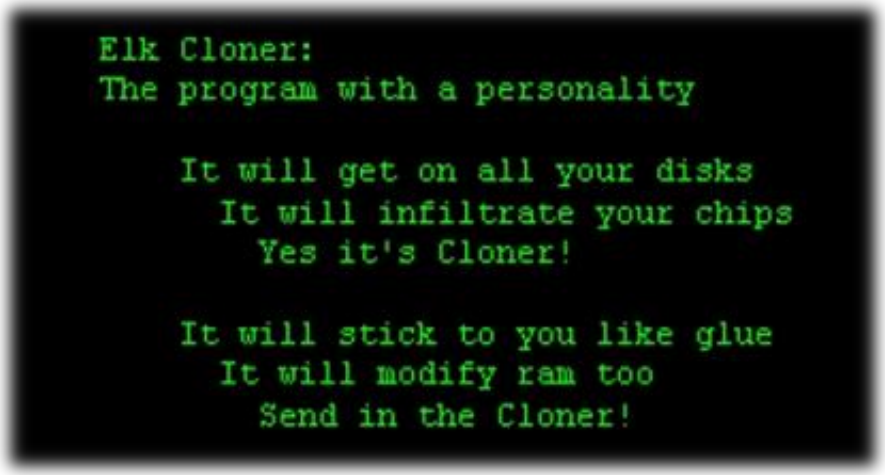
Mi is a vírus?

-Számítógép program, már a 60-as években katonai körök foglalkoztak program írással, hogy az ellenség gépeit tönkre tegyék és adatokat megszerezhessenek.

-önreprodukcióra képes, károkat okozó program

BLZS©

1982-ben az akkor 15 éves amerikai diák, Rich Skrenta úgy döntött, hogy megvicceli ismerőseit, ezért írt egy programot.
A kilencvenes évek közepén, ahogy egyre inkább terjedni kezdett a Windows operációs rendszer, a vírusok többsége is azt vette már célba.
2002-ben rájönnek a vírusírók, hogy nemcsak presztízskérdés már kártevőket készíteni, hanem haszonszerzés, zsarolás vagy éppen információszerzés céljából is.



Miért írnak vírust?

BLZS©

- Anyagi érdek
- Károkozás
- Tudás bizonyítása
- Információ szerzés
- Zsarolás

Vírusfertőzés lehetőségei:

BLZS©

- Külső adathordozó
- E-mail csatolt állomány
- Internetről letöltés
- Interneten fertőzött oldal meglátogatása

Honnan tudom, vírusaim vannak?

BLZS©

Megnyilvánulásokból amik a következők lehetnek:

- Dokumentumainkat jelszóval látja el,
- Elfogy a szabad hely a lemezen,
- Nyomtatáskor nem oda illő szöveget helyez el.
- Néhány Word menüpont eltűnik
- Nem lehet elmenteni a dokumentumot.
- Lassulás
- Programok, adatok sérülése
- Nem indulnak programok,
- Rendszerindítás önmagától, stb.

Sok esetben egyáltalán nem észlelni azonnal a felhasználó egy vírus jelenlétét a rendszerében!

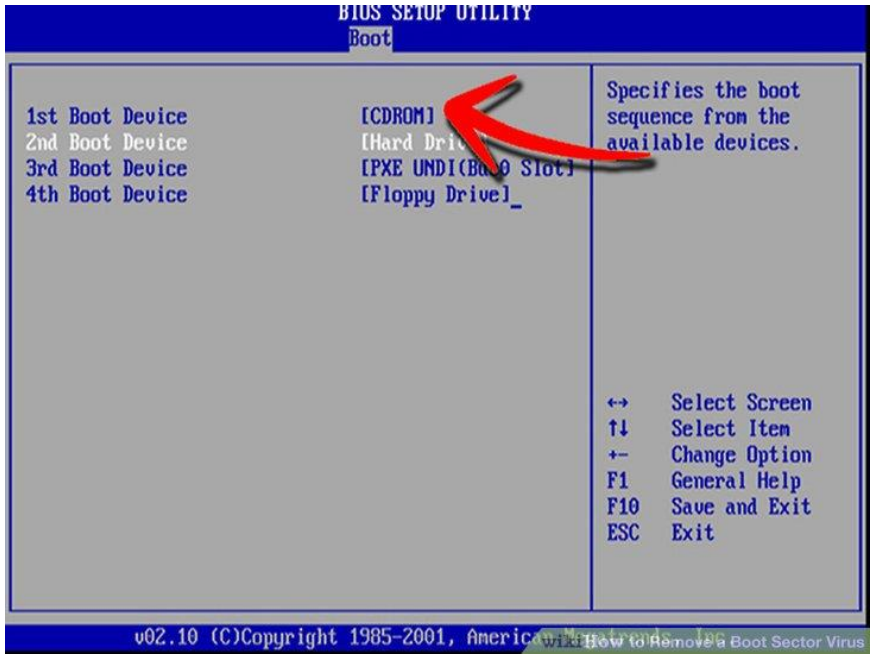
Vírusok fajtái:

BLZS©

Boot vírusok:

Régen a legelterjedtebb vírusok voltak, általában a legkönnyebb kiirtani. Olyan vírusok, amelyek nem várják meg, amíg a számítógépen az operációs rendszer elindul: igyekeznek még az operációs rendszer elindulása előtt aktivizálódni úgy, hogy az elsődleges partíciók boot szektorába írják bele magukat.

Majd a boot szektorból töltődnek be a memóriába.



Vírusok fajtái:

BLZS©

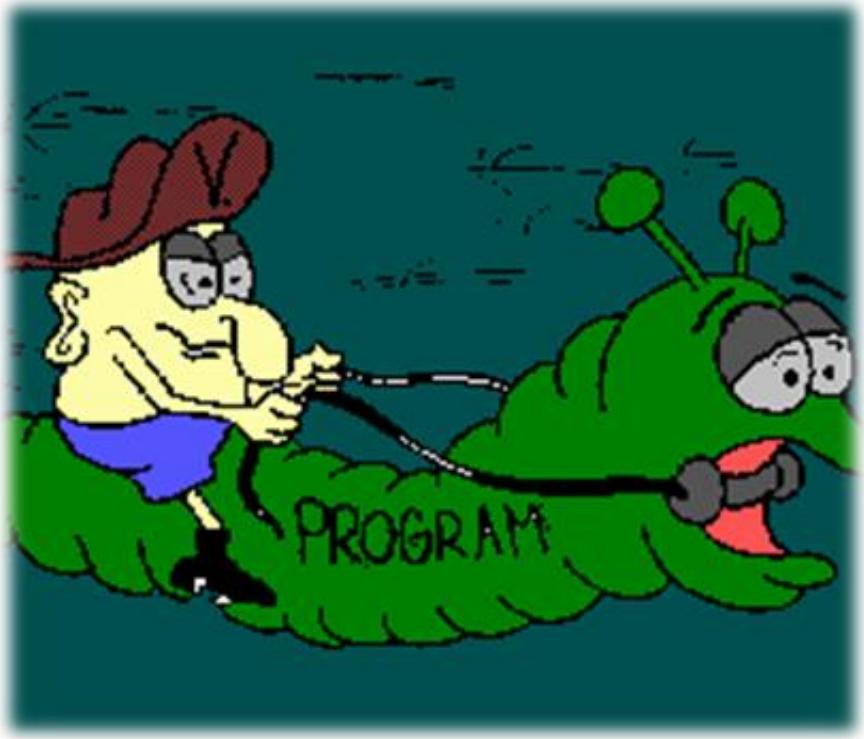
Állományvírusok:

A nevüket azért kapták, mert nem képeznek önálló állományokat a számítógép háttértárán, hanem egy már létező állományt módosítanak.
Leginkább az .exe és .com végrehajtható állományokat fertőzik meg.
Ezt a fajta vírust is könnyű felfedezni de olyan károkat okoznak az állományokban, hogy csak a törléssel és újra telepítéssel lehet célt elérni.

Vírusok fajtái:

BLZS©

Többlaki vírusok:
Az előbbi kettő kereszteződése, az állományokat is és a boot szektort is megfertőzik így könnyebben terjednek. Nehezebb észrevenni és eltávolítani ezeket.

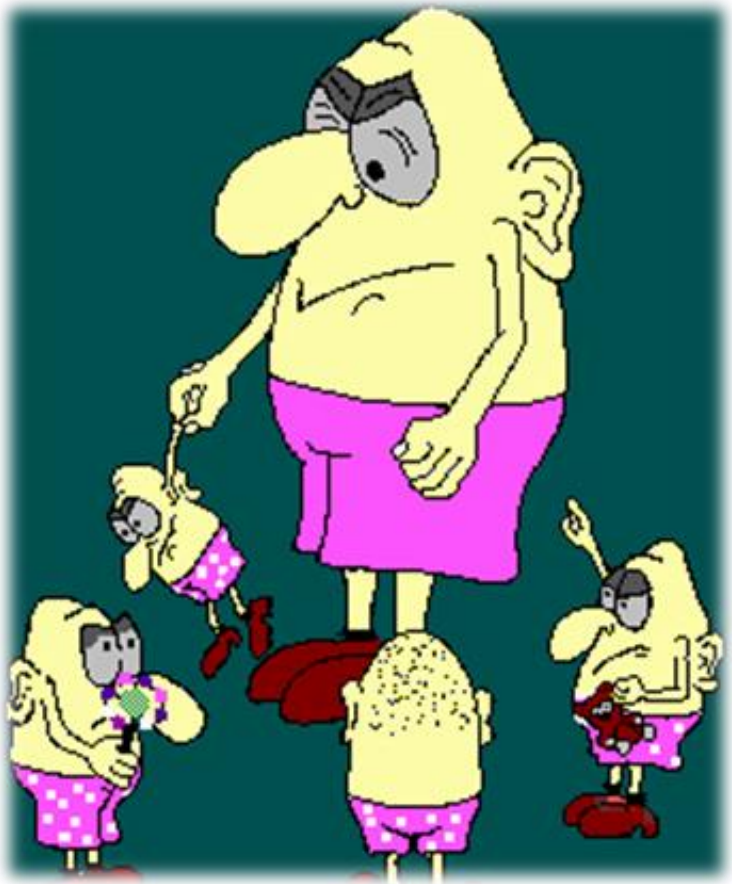


Vírusok fajtái:

BLZS©

Polimorf vírus:

Folytonosan mutálódnak, hogy megtévesszék a vizsgálóprogramokat, amelyek meghatározott víruskódokat keresnek.



Vírusok fajtái:

BLZS©

Lopakodó vírusok:

Képes arra ez a vírus, hogy átmenetileg eltávolítsa magát a memóriából, hogy így kerülje el a lebukást.

Vírusok fajtái:

BLZS©

Makró vírusok:

Gyorsan terjedő Word és Excel állományokat fertőző vírus. Elég megnyitni egy lemezen vagy elektronikus postán kapott állományt és már meg is fertőződtünk. Ez a vírus fajta megfertőzi a Word és Excel központi sablonfile-ját és így minden megnyitott dokumentum megfertőződik.

Vírusok fajtái:

BLZS©

Féreg:

A vírusok egyik alosztálya. A programok hibáját használják ki. A féreg általában a felhasználók közreműködése nélkül terjednek, és teljes (lehetőleg módosított) másolatokat terjesztenek a hálózaton át. A férgek felemészthetik a memóriát és a sávszélességet, ezért a számítógép összeomolhat.

Vírusok fajtái:

BLZS©

Trójai:

Hasznosnak tűnő, de valójában kártékony számítógépes program. Leginkább szórakoztató programnak álcázzák őket készítőik. A trójaiak úgy terjednek, ha a részedett felhasználók megnyitják a programot, mert azt gondolják, hogy hivatalos forrásból származik.

7. óra Vírusok2

BLZS©

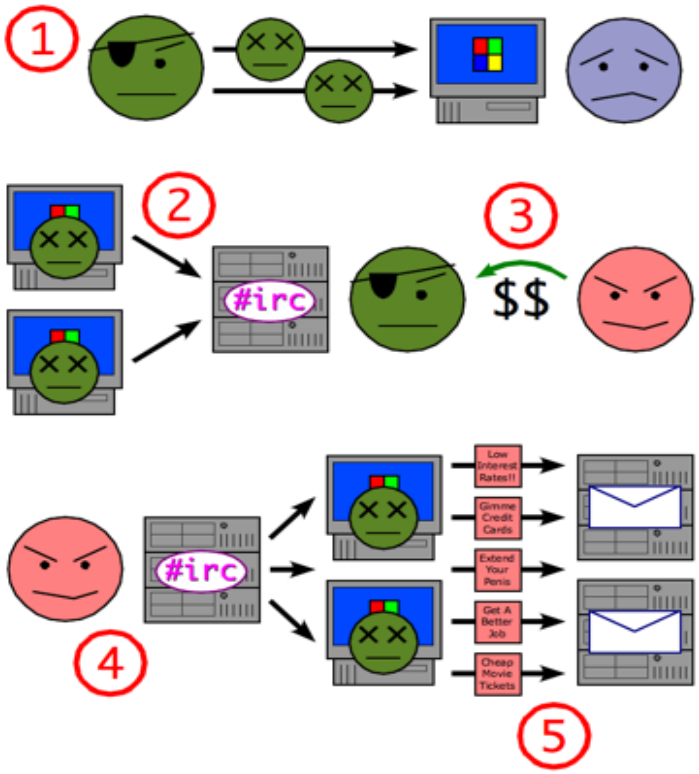
Keylogger programok:

- 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.



BLZS©

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.

Spyware, kémprogramok

BLZS©

•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

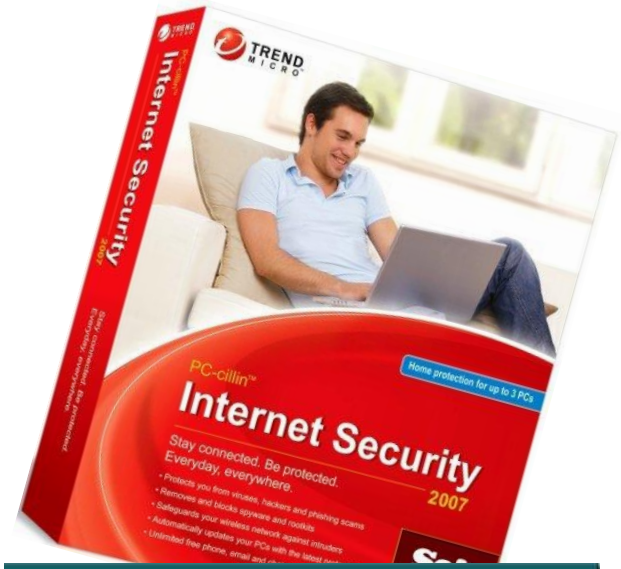
Védekezés a vírusok ellen:

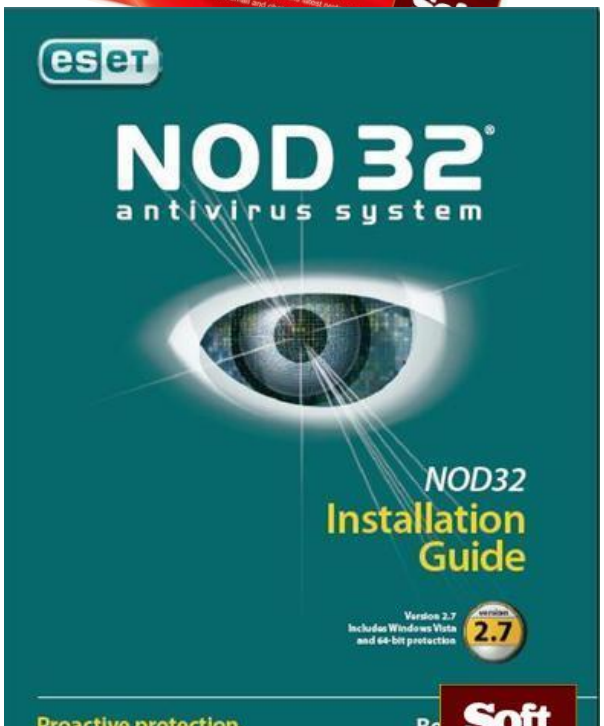
BLZS©

- 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:

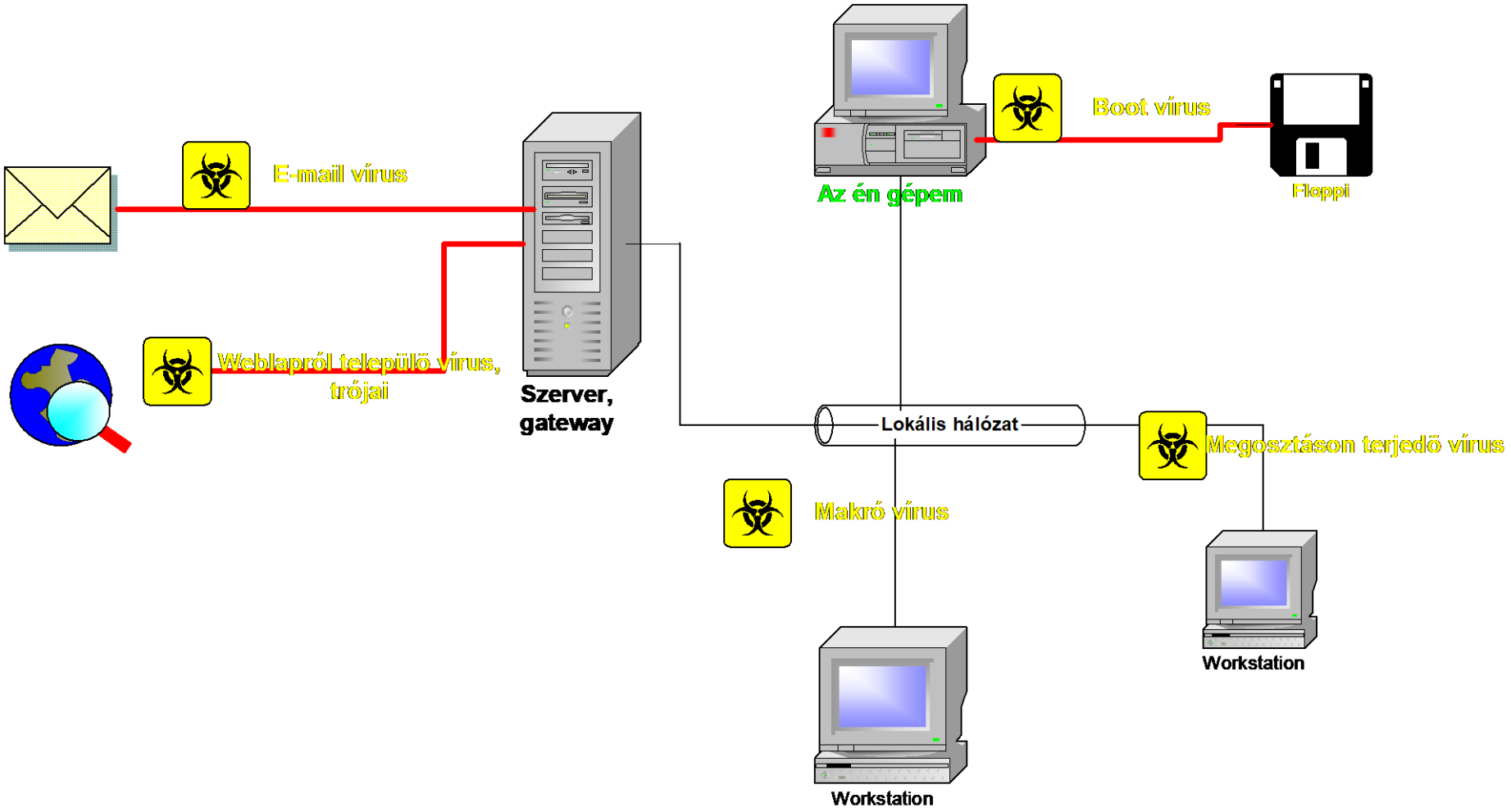
Követelmény, hogy a frissítőfájlok naponta vagy kétnaponta letölthető legyen automatikusan.

Hatékonyság:

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

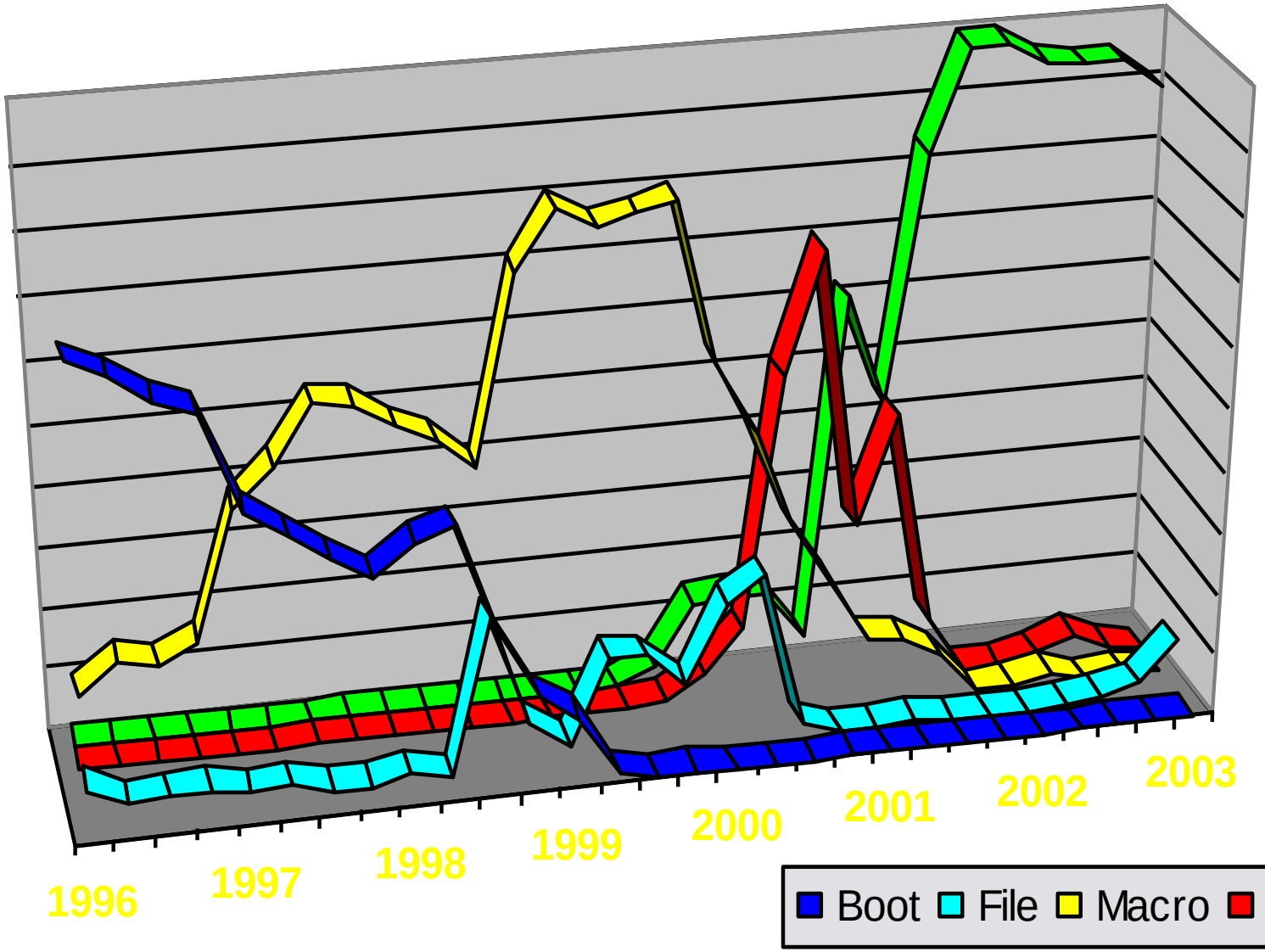
Vírus terjedési pontok!

BLZS©



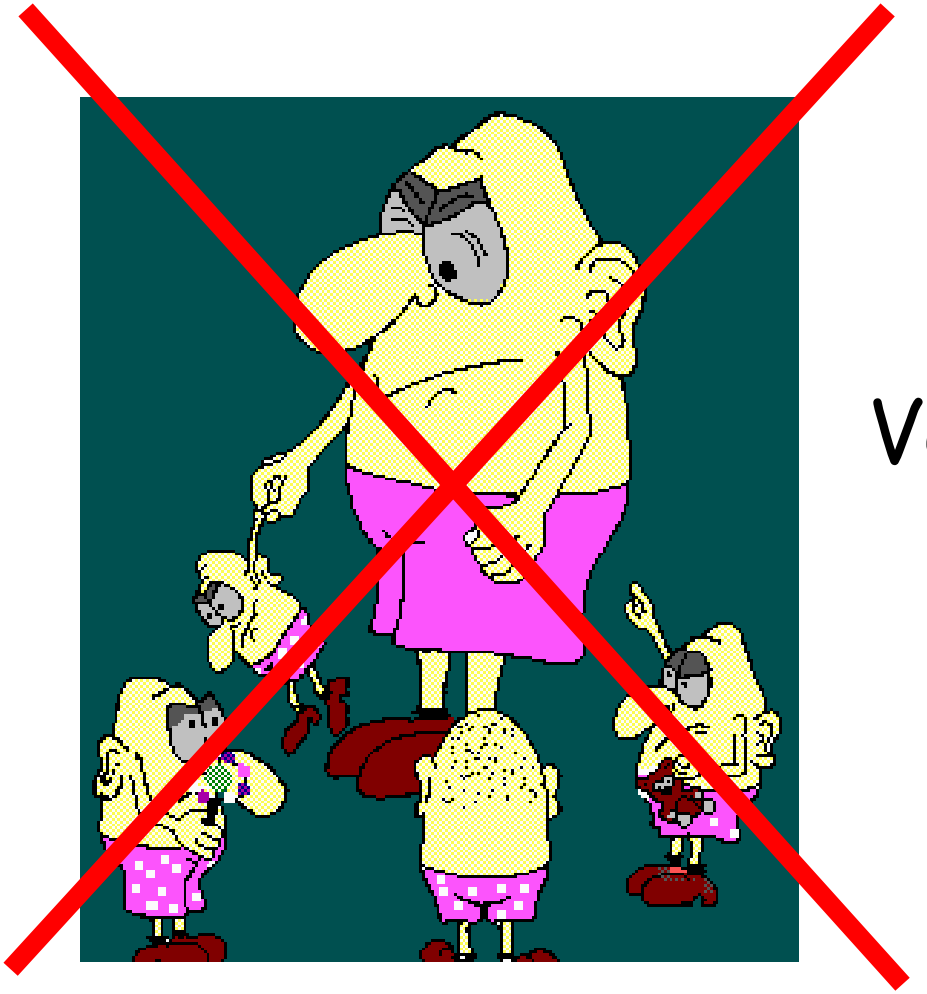
A vírusok fajtáinak alakulása!

BLZS©



BLZS©

Vírusmentes környezetet kívánok!



Vesszenek a vírusok!