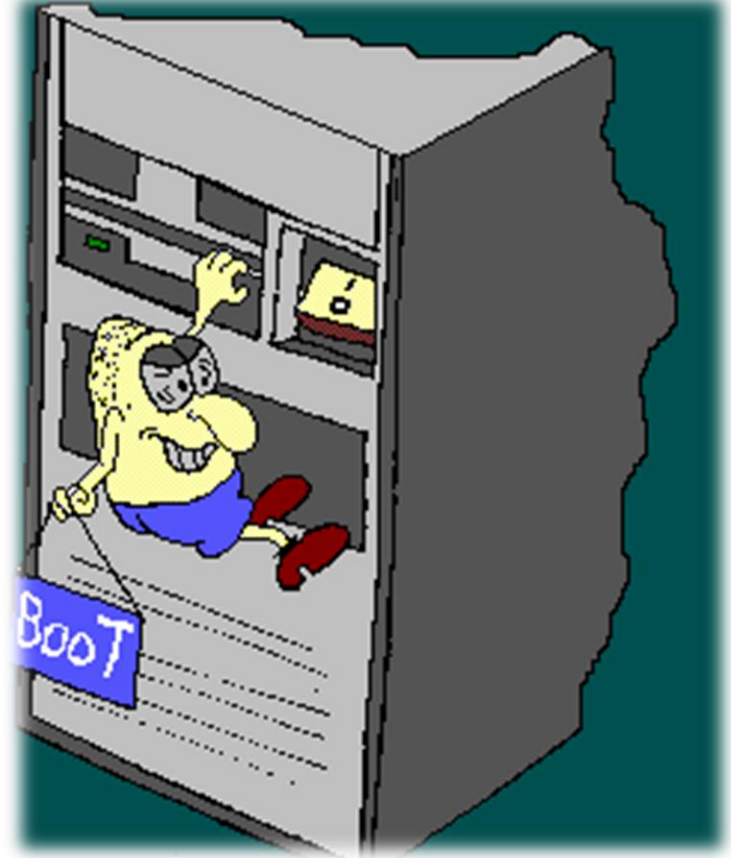


8. óra Segédprogramok_2

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



Miért írnak vírust?

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



Vírusfertőzés lehetőségei:

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



Honnan tudom, vírusaim vannak?

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.



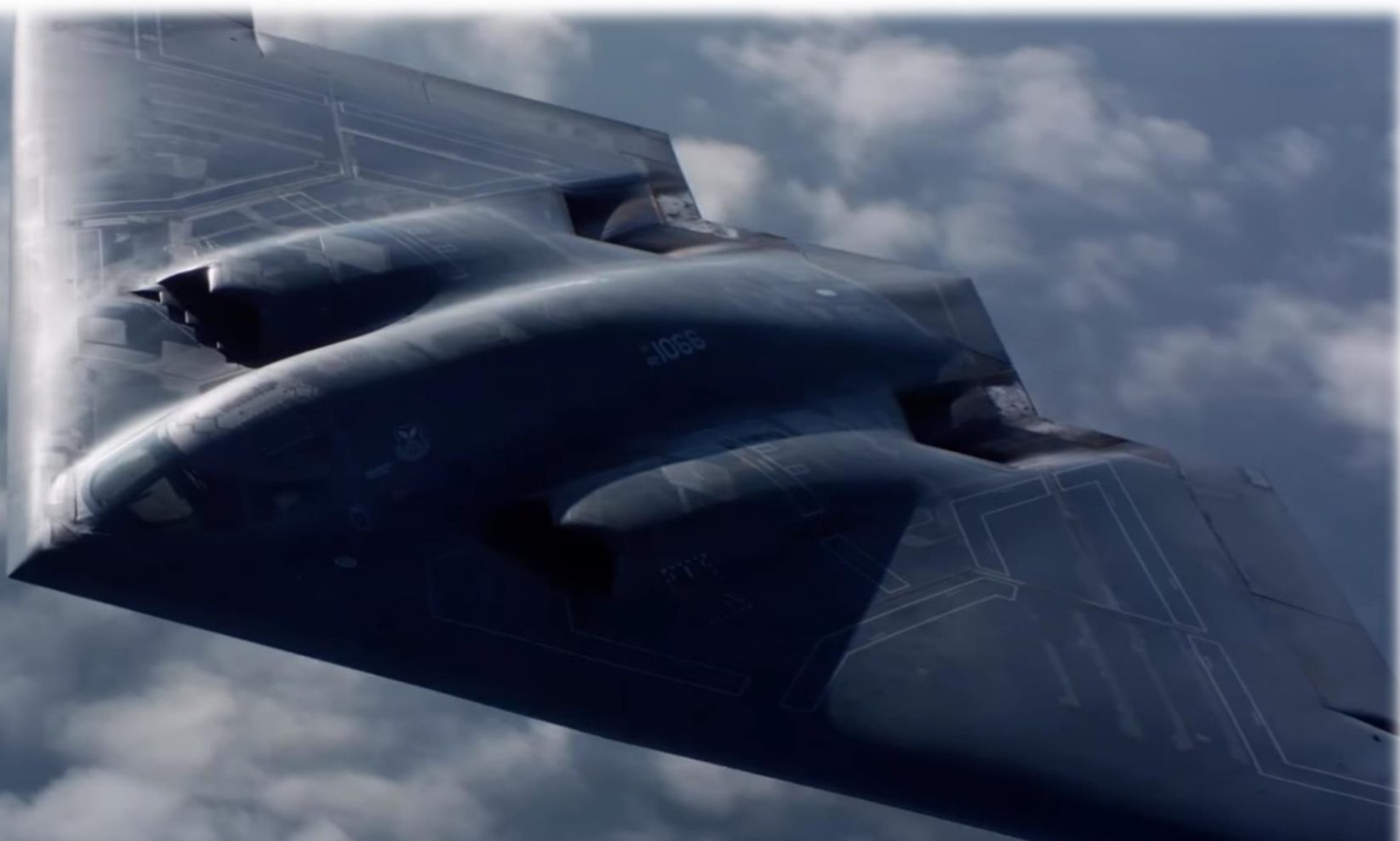
Sok esetben egyáltalán nem észlelni azonnal a felhasználó egy vírus jelenlétét a rendszerében!

Néhány most is terjedő vírus:

BLZS[©]

Lopakodó vírusok:

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



Makró vírusok:

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



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.



Trójai:

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



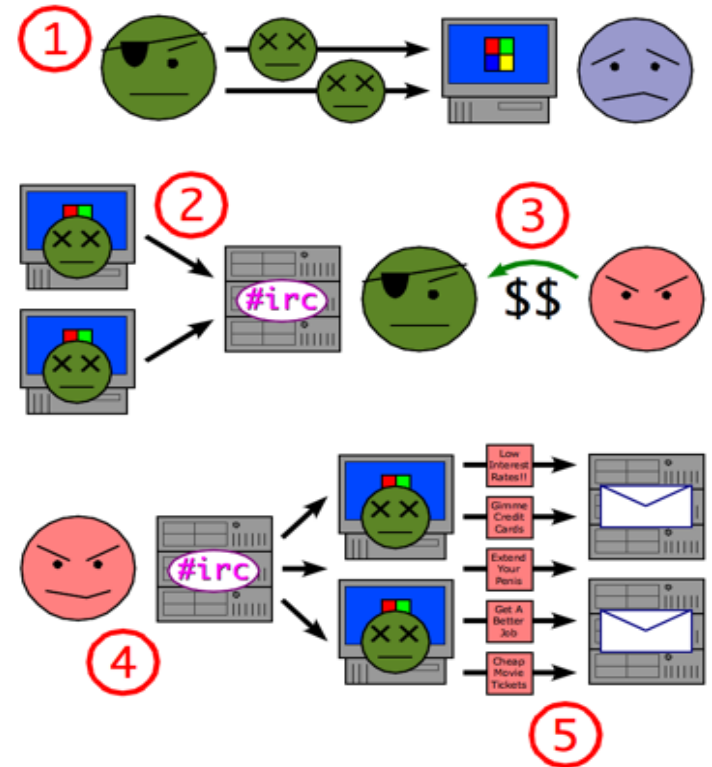
Keylogger programok:

- 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

- **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 károkozók is az operációs rendszer illetve a víruskereső alkalmazások elől.



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:

- 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.

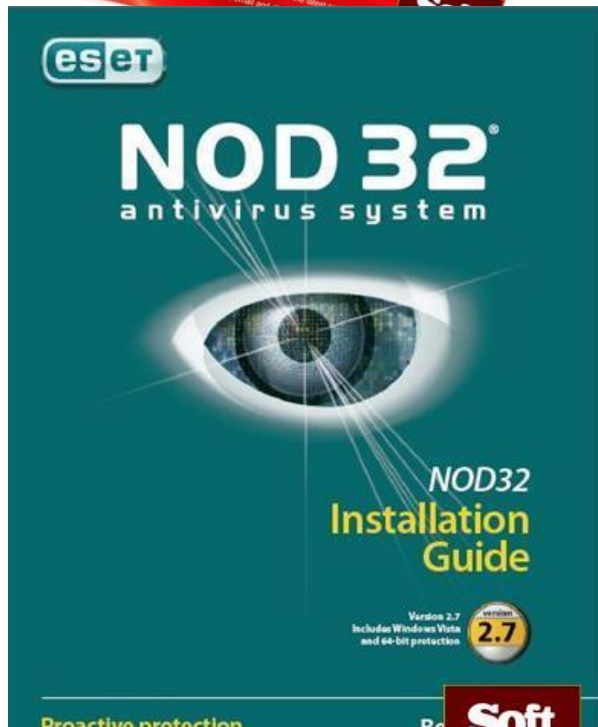
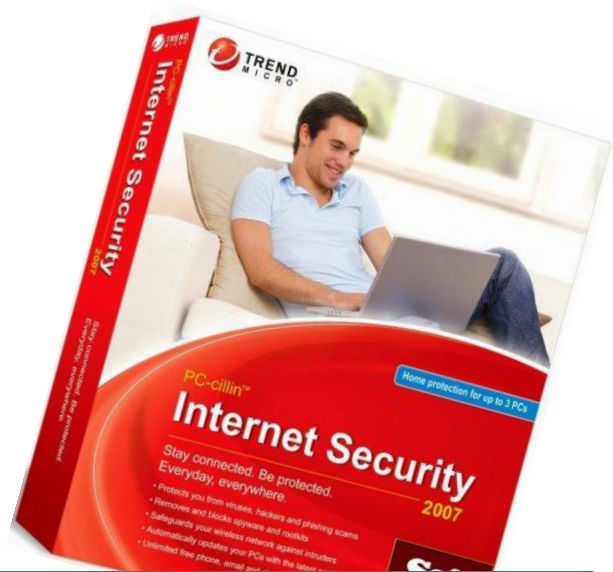
```
Thunderbyte virus detector v8.01 - (C) Copyright 1989-1997 Thunderbyte B.U.

T-----WARNING!-----d
P
W C:\NUTINTH_SHELL.COM s
  probably infected by an unknown virus
T
r Heuristic flags:cFMU l
c e
  c No checksum / recovery information (Anti-Vir.Dat) available. 1
  F Suspicious file access. Might be able to infect a file. 1
M Memory resident code. The program might stay resident in memory.
U Undocumented interrupt/DOS call. The program might be just tricky
  but can also be a virus using a non-standard way to detect itself. 9
T
U
U
U D)delete, K)kill, R)rename, S
W S)can next, N)onStop continue, Q)uit TbScan? > 2
W
W
X
Z
T
H
TL.EXE <Dos exe > J
TLINK.EXE <Win 16-bit> w J
TS.EXE <Dos exe > J

Elapsed time: 00:09
Kb / second: 551
```

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

Szinte mindegyik vírusirtó program felismeri a vírusokat de irtani csak néhány képes.

Nagyrészüik nem tesz mást csak rejtőzködik, de vannak vírusok amelyek tönkreteszik állományainkat, leformázzák a merevlemezünket, vagy nem engedik, hogy újraindítsuk a szg.-et, esetenként 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 víusról, 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!