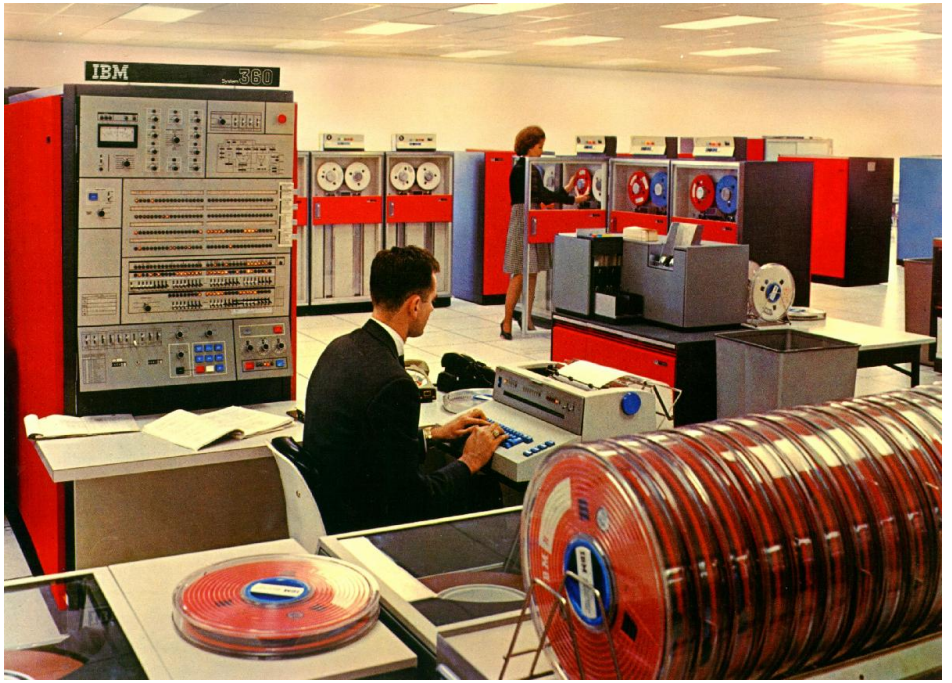
# 1987-2014
# Fejlődő kártevők, lemaradó felhasználók


ANTI VIRUS BLOG

# BEMUTATKOZÁS

Csizmazia-Darab István [Rambo]




**Szakmai tapasztalat:**

- 1979-1980: FÜTI, R20/R40 nagygépes operátor
- 1981-1987: HUNGAROTON hanglemez stúdió, stúdiós
- 1988-1990: Volán Tefu Rt, programozó
- 1990-2000: ERŐTERV Rt, programozó + vírusadmin egy 400 gépes hálóban
- 2001-2003: 2F Kft, F-Secure és Kaspersky support, Vírus Híradó főszerkesztő
- 2003-2005: IDG, PC World online szerkesztő, újságíró
- 2006-2007: Virus Buster Kft, kártevő elemző, sajtóhír felelős
- 2007-2014: Sicontact Kft, IT biztonsági szakértő

ANTI VIRUS BLOG

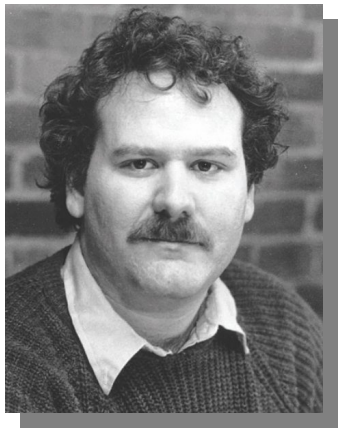
# RÖVID VÍRUSTÖRTÉNELEM

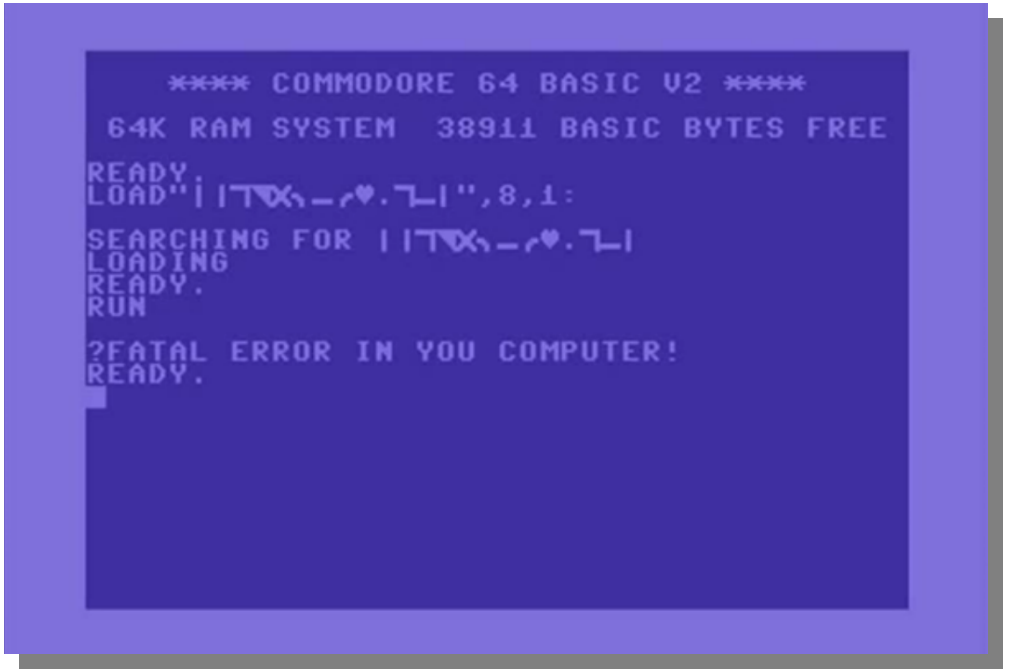
**1981.** Elk Cloner - Apple II. boot szektor

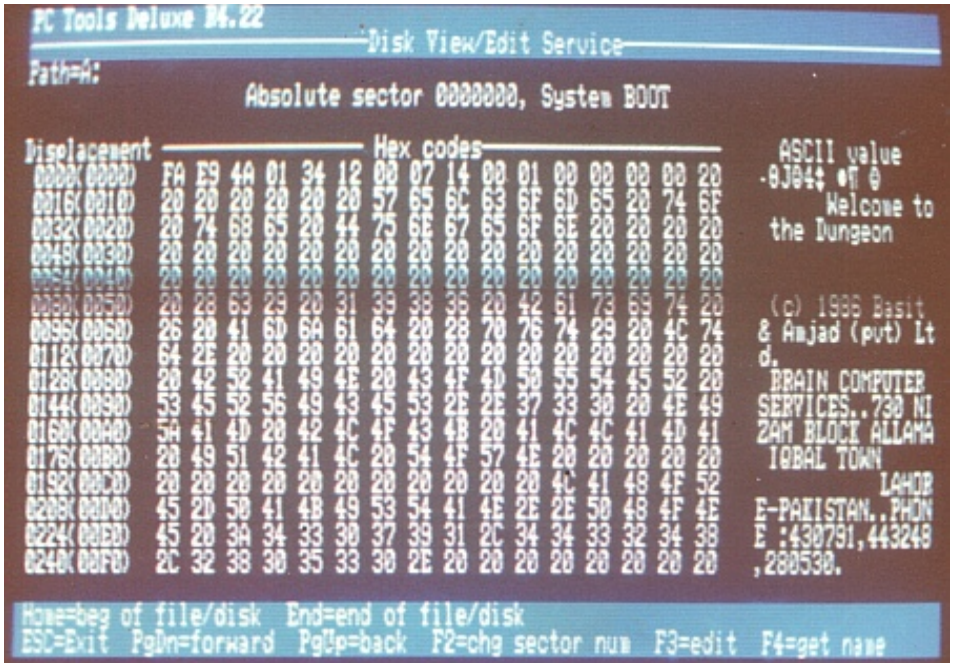
**1983.** Fred Cohen - UNIX VAX 11/750
Programkód megírása: 8 óra, teljes fertőzés: 30 perc

**1986.** Az első C64 vírus: BHP, Bayerische Hacker Post

**1987.** Brain Pakistan - Basit Farooq Alvi és Amjad Farooq Alvi





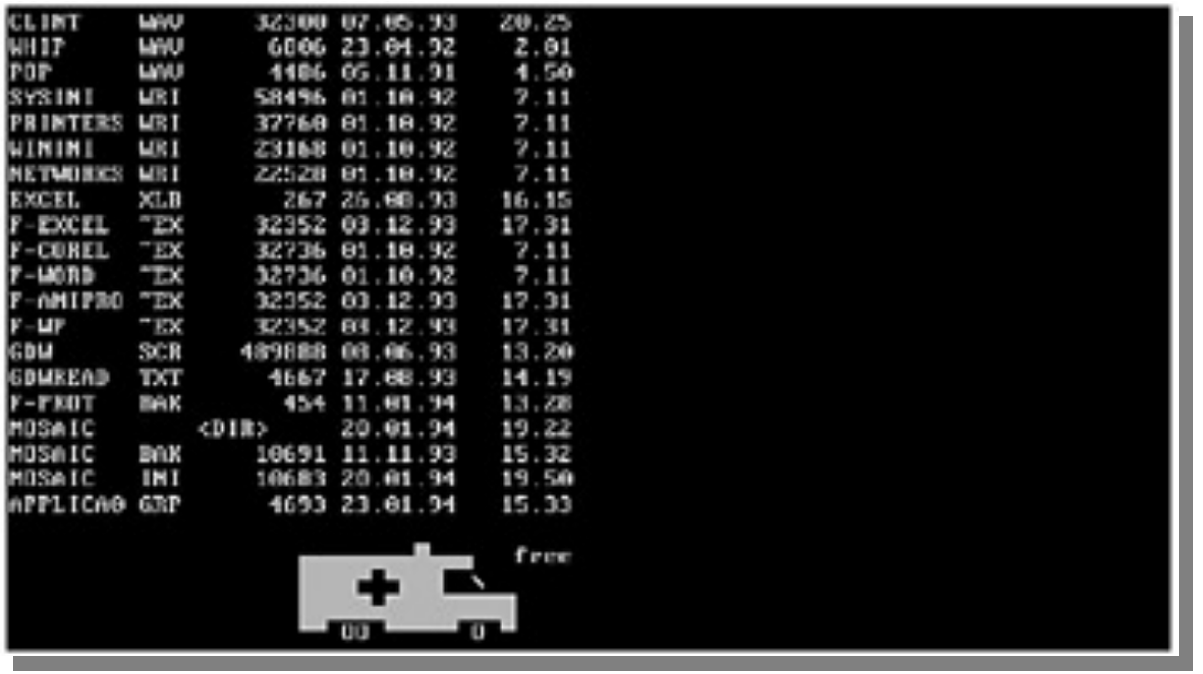
# KEZDETBEN LÁTVÁNYOS KÁRTEVŐK

**1989.** Bulgária
Yankee Doodle

**1989.** Izrael
Saddam vírus
SCANV68.ZIP

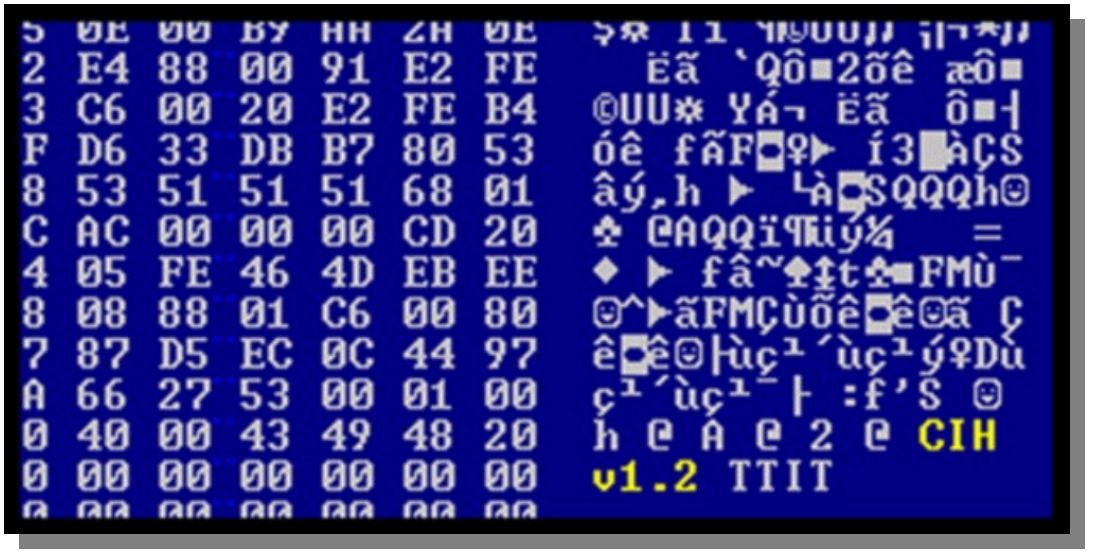
```
                        .COM files: Extends .COM files. Adds about 918 bytes to
                                    the end of the file.
                        .EXE files: Not infected.
Infection trigger...: every call to INT 21h
Interrupts hooked...: 21h, 6Bh.
Damage.............: Prints the string:
                                    HEY SADAM
                                    LEAVE QUEIT BEFORE I COME
Damage trigger......: Counts the number of times INT 21H was requested
                                    and on every eight time will print the string.
```

**1990.** Németország (NSzK)
Ambulance



# KÉSŐBB DURVUL A PAYLOAD...

**1998. június - BIOS chip CIH**
- A BIOS PROM felülírása
  a gép nem tud bootolni
  floppyról sem
- Tajvani készítője Chen Ing-Hau
- 1998. szeptember
  fertőzött CHIP és PC GURU
  CD melléklet




- fájltörlés
- BIOS törlés
- fájl felülírás
- MBR felülírás
- polimorfizmus
- exe tömörítők

- rejtőzködés
- rootkitek
- hátsó ajtó
- botnet
- BIOS-os kártevők
- bootkitek
- kormányzati kémprogramok

rongálás, kémkedés, anyagi haszonszerzés, botnetek, szabotázs

# AUTOMATIZÁLT TÁMADÁSOK

- Profi bandák működése világszerte

- 2005. Az USA-ban több pénz az elektronikus csalásokból, mint a drogkereskedelemből: 105 milliárd dollár


- 2010. U.K. Zeus kártevő, 20 millió GBP, 37 öszvér (mule) elítélése

- Olcsó botnetek, 24 órás supporttal bérelhető


- Egyre olcsóbbak az exploit kitek, pár ezer helyett már pár száz dollárért
- Egyre kisebb vállalatok is célpontba kerülnek
- 2012. december tökéletes magyarságú ZEUS kártevő az OTP, CIB bank ellen

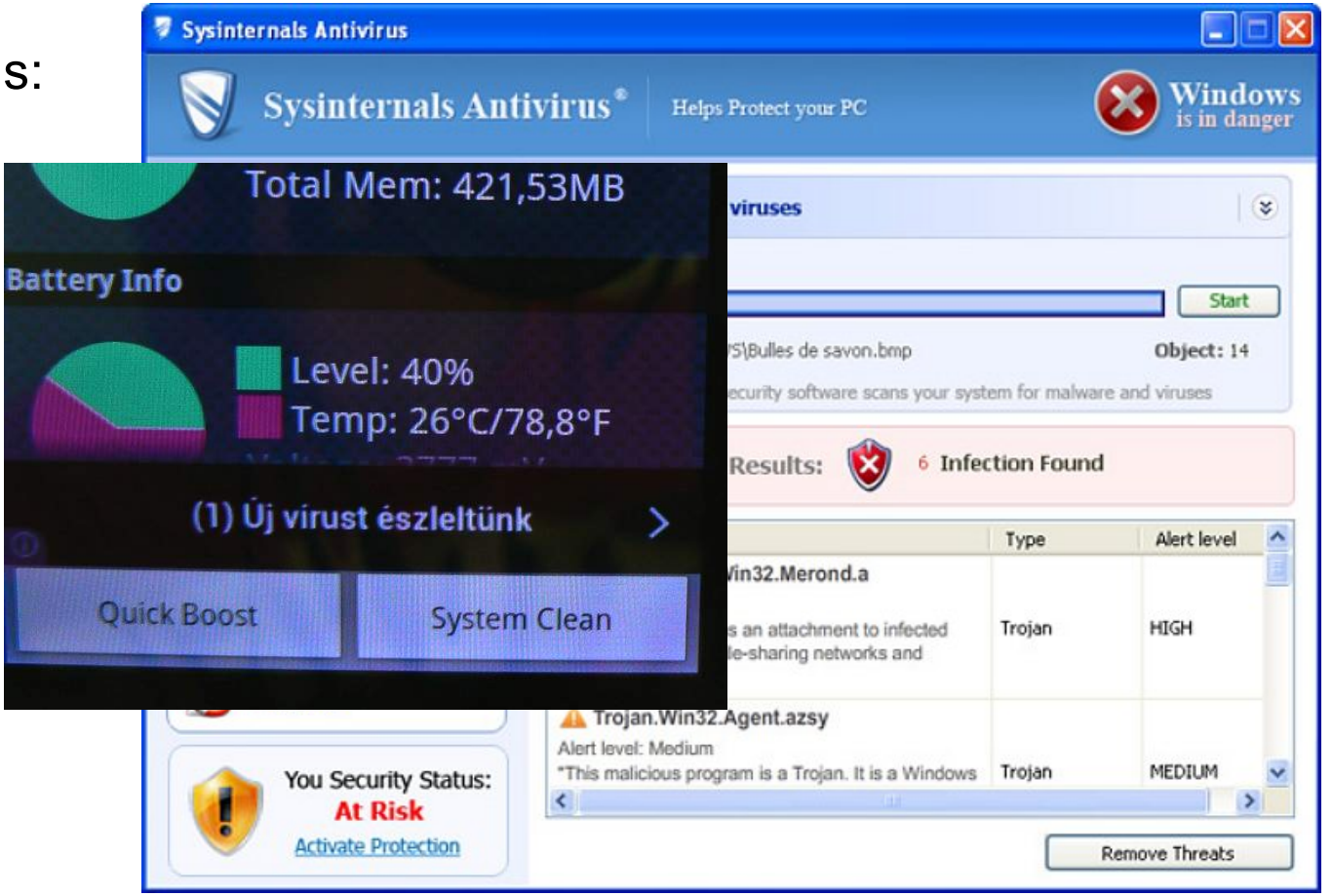
- Bitcoin bányászat: egy kétmilliós hálózat esetén az elérhető profit 58 ezer dollár NAPONTA, 1.7 millió pedig havonta
- Hackertámadás miatt becsődölt Mt. Gox (tőzsde) és FlexCoin (bank)

# HAMIS ANTIVÍRUSOK

- Hamis antivírus business, 50 USD a semmiért

- 2008. Hamis antivirus: a tagok 32 millió forintnyi összeget keresnek - hetente

- 2010. Hamisított antivírus:
  Wireshark Antivirus
  SysInternals Antivirus
  Win 7 Smart Security
  XP Smart Secuity




- Később Macintoshra:
  Mac Defender,
  Mac Protector,
  Mac Security

- És aztán Androidra is:
  Opera Virus Scanner
  Android Virus Scanner
  Android Defender Platinum

ANTI VIRUS BLOG

# POLICE TÍPUSÚ KÁRTEVŐK

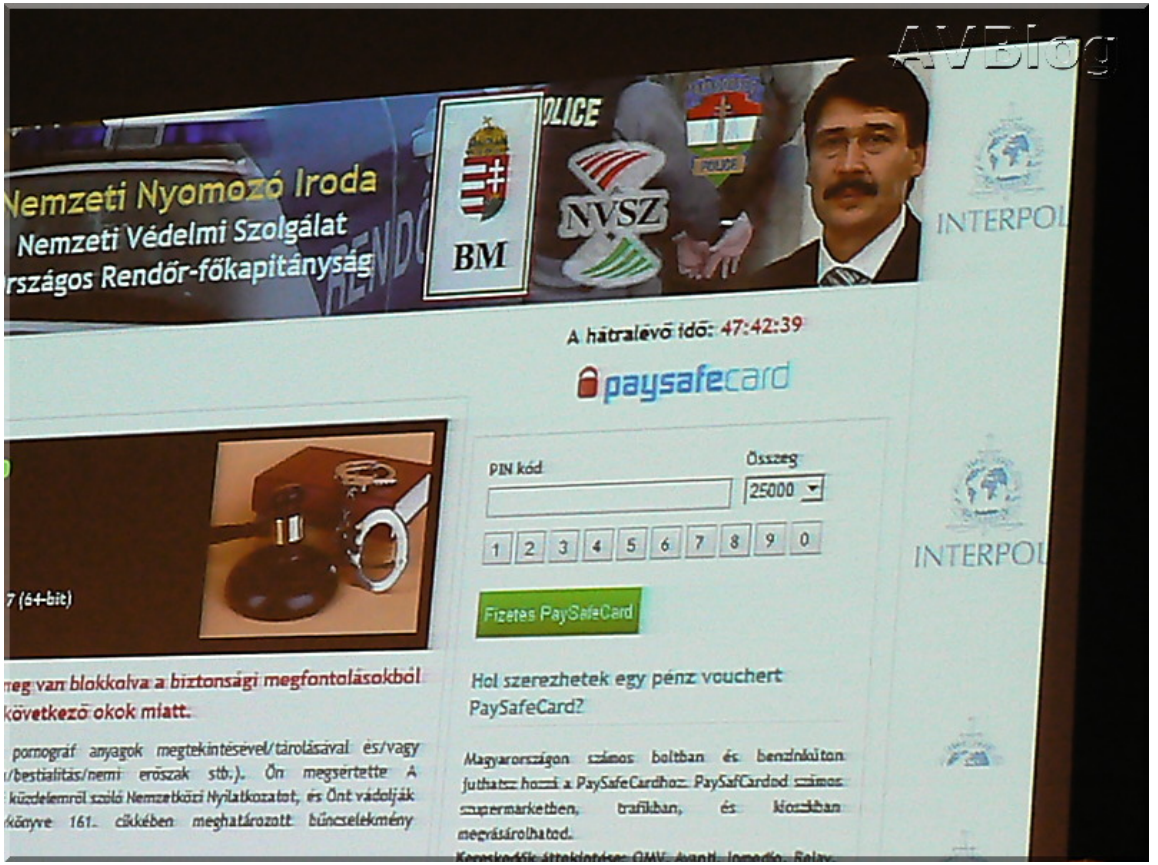
- 2010-2013. RIAA, MPAA, ICCP, FBI ág

- Saját országbeli rendőrség

- Hamis szerzői jogi, pedofil vád

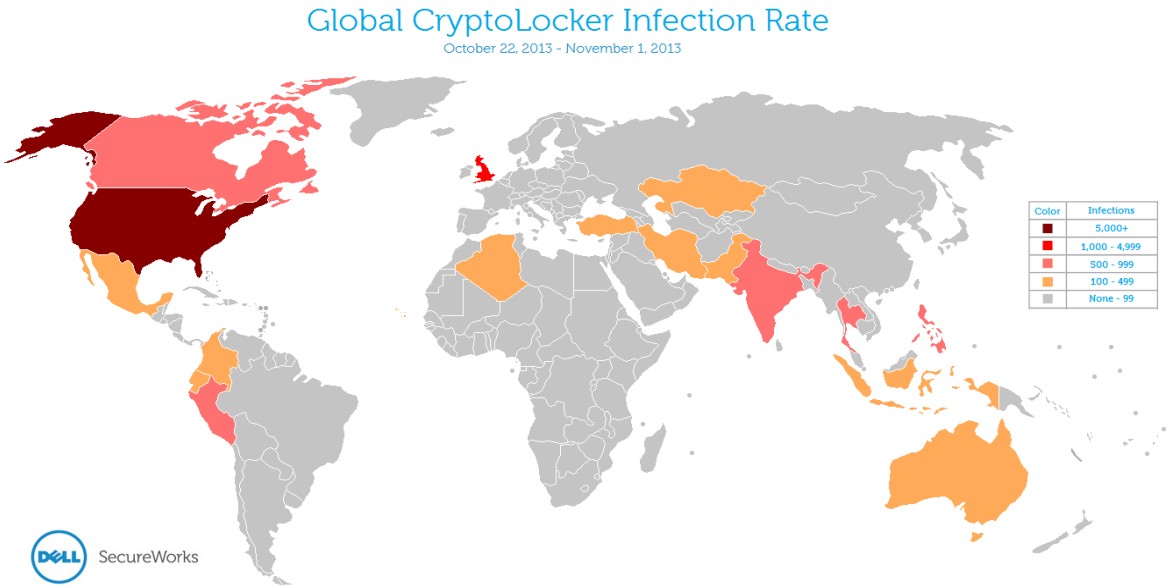
- Állítólagos szexuális visszaélést "bizonyító" képek, névvel, születési hellyel, idővel

- A nagyobb hitelesség miatt az áldozat böngészőjéből elérhető előzménylisták



# ZSAROLÓ CRYPTOLOCKER

- Törli a backupot és a Shadow Copy-t
- Letiltja a SAFE módot - új felhasználói fiókkal mégis választható
- USB eszközökkel is terjed, trójaiból féreg lett
- Váltságdíj fizetés után sem biztos, hogy megérkezik a privát kulcs
- A 2.0-ban már 4096  bites egyedi RSA kulcs




- Minden felmappelt hálózati, felhős, és külső tárhely is elkódolásra kerül
- Virtuális Windows alatt is fertőz, a megosztott mappákban is pl. Linux
- 250,000 fertőzött rendszer, $35 millió USD váltságdíj  (2014. DELL Secure Works)

ANTI VIRUS BLOG

# HOZZÁÁLLÁS I.

- Figyelmetlenség
- Képzetlenség
- Hiszékenység
- Közömbösség
- Frissítések hiánya
- Mentések hiánya


PEDIG:
- Az események gyorsabban változnak
- Az események gyakrabban történnek

**A fejlesztők és szolgáltatók is felelősek**
- Facebook: alapértelmezett megosztás mindent mindenkivel
- Microsoft: alapértelmezetten rejtett ismert fájltípusok kiterjesztése, default autorun, automatikusan lefutó office makrók, automatikusan lefutó Outlook Express mail preview, alapértelmezett rendszergazdai jogok, stb.

*"If you have to go to the command line people aren't going to use it. If you have to go three menus deep, people aren't going to use it."*
*<Edward Snowden>*

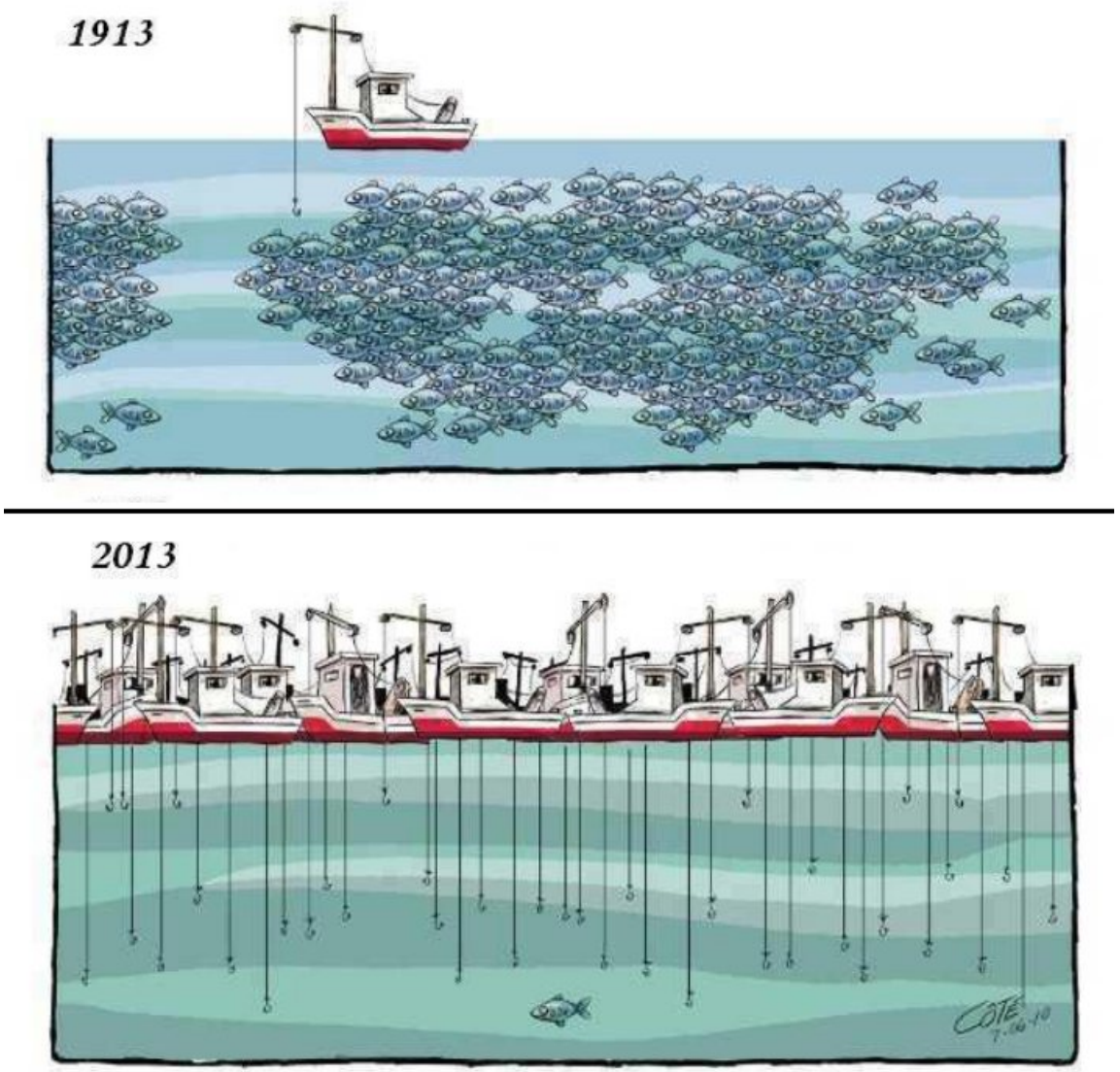
ANTI VIRUS BLOG

# HOZZÁÁLLÁS II.

**2013. North Carolina State University**
- 89% állítja, hogy nem lehet becsapni adathalász e-mail üzenettel
- a teszt szerint csak 7.5%

**2012. ESET USA**
- a dolgozók 80%-a BYOD
- az okostelefonon 24%-án céges adatok
- a noteszgépek 41%-án céges adatok

**2013. ESET Írország**
- 45% ingyenes AV
- 36% Internet Security
- 6% nem is tudja, mit használ




ANTI VIRUS BLOG

# TÉVHITEK ÉS CÁFOLATOK I.

***"Vírust csak warez/pornó oldalakon lehet kapni"***


- Fertőzött bannerek
- Fertőzött gyári eszközök
- Feltört oldalak, feltört szerverek
- Gyenge biztonságtudatosság
- Nem lehet "okosan" netezni
- Célzott testre szabott social engineering trükkök
- APT támadások, pl. NY Times

ANTI VIRUS BLOG

# TÉVHITEK ÉS CÁFOLATOK II.

***"Az 'abcd1234' elég erős jelszó"***


- Sok a gyenge jelszó
- Adobe, Forbes, Kickstarter, Linkedin kiszivárogtatások tanulságai
- 2013 worst passwords: password, 123456, letmein, abc123, adobeadobe, stb.
- Sok felhasználónál ugyanaz a jelszó mindenütt
- Sok felhasználó a jelszó-emlékeztetőkben egy az egyben megadja a jelszavát
- 16% sosem változtatja meg a jelszavát
- 18% figyelmen kívül hagyja, ha jelszócserére figyelmeztetik

# TÉVHITEK ÉS CÁFOLATOK III.

***"Aki ért a géphez, annak nincs szüksége vírusirtóra"***

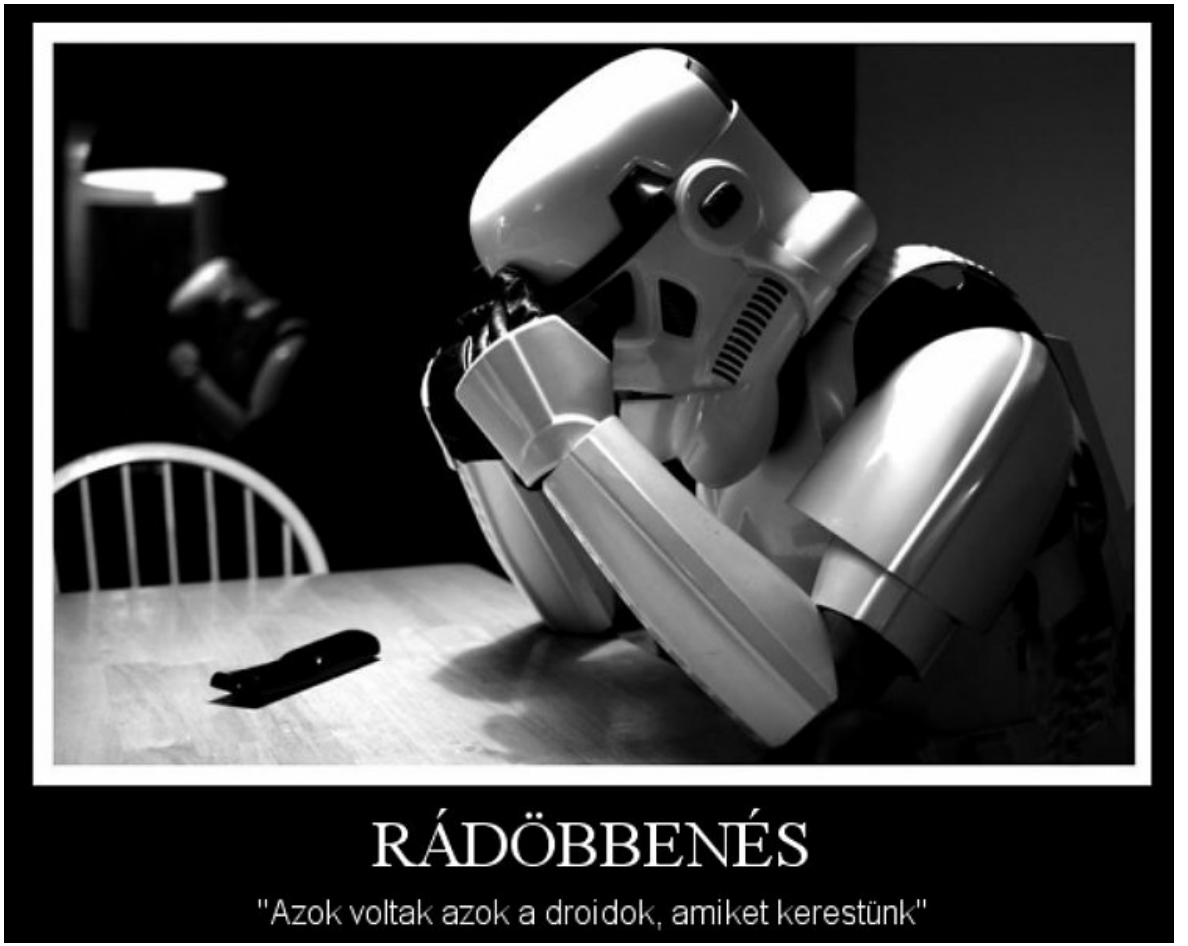

- A brit netezők több, mint fele nem telepít antivírust a gépére (2014)
- 2011. Magyarország - 26% kikapcsolja, hogy mégis megnézze a fertőzött weboldalt
- 2011. Magyarország - 17% kikapcsolja, hogy mégis futtassa a fertőzött állományt
- Rootkitek, bootkitek, BIOS szintű "észrevehetetlen" kártevők

*"Tökéletes védelem sajnos nincs. Ha a felhasználó képzettebb, akkor a védelem is eredményesebb."* *<Szőr Péter, 1970-2013>*

ANTI VIRUS BLOG

# MIT HOZHAT A JÖVŐ? I.

- Egyre több kártevő, egyre több támadás, sajnos ez a realitás
- Durvul a CryptoLocker vonal, gyorsabb, erősebb kulcs, több fájlkiterjesztés, jobb rejtőzködés
- A polimorfizmus miatt muszáj a viselkedéselemzést kiemeltebben fejleszteni
- Rengeteg JAVA alapú támadás




- Az Android lett az új vadnyugat, az új Windows.
- 81% részesedés, bárki lehet fejlesztő, figyelmen kívül hagyott 2 faktoros autentikáció
- Hamis tanúsítványok asztali webböngészőnél figyelmeztetés, mobil alkalmazásoknál semmi
- A dolgok internete, Android @ home, Google Glass, stb.

# MIT HOZHAT A JÖVŐ? II.


Software Update

- További kifinomultabb kormányzati kártevők, a kiszivárogtatók megfélemlítése, megbüntetése
- Még inkább bizalmi kérdés lesz a biztonsági program és szolgáltatás választása
- Snowden után a nyílt forráskód további előretörése várható
- Rossz példa: 2014-ben havonta csupán egyszeri Microsoft Patch Thuesday
- Jó példa: a Macintosh Mountain Lion óta bevezetett napi, titkosított csatornán történő frissítése
- Több és rendszeres biztonsági képzés a munkavállalóknak
- Már az általános iskola 1. osztályától tananyag kellene az internetes veszélyekről