

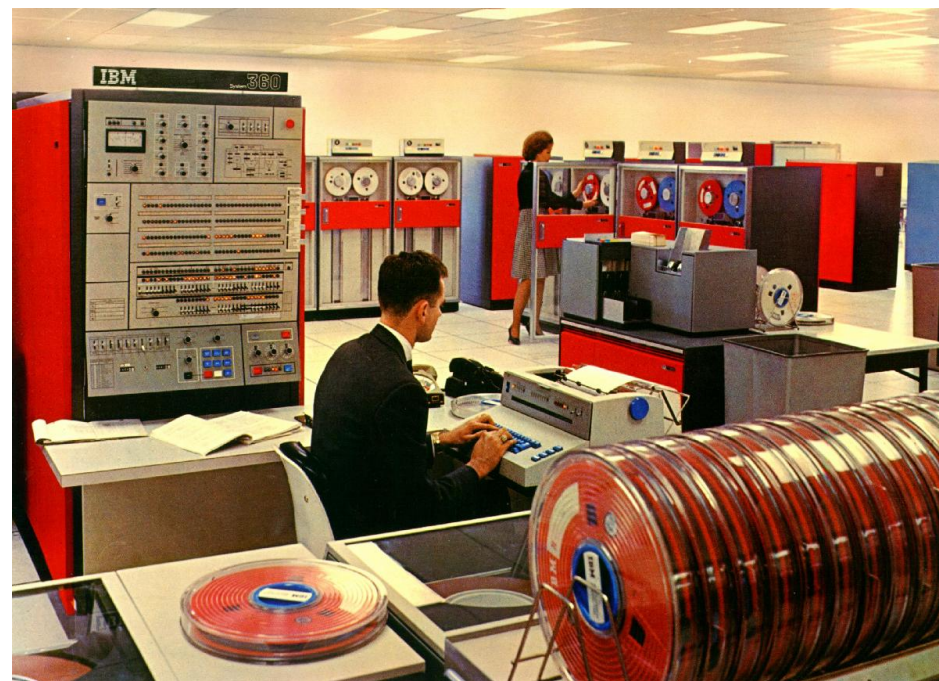
1987-2014

Fejlődő kártevők, lemaradó felhasználók



BEMUTATKOZÁS

Csizmazia-Darab István [Rambo]



Szakmai tapasztalat:

- 1979-1980: FÜTI, R20/R40 nagygépes operátor
- 1981-1987: HUNGAROTON hanglemezz 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



RÖVID VÍRUSTÖRTÉNELEM

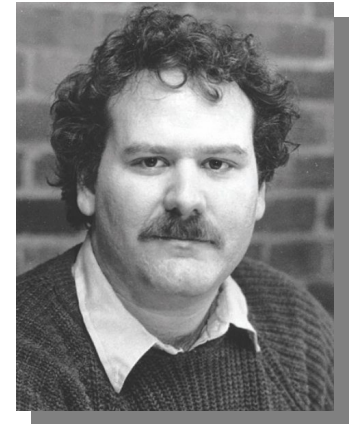
1981. Elk Cloner - Apple II. boot szektor

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



```
**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM 38911 BASIC BYTES FREE
READY.
LOAD" | ITX - r. 7 | ", 8, 1:
SEARCHING FOR | ITX - r. 7 |
LOADING
READY.
RUN
?FATAL ERROR IN YOU COMPUTER!
READY.
```

```
PC Tools Deluxe 34.22 Disk View/Edit Service
Path=A:
Absolute sector 0000000, System BOOT

Displacement Hex codes ASCII value
0000(0000) FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20 -0J04: 01 0
0016(0010) 20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F Welcome to
0032(0020) 20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20 the Dungeon
0048(0030) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050) 20 28 63 23 20 31 39 38 36 20 42 61 73 68 74 20 (c) 1986 Basit
0096(0060) 26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74 & Amjad (pvt) Lt
0112(0070) 64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20 d.
0128(0080) 20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20 BRAIN COMPUTER
0144(0090) 53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49 SERVICES..730 NI
0160(00A0) 5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41 2AM BLOCY ALLAMA
0176(00B0) 20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20 IQBAL TOWN
0192(00C0) 20 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52 LAHOB
0208(00D0) 45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E E-PAKISTAN..PHON
0224(00E0) 45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38 E :430791,443248
0240(00F0) 2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20 ,280530.

Home=beg of file/disk End=end of file/disk
ESC=Exit PgDn=forward PgUp=back F2=chg sector num F3=edit F4=get name
```

ANTI VIRUS BLOG



KEZDETBEN LÁTVÁNYOS KÁRTEVŐK

1989. Bulgária
Yankee Doodle

```
.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

```
CLINT MWV 32300 07.05.93 20.25  
WHIT MWV 6006 23.01.92 2.01  
POP MWV 4406 05.11.91 4.50  
SYSINI MRI 58496 01.10.92 7.11  
PRINTERS MRI 37760 01.10.92 7.11  
WININI MRI 23168 01.10.92 7.11  
NETMIBKS MRI 22520 01.10.92 7.11  
EXCEL XLB 267 26.00.93 16.15  
F-EXCEL TEX 32352 03.12.93 17.31  
F-COREL TEX 32736 01.10.92 7.11  
F-MORB TEX 32736 01.10.92 7.11  
F-AMIPRO TEX 32352 03.12.93 17.31  
F-MP TEX 32352 03.12.93 17.31  
GDM SCR 489888 00.06.93 13.20  
GDMREAD TXT 4667 17.08.93 14.19  
F-FRMT BAK 454 11.01.94 13.20  
MOSAIC <DIR> 20.01.94 19.22  
MOSAIC BAK 10691 11.11.93 15.32  
MOSAIC IMI 10683 20.01.94 19.50  
APPLICAB GRP 4093 23.01.94 15.33
```



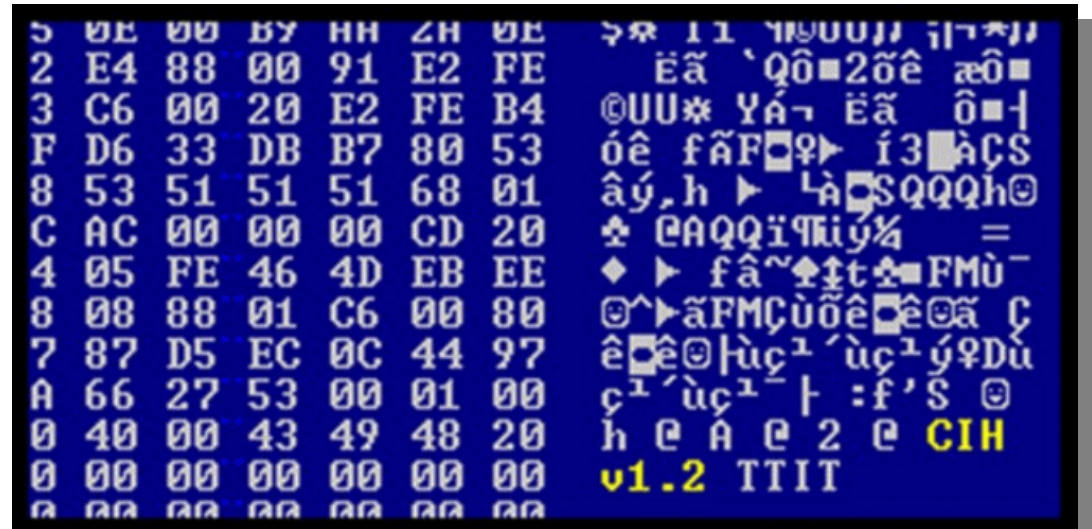
ANTI VIRUS BLOG



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



- fájl törlés
- 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)



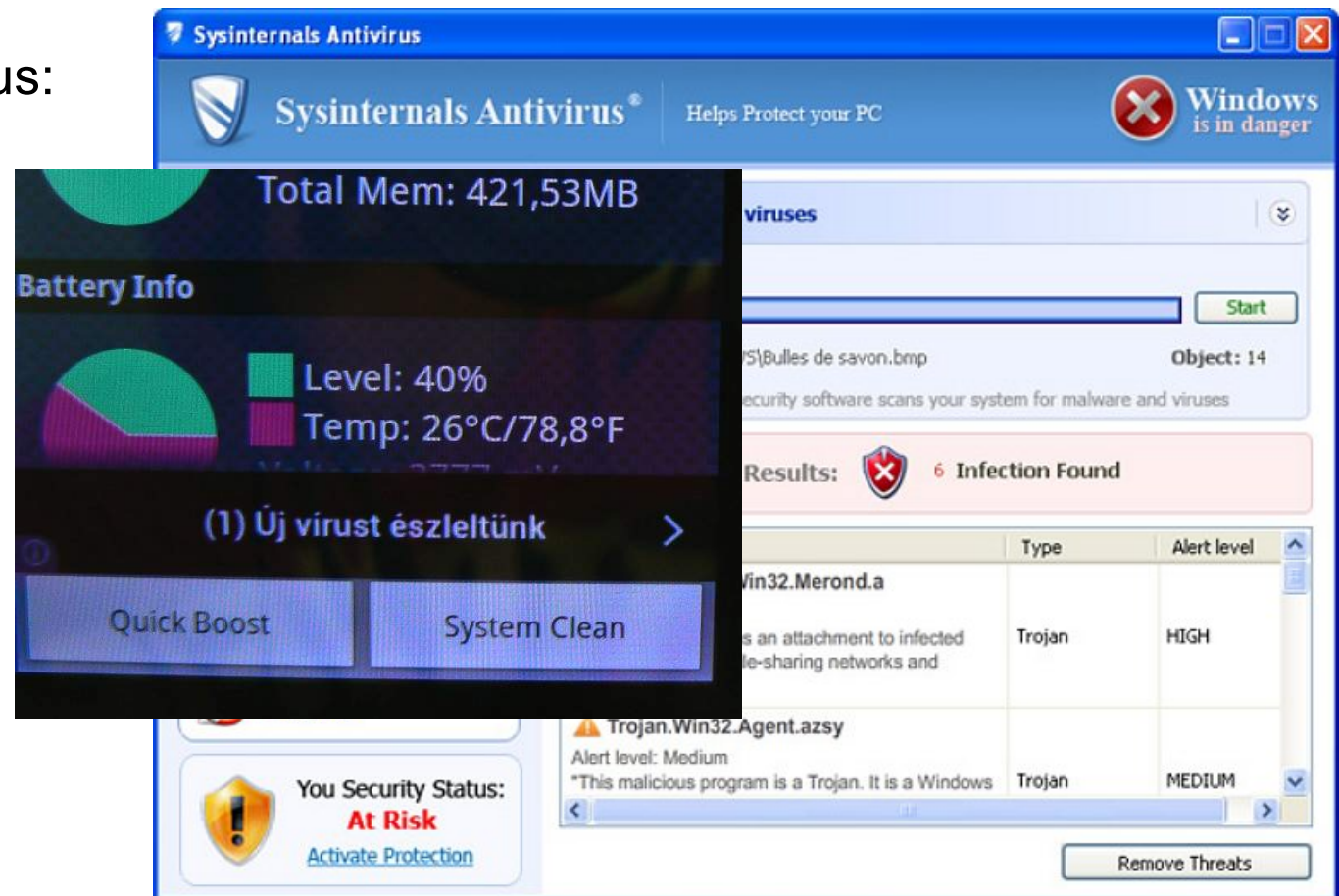
HAMIS ANTIVÍRUSOK

- 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 Security

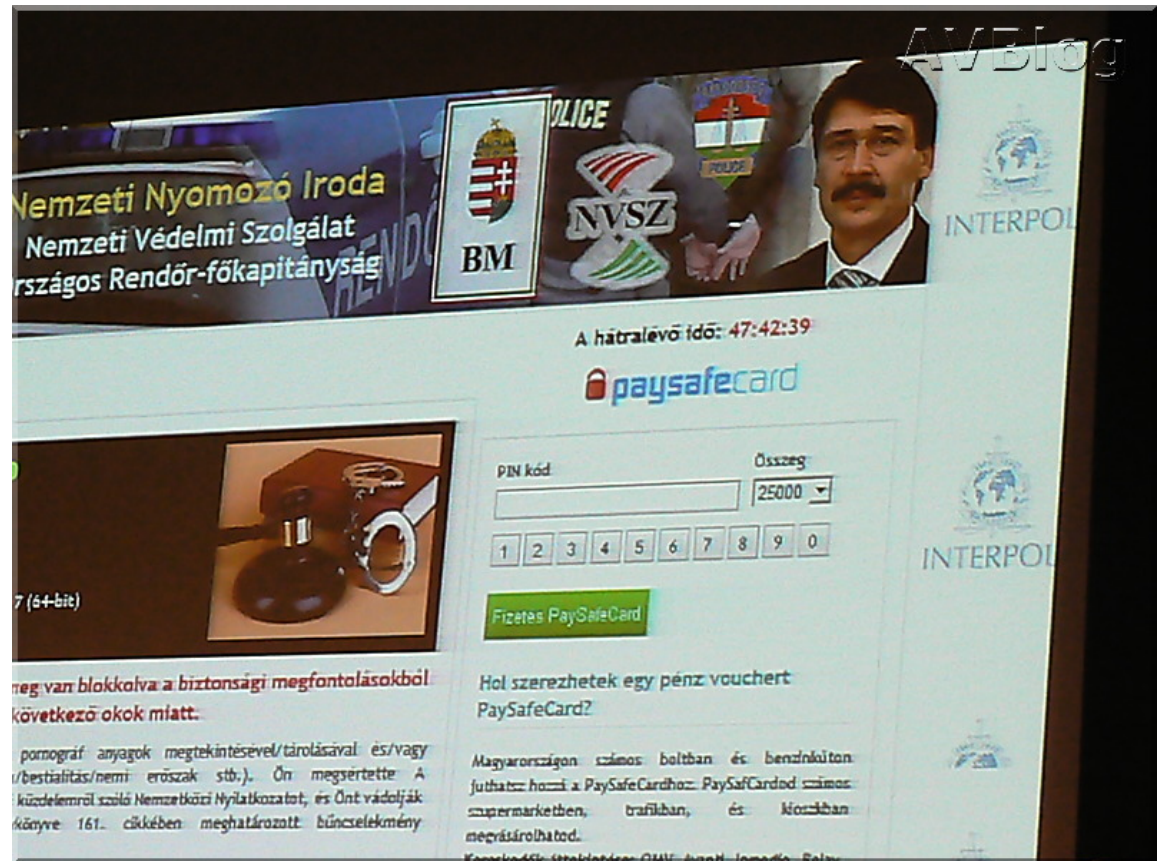
- Később Macintoshra:
 - Mac Defender,
 - Mac Protector,
 - Mac Security

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



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

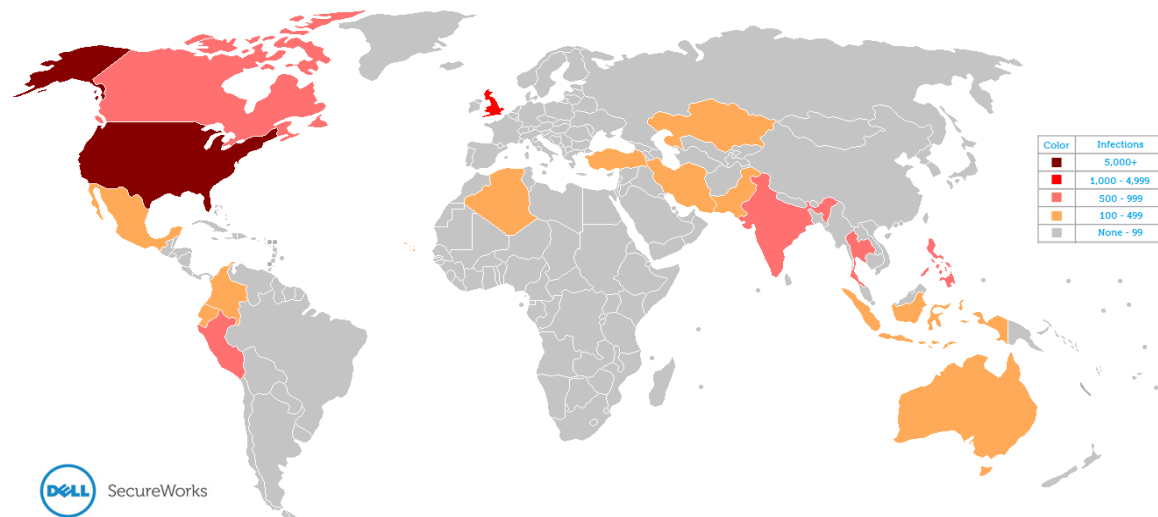


ZSAROLÓ CRYPTOLOCKER

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

Global CryptoLocker Infection Rate

October 22, 2013 - November 1, 2013



- 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 váltásdíj (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 fájl típusok 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>*



HOZZÁÁLLÁS II.

2013. North Carolina State University

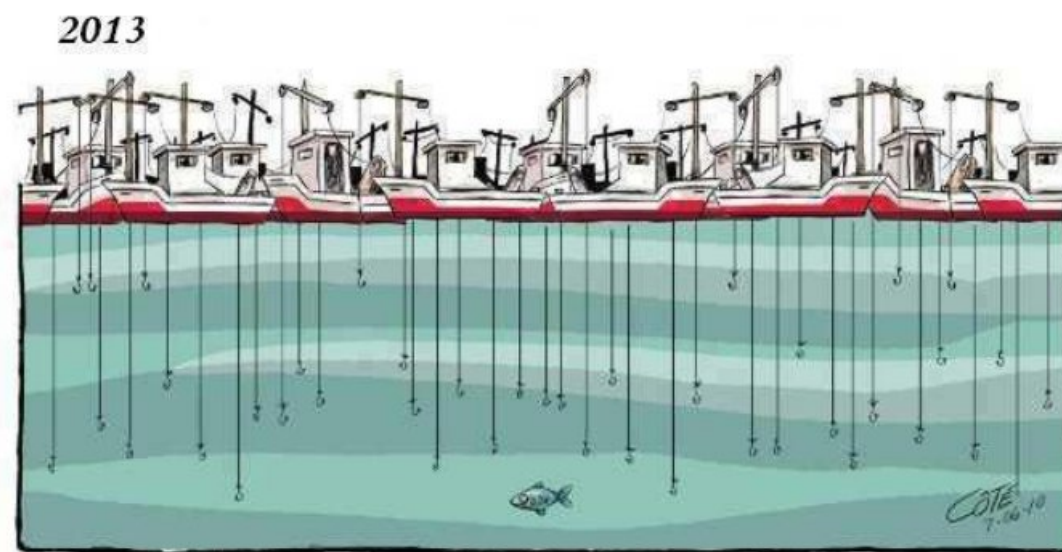
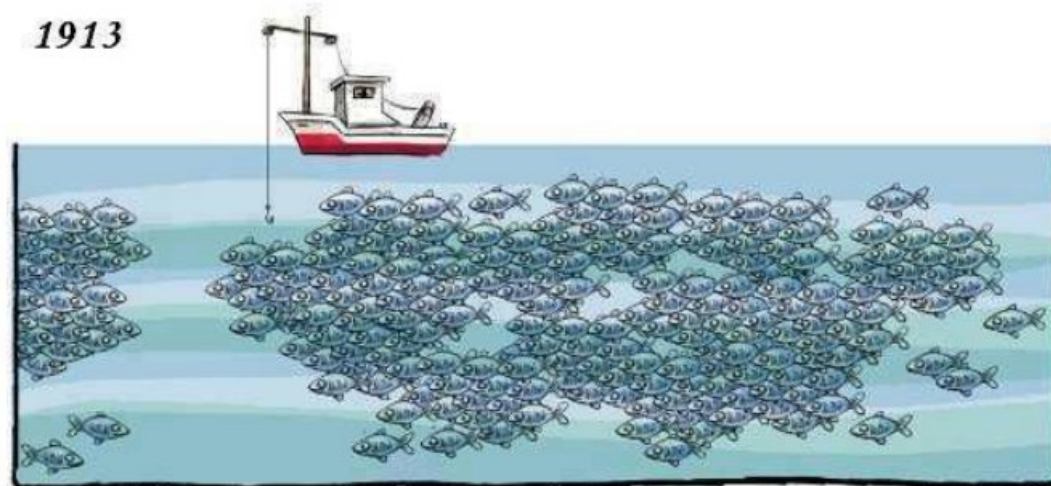
- 89% állítja, hogy nem lehet becsapni adathalász e-mail üzenettel
- a teszt szerint csak 7.5%

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"*

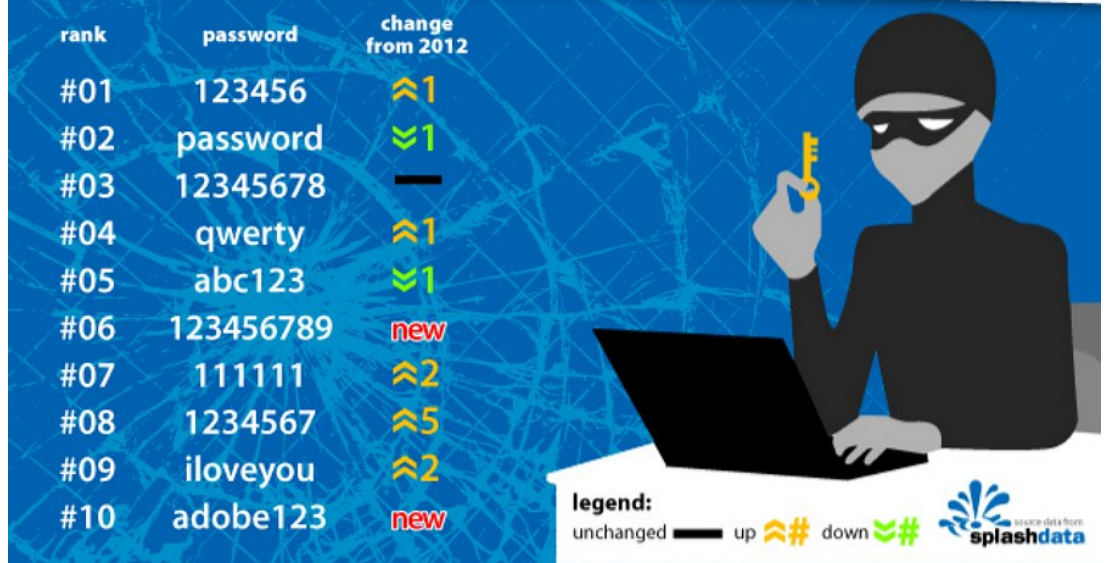
- Fertőzött bannerek
- Fertőzött gyári eszközök
- Feltört oldalak, feltört szerverek
- Gyenge biztonságtudatosság
- Nem lehet "okosan" netezni
- Célzott testre szabott social engineering trükkök
- APT támadások, pl. NY Times



TÉVHITEK ÉS CÁFOLATOK II.

"Az 'abcd1234' elég erős jelszó"

WORST PASSWORDS OF 2013



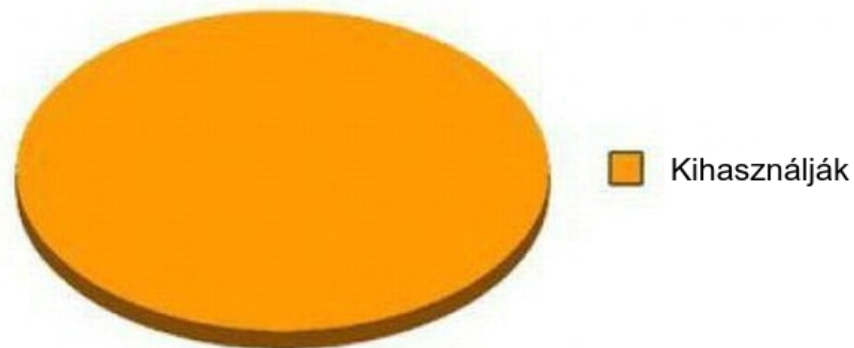
- Sok a gyenge jelszó
- Adobe, Forbes, Kickstarter, LinkedIn kiszivárogtatások tanulságai
- 2013 worst passwords: password, 123456, letmein, abc123, adobeadobe, stb.
- Sok felhasználónál ugyanaz a jelszó mindenütt
- Sok felhasználó a jelszó-émlékeztetőben egy az egyben megadja a jelszavát
- 16% sosem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



TÉVHITEK ÉS CÁFOLATOK III.

"Aki ért a géphez, annak nincs szüksége vírusirtóra"

MIT CSINÁLNAK A SZÁMÍTÓGÉPES KÁRTEVŐK A SEBEZHETŐSÉGEKKEL?



- 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 képzetebb, akkor a védelem is eredményesebb."
<Szőr Péter, 1970-2013>



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 Tuesday**
- **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

