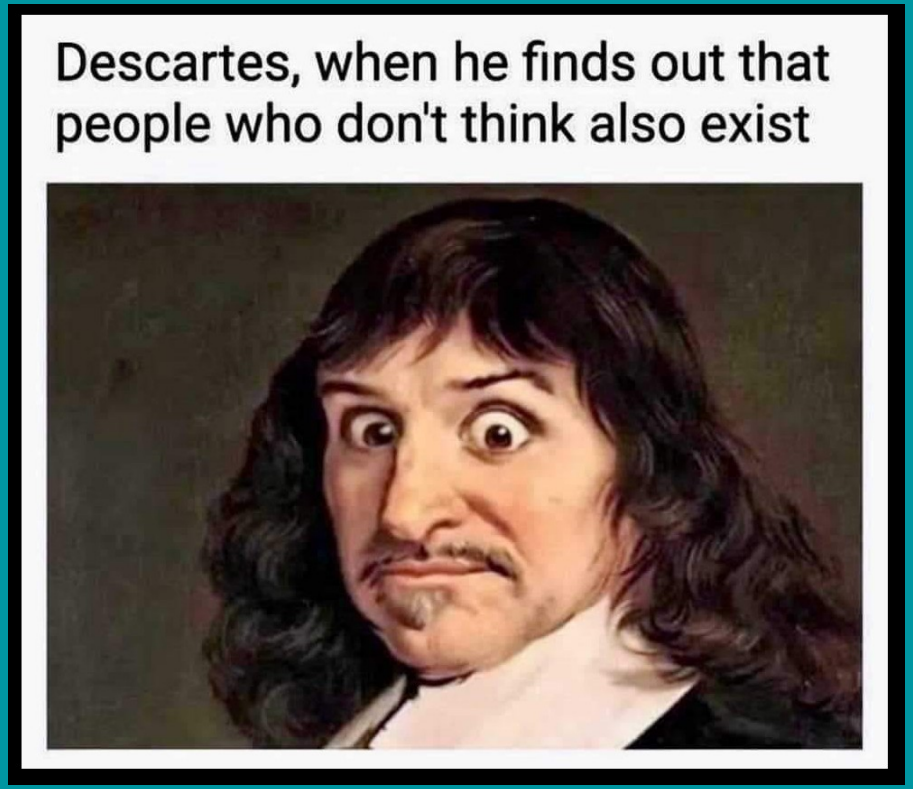
A vírustörténelem legnagyobb baklövései



ÓBUDAI EGYETEM

ESET Digital Security
Progress. Protected.

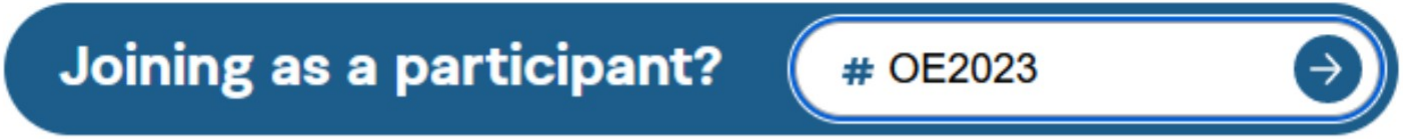
2023. december 6.

Csizmazia-Darab István

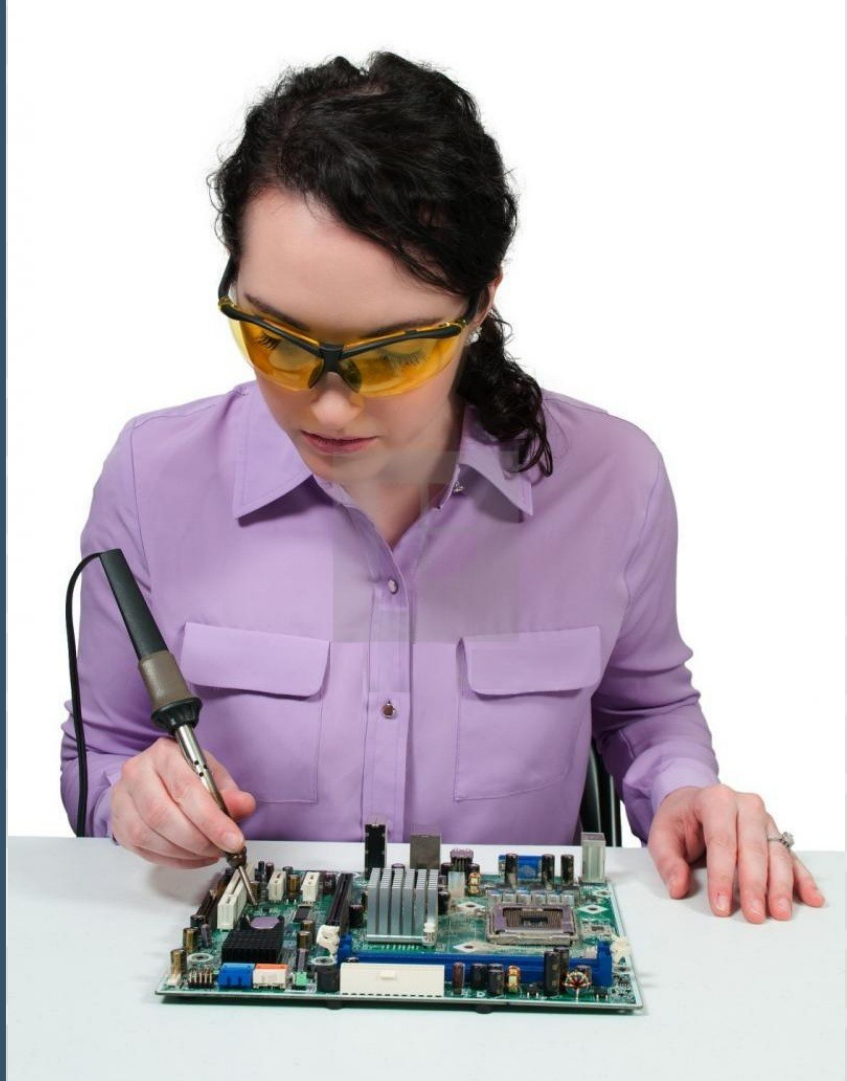
[Rambo]

IT biztonsági szakértő, ESET/Sicontact

www.slido.com



TARTALOM



- Egyszer volt, hol nem volt
- Kié a legnagyobb hiba?
- Főbb szerepekben
- Összegzés vagy ilyesmi

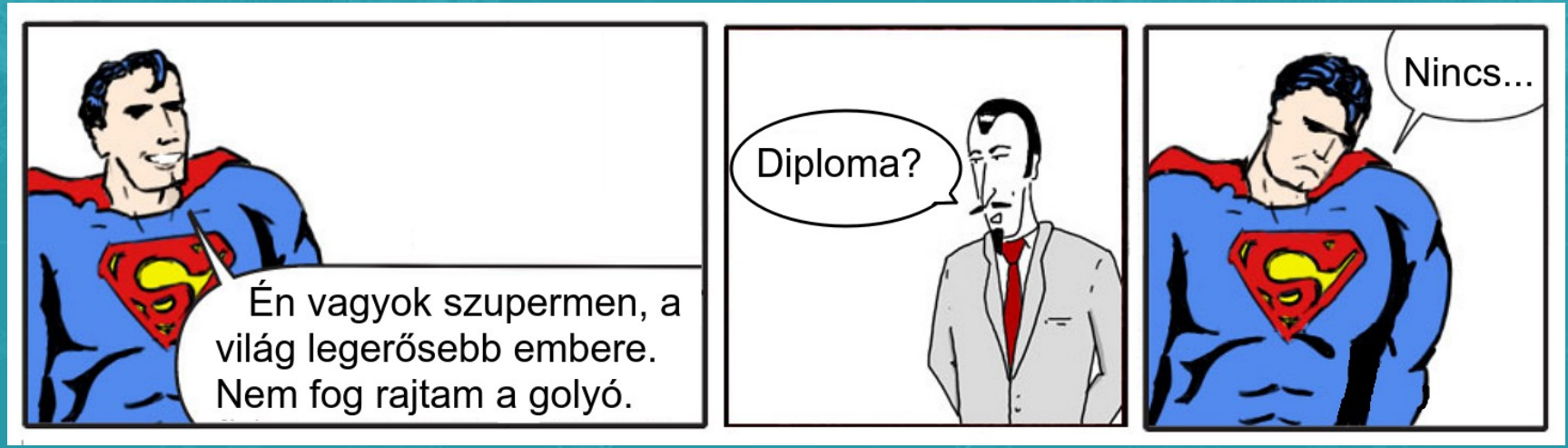
MINDEN JÓ VALAMIRE, HA MÁSRA NEM, HÁT ELRETTENTŐ PÉLDÁNAK. (MURPHY)

Egyszer volt, hol nem volt

"Ki a múltat háborgatja, folyjon ki a fél szeme.
De ki a múltat elfelejti, annak mind a kettő".
(Alexander Szolzsenyicin: A Gulág szigetvilág)

Egyszer volt, hol nem volt

“Semmi sem állandó, csak a változás maga.”
- fényképész, gyors és gépíró szakma
- 1526. a mohácsi vész, 1222. az Aranybulla
- kovalens kötés
- törtet törttel úgy osztunk, hogy a változatlan osztandót megszorozzunk az osztó reciprok értékével.



1986.


```
                    ASCII value
00 00 00 00 20      -0J04↕●¶0
6D 65 20 74 6F            Welcome to
6E 20 20 20 20      the Dungeon
20 20 20 20 20
20 20 20 20 20
61 73 69 74 20      (c) 1986 Basit
74 29 20 4C 74      & Amjad (put) Lt
20 20 20 20 20      d.
55 54 45 52 20      BRAIN COMPUTER
33 30 20 4E 49      SERVICES.. 730 NI
4C 4C 41 4D 41      ZAM BLOCK ALLAMA
20 20 20 20 20      .IQBAL TOWN
4C 41 48 4F 52                LAHDR
2E 50 48 4F 4E      E-PAKISTAN..PHJN
34 33 32 34 3B      E :430791,443248
20 20 20 20 20      ,280530.
```

- Az MSZMP KB aláírja a McDonald’s kialakításáról szóló szerződést :-D
- Stallone Cobra
- Ronald Reagan az USA elnöke
- Csernobili atom katasztrófa
- **Brain vírus (Pakisztán): név, cím, telefonszám a kódban :-)**

Egyszer volt, hol nem volt

1989.02.07.
- VIRUSCAN 0.3V19: 19 fő vírustörzs és alváltozatok.
- Az összes fertőzés 90%-a Pl. Casdae-1701 (Potyogós)

III. ÉVFOLYAM 25. SZÁM
1988. DECEMBER 14.
MONITOR
9

Hozzászólás vírusügyben

Több alkalommal írtak lapjukban és a *Mikrovilágban* is vírusokról szóló cikkeket. Ezek többnyire külföldi példákra hivatkoztak.

A vírus azonban hazánkat is elérte. Jó nevű felsőoktatási intézményünk több gépe is elfertőződött már. Még belegondolni is rossz, mi történik, ha minden felhasználó továbbadja barátainak, környezetének a veszélyes kórt. Most a vírusok egyik legkellemetlenebb fajtájáról lesz szó. Terjedése igen gyors, és mivel beleír a FAT táblába, teljes adatvesztést okozhat. További kísérőjelenség még, hogy a képernyőkarakterek időnként „lezuhannak" az alsó sorba. Ez azonban csak XT gépen fordul elő. E rövid ismertetővel segítséget szeretnék nyújtani a számítógépeseknek, hogy mi a teendő fertőzésgyanús esetben.

A vírus jelenléte felismerhető a PC-Tools 4.xx-es verziójával. A program F(ind) funkcióját kell meghívni, és a következő hexa-sorozatot keresni: 01 FA 8B EC E8 00 00 5B 81 EB. Először a winchestert, majd utána minden egyes hajlékonylemezünket végig kell vizsgálni. Ha találtunk ilyen karaktersorozatot, az egyértelműen jelzi, hogy fertőzött a lemezünk. Az érintett program nevét a PC-Tools kiírja. Könnyen észrevehetjük a vírus jelenlétét úgy is, hogy írásvédett lemezt teszünk a meghajtóba, és katalógust kérünk. Ekkor az „Error on drive A, Attempt to write on write protected disk" hibaüzenetet kapjuk.

A vírus a DOS-utasításokkal is terjed, tehát ha egy gépen „csak" a winchester vírusos, hajlékonylemezünkre egy sima **dir a:** parancs is életveszélyes lehet. A rendszerállományok hosszát szintén megnézhetjük: a DOS 3.3-as COMMAND.COM eredeti hossza 25 307 bájt. Indításakor 1701 bájttal lesz hosszabb az eredeti program. A vírus az .EXE és a .COM állományokat támadhatja meg. Egy programhoz többször is hozzámásolódhat.

Ha már a gépünkben van, akkor csak a merevlemez újraformázása segít, abból is a kemény, vagyis fizikai formázás. Erre azért van szükség, mert van a vírusnak olyan formája, amely több DOS-formázást is elvisel a winchesteren. Megfelelő erre a célra például a Disk Manager vagy a diagnosztikai lemez. Ezt vírusmentes gépen másoljuk hajlékonylemezre, és onnan indítsuk el. A rendszert és a használatban levő programjainkat utána kizárólag biztos forrásból másoljuk vissza.

Ha „tiszták" vagyunk, elég arra vigyázni, hogy a jövőben új programokat csak a fent leírt ellenőrzés után másoljuk be winchesterünkre. A vizsgálat előtt még katalógust sem szabad kérni! További védekezésként, különösen ha többen is dolgoznak egy gépen, hasznos lehet egy rövid programot írni a COMMAND.COM hosszának figyelésére, és ezt az AUTOEXEC.BAT-ba beleírni.

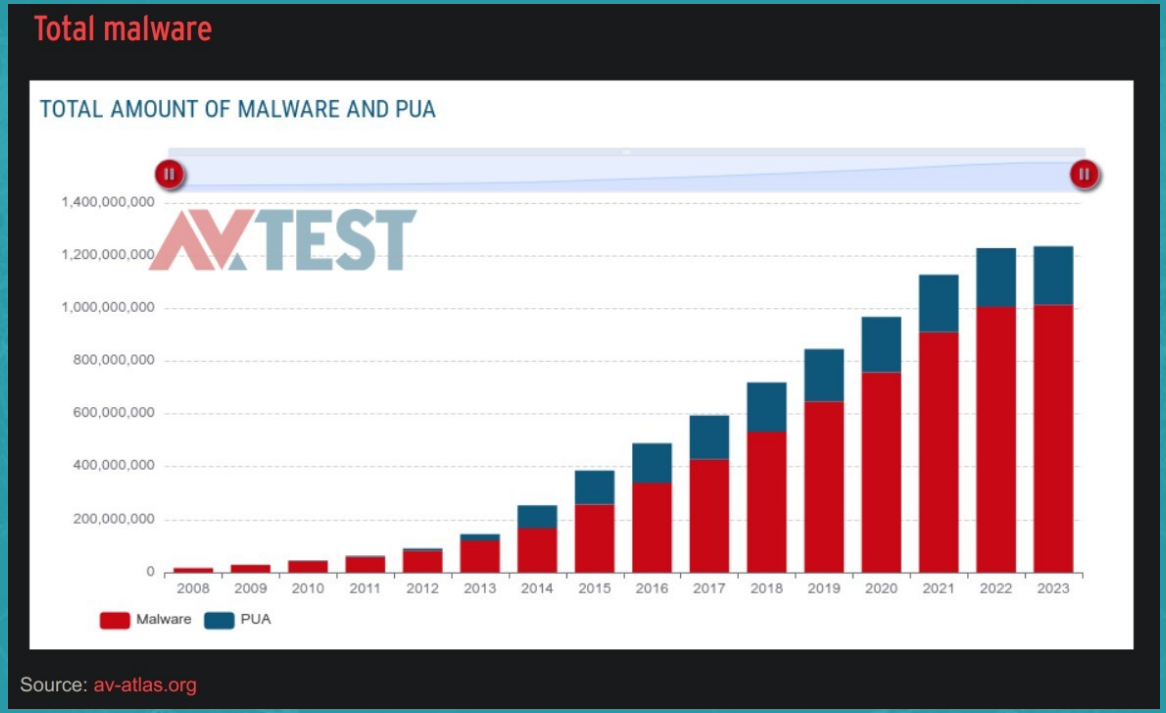
Csizmazia D. István

Egyszer volt, hol nem volt


```
      >>>>> VirusScanList Version: 1.23 - Date : 05-July-95 <<<<<<
       ----> OFFICIAL Virus Help The Netherlands Release <-------
             ~~~~~~~~ ~~~~~ ~~~~ ~~~ ~~~~~~~~~~~ ~~~~~~~
...
 233. GVP-HS15.lha                ?  TR! Destroys many dirs and devices!
      HardDiskSpeeder v1.5  1460  PP Karaçiç Trojan
                            1924  UP
 234. SCANSYS.LHA                 ?  File Deleter!
      scansystem           10720  UP
 235. lha170.lha           33323  FK! 1.70 version
 236. trsi-mem.lha          3178  biomechanic TR!
      Members.exe           8584  Supposed to be a Schnelltro!
 237. LHA 1.62                    ?  FK! 1.62 version
 238. DMSWB208.LHA                ?  Contains DMS 2.06 TR!
      DmsWb 2.08           45732  UP
 239. Bulletin-Trojan      77740  Changes many dirs
 240. scansystem.lha              ?  File Deleter! See '234.' also
 żżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżż
  Signed : Jan Hendrik Lots
```

1995. július
- összesen csak 240 vírus (2014. 200m)
- VIRNET BBS, 300 baud modem
- Nosztalgia: Slovakian Antivirus Center - www.sac.sk

Egyszer volt, hol nem volt



- 1.22mrd egyedi kártékony kód (AV-Test.org)
- 216e biztonsági rés (CVE-Mitre Exploits cve.org)
- 5.18mrd netező (Statista.com), 15.1mrd IoT eszköz (IoT Analytics)
- 12.7mrd feltört, ellopott jelszó (Haveibeenpwnd.com)

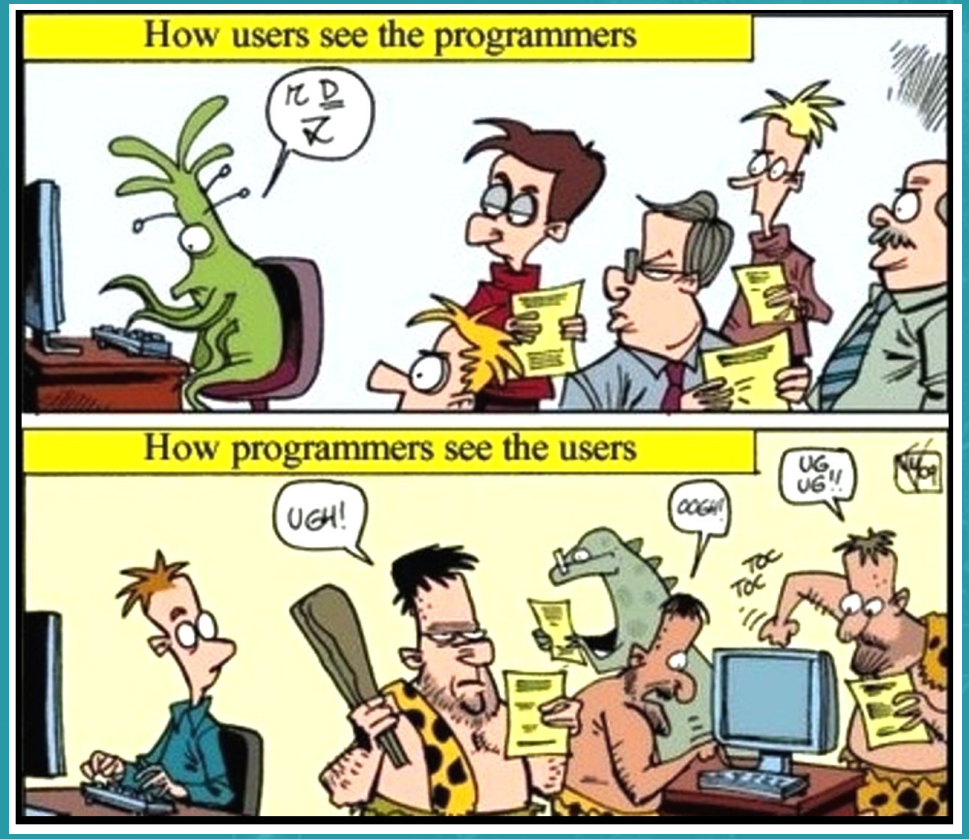
Főbb szerepekben

I. AV ipar és tesztlaborok

II. Felhasználók

III. A sötét oldal

IV. OS és alkalmazás fejlesztők



Kié a legnagyobb hiba?

Azok a fránya alapértelmezett értékek

```
QUICK START INSTRUCTIONS FOR McAFEE ASSOCIATES PROGRAMS
Last revised February 15, 1994.
Copyright 1990-1992 by McAfee Associates.
All rights reserved.

/M - This option tells VIRUSCAN to check system memory for all
known computer viruses that can inhabit memory.  SCAN by default
only checks memory for critical and "stealth" viruses, which are
viruses which can cause catastrophic damage or spread the virus
infection during the scanning process.  By default, SCAN will
check memory for the following viruses:

1024            1253            1530            15xx variant
1963            1971            2153            2560
3040            337             3445-Stealth    4096
```

- 1994.07.15. McAfee VIRUSSCAN.EXE 1.17 verzió
- Váratlanul CSAK a gyakori vírusokat ellenőrzi
- Észre kellett venni, override „/M” paranccsal

Az ég kék, a fű zöld, a plagizáló másol I.

- 2010. január: kb. 50e minta/nap
- A Kaspersky lopott észlelésekre gyanakszik
- 10 tiszta minta VT-be ("Hello World" Linux mingw crosscompiler)
- Megszületett a "Trojan-Spy.Win32.Bzub.hrs", a "Trojan.Win32.KillWin.se", és a "Trojan-Downloader.Win32.Zlob.bmwy" :-)

Az ég kék, a fű zöld, a plagizáló másol II.

virustotal

SHA256: 0de6dfa1cc4a89c591a7d9fcbf241e4a25aadce63b187c37a18cf047c9f89772

Fájl neve: 5295d6d366c35594ab8b1ff5d67d8202

Észlelési 12 / 41

Vírusirtó	Eredmény	Utolsó frissítés
AntiVir	TR/Spy.BZub.hrs	20100129
Antiy-AVL	Trojan/Win32.BZub.gen	20100128
Comodo	TrojWare.Win32.Spy.BZub.hrs	20100130
F-Secure	Suspicious:W32/Riskware!Online	20100129
Fortinet	W32/BZub.HRS!tr	20100130
Ikarus	Trojan-Spy.Win32.BZub	20100130
Kaspersky	Trojan-Spy.Win32.BZub.hrs	20100130
McAfee-GW-Edition	Trojan.Spy.BZub.hrs	20100130
Symantec	Supicious.Insight	20100130
TheHacker	Trojan/Spy.BZub.hrs	20100130
VBA32	Trojan-Spy.Win32.BZub.hrs	20100129
a-squared	Trojan-Spy.Win32.BZub!IK	20100129

- 10 nap múlva már 12-14 AV gyártó is "észleli" ezeket, 9 azonos néven
- Sajtótájékoztató Moszkvában, az AMTSO elhatárolódik, a TheRegister kritizál

Unortodox tesztelési körülmények I.

- 2009.09.08.: NSS Labs Endpoint Security Test rövid jelentés
- A tesztelési körülmények részleteit nem közölték, a gyártókkal sem
- Nincs kapcsolat a gyártókkal, nem tudtak ellenőrizni/javítani
- **A teszt következtetései nem a teszteredményeken alapultak**

Summary

The NSS Labs Endpoint Security test (see above) was challenged by Sophos, AVG and Panda Security. The following conclusions were reached by the Review Analysis Committee, which compared AMTSO's Fundamental Principles of Testing to the above report. Principle 9, which relates to active contact points, was evaluated through interviews with the testing organization and the challenging organizations.

The principles and results are as follows:

✔	1. Testing must not endanger public.
✔	2. Testing must be unbiased.
?	3. Testing should be reasonably open and transparent.
✔	4. The effectiveness and performance of anti-malware products must be measured in a balanced way.
✔	5. Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.
x	6. Testing methodology must be consistent with the testing purpose.
x	7. The conclusions of the test must be based on the test results.
✔	8. Test results should be statistically valid.
✔	9. Vendors, testers and publishers must have an active contact point for testing-related correspondence.

Unortodox tesztelési körülmények II.

- A részletes vizsgálati eredményeket 2000 USD-ért vásárolhatták meg
- **5000 USD-ért bármilyen vizsgálati módszertant lehetett vásárolni :-/**
- 2010. AMTSO (Anti-Malware Testing Standards Organization) kizárás

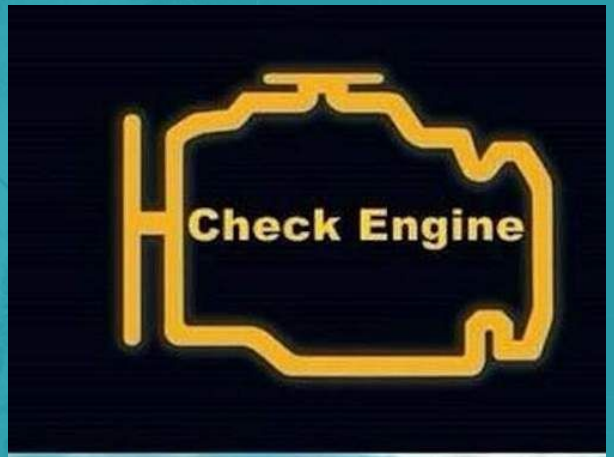
Később viszont sok érdekes és értékes kutatás született náluk

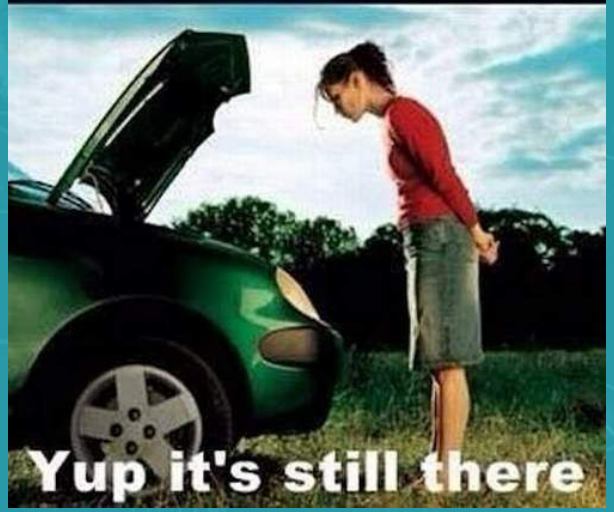
Botrány és kitiltás

2017. USA Kaspersky tiltás a kormányzati gépekről

- 2015-ben orosz hackerek a víruskeresőt használva loptak minősített anyagokat egy NSA alkalmazott otthoni gépéről
- ezt izraeli titkosszolgálati ügynökök fedezték fel, akik maguk is feltörték a Kaspersky hálózatát
- valós időben rögzítették, hogyan kérdeznek le kulcsszavakat a felhasználói gépeken

Frissítések elhanyagolása I.





- 2003.01.25.: SQL Slammer/Zaphire worm

- MS SQL Server 2000 biztonsági rése puffertúlcsordulás

- A patch 2002.07.24-én jelent meg :-)

- "Flashworm", nincs fertőzött fájl, csak a memóriában

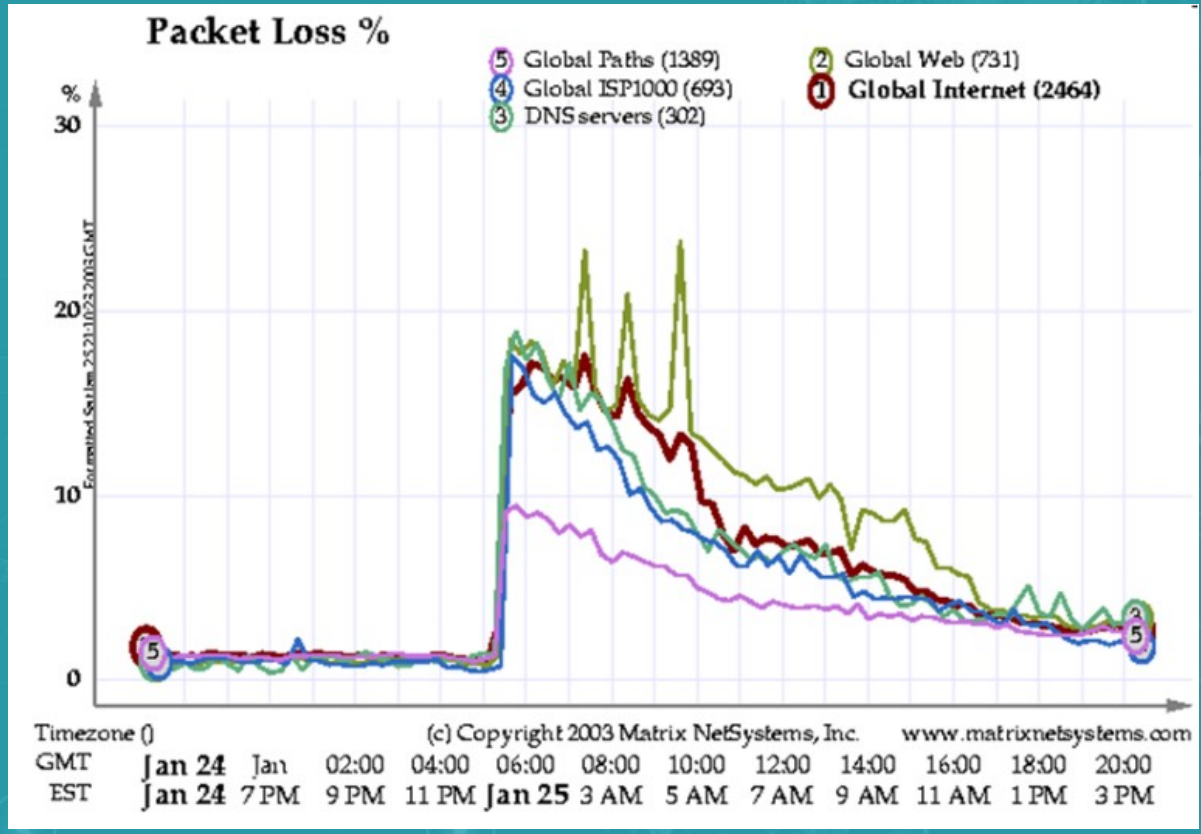
- Az akkori AV-knak esélye sem volt

- **Aha! - A biztonsági frissítések fontossága**

Frissítések elhanyagolása II.

- A számítógépek 90%-a már az első 10 percben megfertőződött

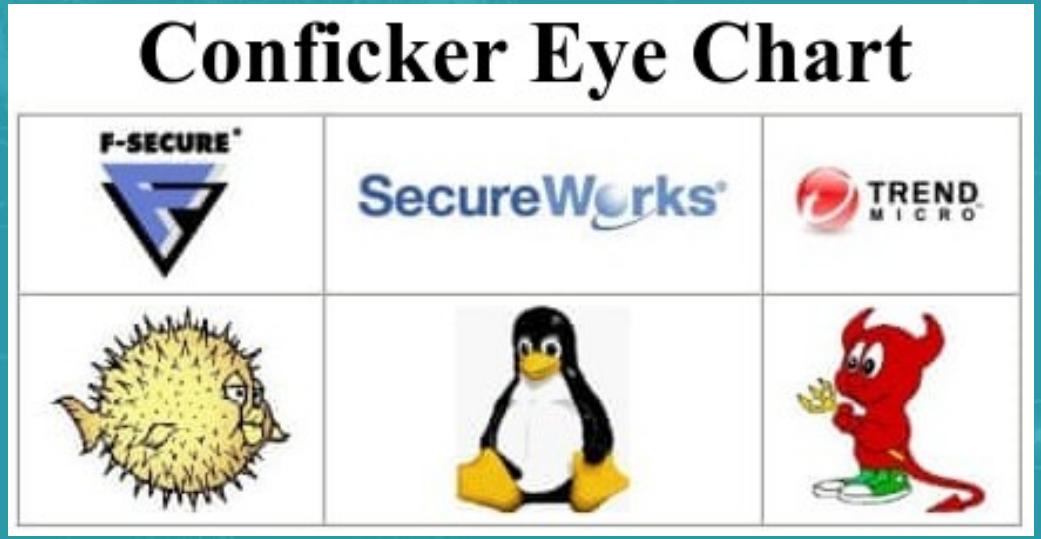
- Összesen 750m USD kárt okozott



Frissítések elhanyagolása III.

2007. Win32/Conficker hálózati féreg (önmagától terjed)

- M$ Win MS08-067 security bulletin
- RPC (Remote Procedure Call) kihasználás
- Kapcsolatok távoli szerverekkel
- Módosítja a helyi HOSTS fájlt - blokkolta az AV weboldalakat
- **2014-ben is még a Virus top10-ben volt**



Frissítések elhanyagolása IV.

Elmaradt szoftverfrissítés is közrejátszhatott egy katonai helikopter balesetében

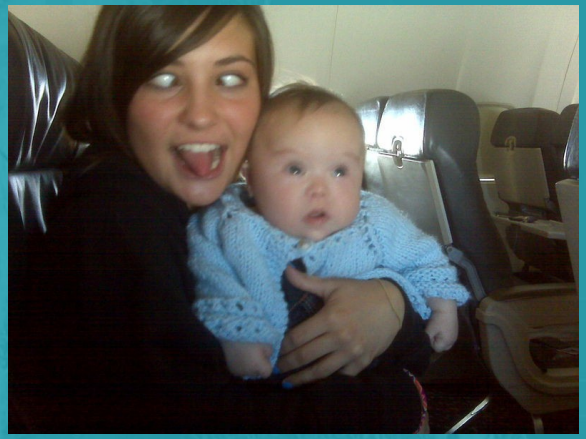
TÖKÖLI GÁBOR | 2023.04.18. | BIZTONSÁG

CIO HUNGARY

Az ausztrál hadsereg gépe a pilóta hibájából pottyanhatott a tengerbe, de elvileg rendelkeznie kellett olyan programmal, ami megakadályozta volna a kockázatos manővert.

Az Australian Broadcasting Corporation (ABC) belső forrásaira hivatkozva számolt be róla, hogy az eredetileg európai tervezésű MRH-90 Taipan helikopterek szoftverfrissítését annak ellenére sem telepítették a teljes ausztrál flottájára, hogy a

PEBKAC



2008. szeptember - Sarah Palin republikánus szenátor Yahoo! fiókját feltörték és közzétették

- Tadaam, új jelszó kérése!
- A "titkos" biztonsági kérdés: Hol találkozott a férjével: a középiskolában
- **Ne védjük titkainkat nyilvános információkkal**

2009.06.01. Twitter-hack

- Obama, FoxNews stb.
- **Jelszó: “Hapiness”**
- **Válasszunk erős jelszót + 2FA**

2021. Solarwinds

- A SolarWinds Orion ITSEC monitoring rendszeren át
- Orosz hackerek hátsó ajtót (backdoor) telepítettek
- Legalább 18,000 érintett szervezet (USA, EU)
- USA minisztériumok, FireEye, M$, Intel, Cisco, Deloitte, Nvidia, stb.
- **A frissítésért felelős szolgáltatásuk hitelesítése: solarwinds123 jelszóval**

The Hacker News

SolarWinds Blames Intern for 'solarwinds123' Password Lapse

Mar 01, 2021 Ravie Lakshmanan

As cybersecurity researchers continue to piece together the sprawling SolarWinds supply chain attack, top executives of the Texas-based software services firm blamed an intern for a critical password lapse that went unnoticed for several years.

The said password "solarwinds123" was originally believed to have been publicly accessible via a GitHub repository since June 17, 2018, before the misconfiguration was addressed on November 22, 2019.

ChatGPT

2023.03. ChatGPT "karbantartás"
- A hiba miatt elérhetők más felhasználók beszélgetései

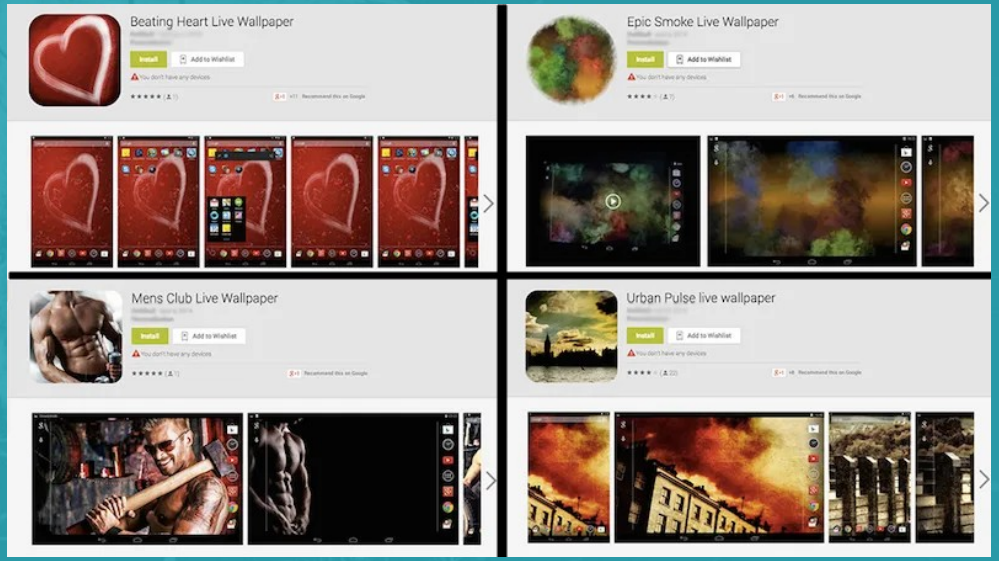
2023.04. Samsung
- bizalmas anyagokat teszteltek, készítettek, javítgattak
- új hardverhez kapcsolódó belsős értekezleti anyagok és forráskód is kiszivárgott
- egy hónap alatt 3 különböző eset

Kapitális hiba a GPCode-ban

- 2008. GPCode régi fájltitkosító váltságdíj-kártevő
- erős, 1024 bites RSA titkosítás
- az első PoC verzióban sima törlés a kódolás után :)
- nem felülírás, nem wipe
- **publikálás -> pár hét múlva javították a hibát :(**

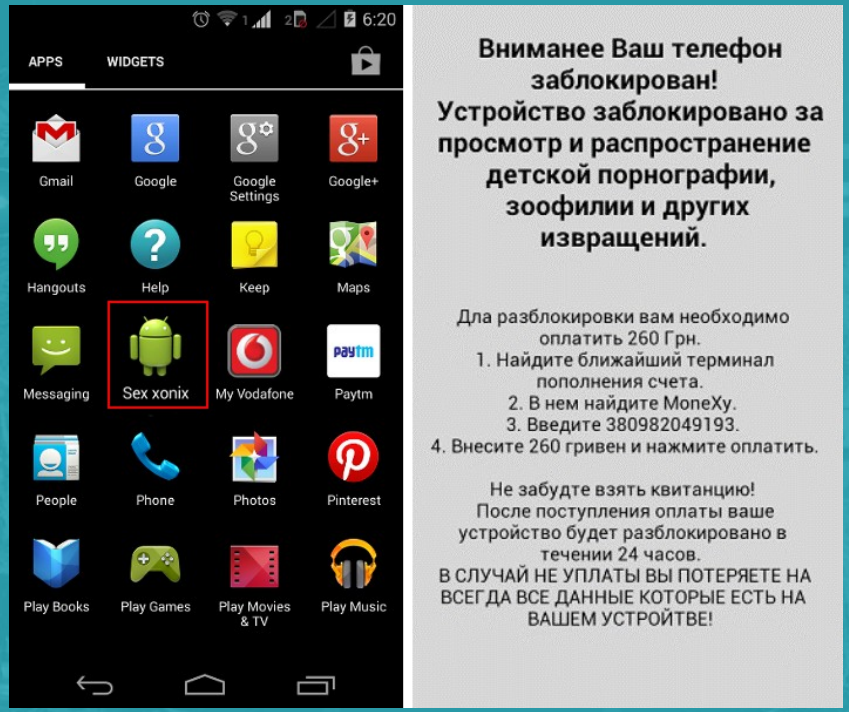
Akiknek látszólag nem fejlődött ki a barázdált agykérgük

- 2014. április: Bitcoin bányász trójai a Google Playen
- PC-n jó ötlet, ott jelentős bevételt termel



- Akku problémák: csak töltőre csatlakoztatva
- /5 sec akku töltöttségi szint ellenőrzés
- Akku 50% + töltő + aktív képernyő kikapcsolva
- Gyors felmelegedés, gyors merülés - könnyen észlelhető
- **Rossz és LASSÚ ötlet volt :-)**

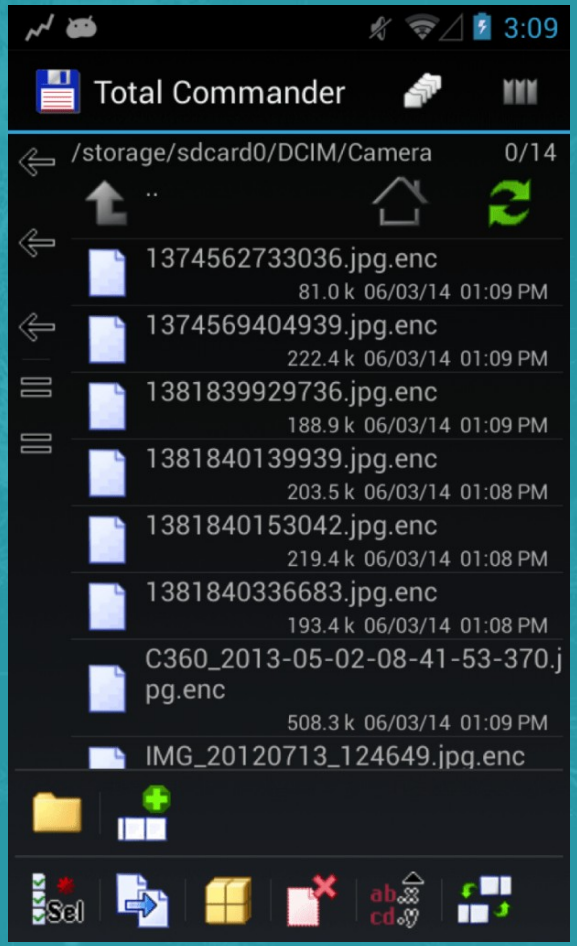
Kapitális hiba a SimpLockerben I.



2014. június: Simplocker - az első váltságdíjas kártevő Androidon

- Beolvassa az SD-kártyát, AES titkosítja az adatokat, váltságdíj
- jpeg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp és mp4 fájlt
- Hrivnyában (ukrán) követelt váltságdíjat oroszul

Kapitális hiba a SimpLockerben II.



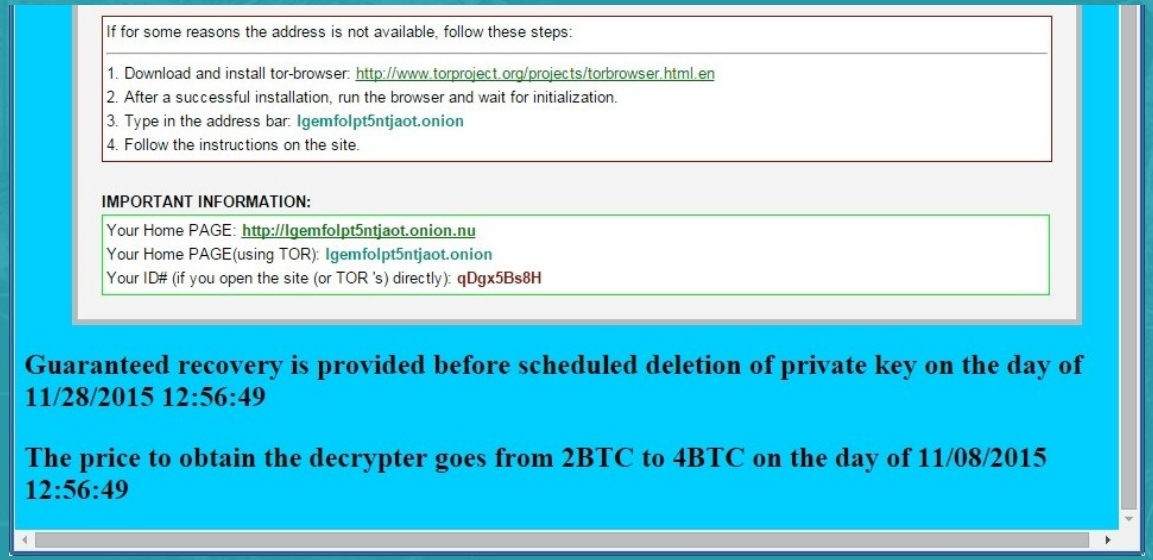
- A dekódoló jelszavak fix konstansként tárolva :-)

- AV-gyártók free dekódoló szkriptek

- **2014. július SimpLocker 2.0:**
  ZIP, 7z és RAR – de a konstans maradt :-O

Helyreállítani nem tudó hibás ransomware I.

2015. Power Worm: Windows alá készült, 2 BTC
- az eredetileg csak Word és Excel állományok helyett a hibás titkosító algoritmus miatt más fájlkiterjesztéseket is elkódolt
- programozási hiba miatt a fizetőknek sem lehetett helyreállítani

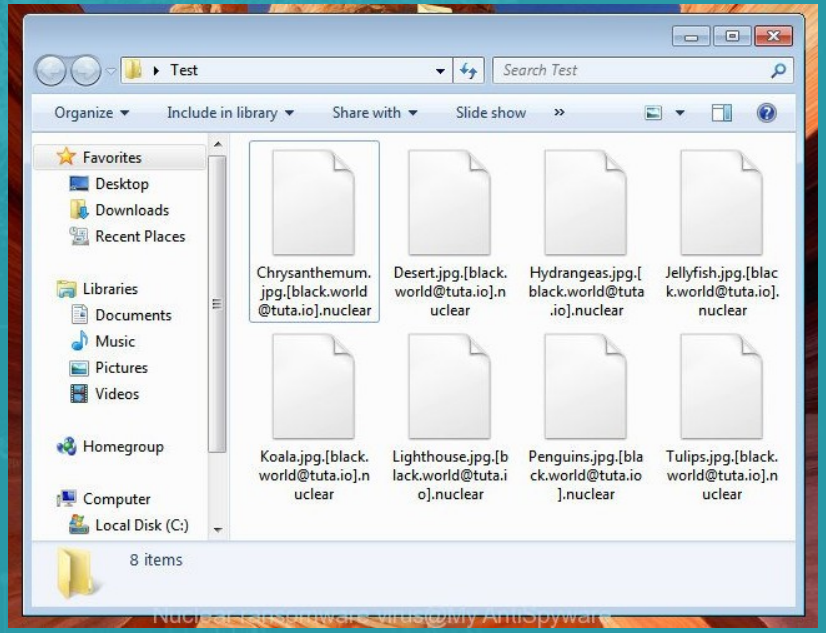


2016. GitHubról származó RANSOM_CRYPTEAR.B egyik átirata
- az úgynevezett "Hidden Tear"

Helyreállítani nem tudó hibás ransomware II.

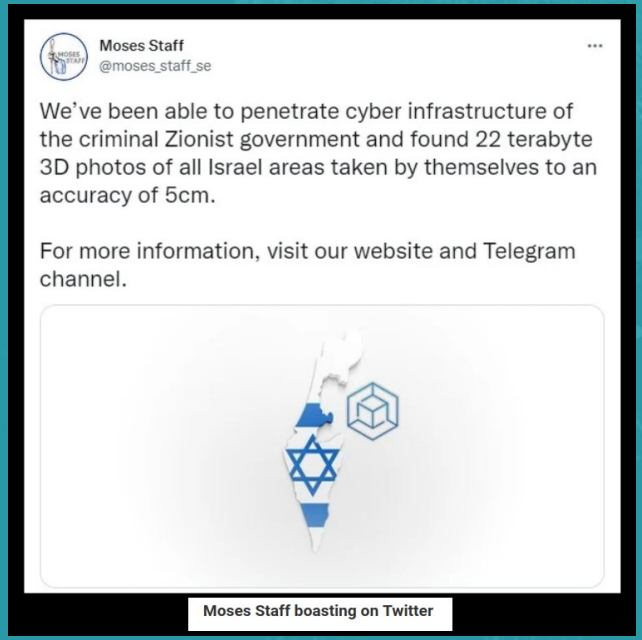
2017. BTCware/Nuclear

- programozási hiba miatt a 10 MB feletti állományoknál nem működött a helyreállító kulcs



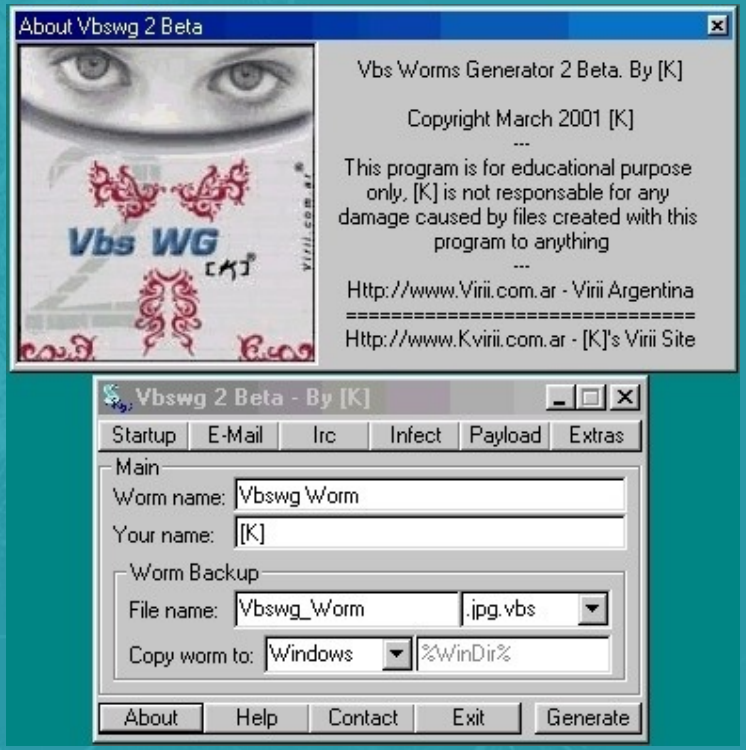
2021. Moses Staff

- nem hiba, hanem feature
- egy iráni szervezet
- szándékos rongálás: szabotázs
- politikai motiváció



Moses Staff boasting on Twitter

1995. M$ - Macro vírusok I.



- 1995, első makróvírusok az Office 95-ön
- Kis munkával könnyen sok új változat
- **Vissza kellett fejteni a fájlformátumokat**
- Wormgenerator-ok tömeges megjelenése
- **Alapértelmezetten az automatikus makrók 2000-ig futottak**
- **6 évig nyitva volt**
- Maradt a „Shift” lenyomás módszer

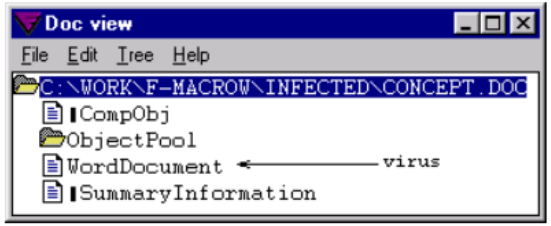
1997. M$ - Macro vírusok II.

- Eleinte csak pár tucat észlelés az Office 97 makróvédelemben
- A kezdeti makrók Word Basicben
- Később áttérés a Visual Basic for Applications formára
- **Megnyitáskor AUTOMATIKUS konvert WB makró → VBA makró**
- Előtte mindenből csak egy verzió volt: például Wazzu.A

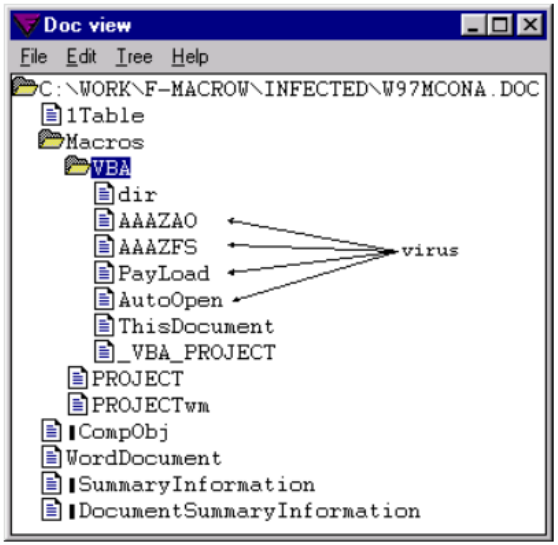
- **Már a különböző területi nyelvek miatt is rengeteg új alverzió lett**
- **Meredeken nőtt a makrovírusok száma :-O**

2014. M$ - Macro vírusok III.

WM/Concept.A:



W97M/Concept.A:



EPILÓGUS – 2014. június

- Tömeges spamek kártékony makrókkal

- számla, csomagszállítás, bírósági idézés, stb.

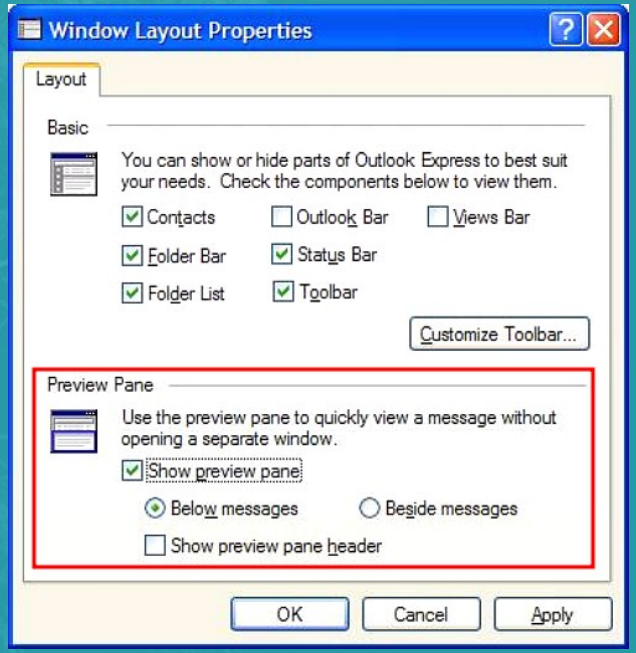
- „Kérem, kapcsolja be a makrók futtatását” :)

- A VBS férgek aránya 6%-ról 28%-ra nőtt (Sophos Lab)

1999. - Gyors előnézet

MS Outlook Express quick preview

- 1999. A KAK worm
- Outlook Express automatikus e-mail betekintő előnézet
- **Javascript futtatás a levél megnyitása nélkül**
- **2004. 6 év után XP SP2**



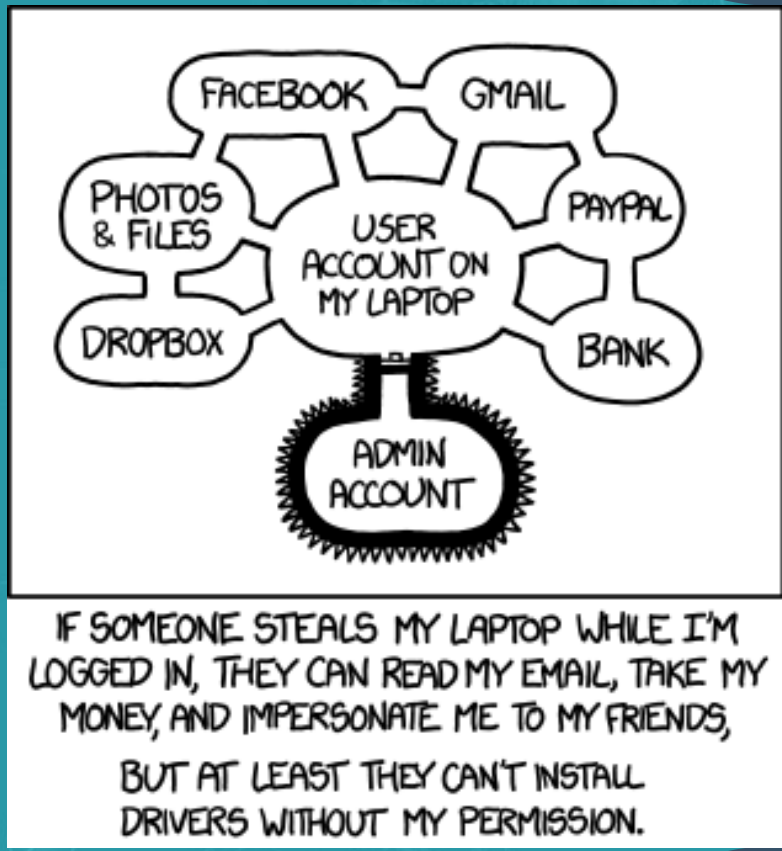
2001. M$ - Rendszergazdai jogok

- XP (2001) alapértelmezett admin jogok

- Vista (2007) UAC

- 6 évig nyitva

- DropMyRights segédprogram



2001. M$ - Ismert fájl típusok megjelenítése I.

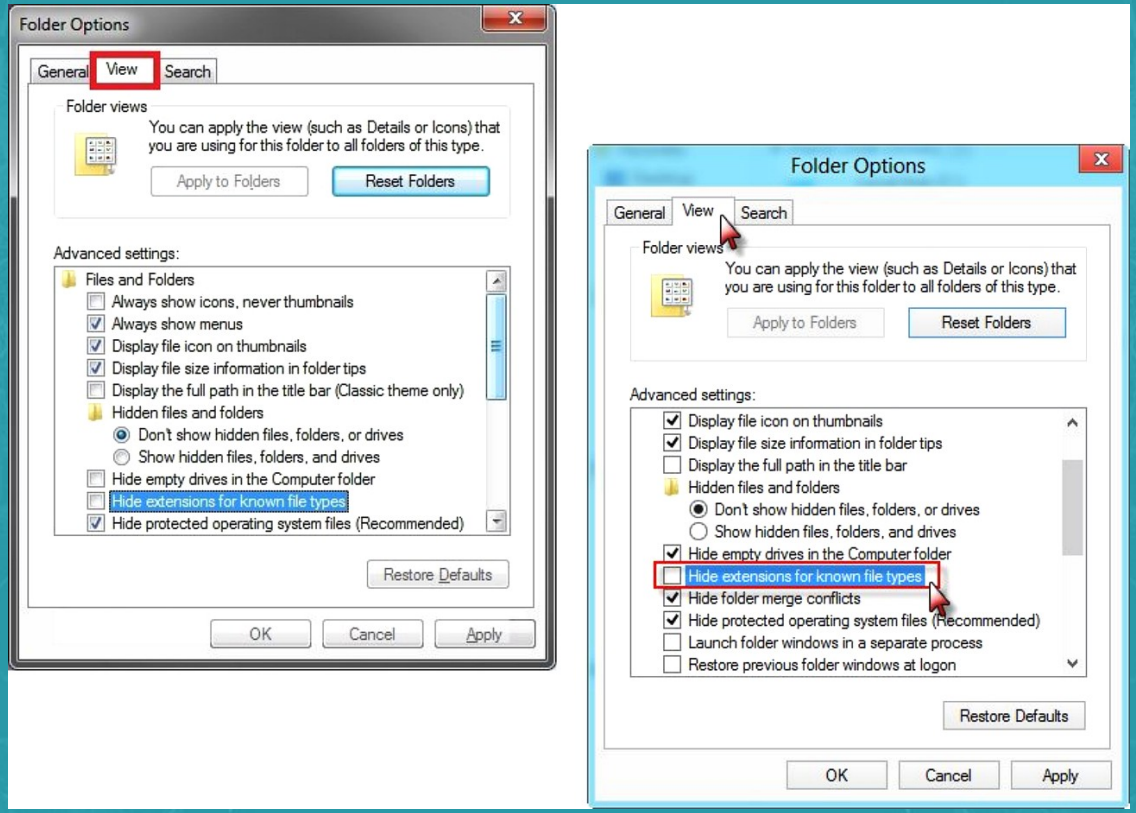
- Windows XP óta alapértelmezett a rejtett opció

- Rossz ötlet - pl. worm programok

- 2000: "Love-letter-for-you.TXT.VBS"

- 2001: "AnnaKournikova.jpg.vbs"

2001. M$ - Ismert fájl típusok megjelenítése II.



- Máig - 22 éve! - a Win11-ben is rejtett
- OSX alatt is ajánlott visszaállítani

2007. M$ - Autorun

- 2007. június: Első Autorun vírusészlelés (rejtett autorun.inf)

- Az automatikus futtatás tiltása kellett volna (WGA, Windows Genuine Advantage)

- 2011. február. javítás

- 5 évig sebezhető volt

- "Sérülne a felhasználói élmény..."

- Sok felhasználó nem frissítette,
  pl. illegális Win-másolatok, lustaság stb.

2007. M$ - Java

InfoWorld

CHANNELS App Dev Applications Big Data Cloud Computing Consumerization

News Blogs Test Center Technologies Tech Watch White Papers We

JANUARY 22, 2013

Disabling Java in Internet Explorer: No easy task

Firefox, Chome, and Safari let you. But short of a complex, CERT-documented process, there's no reliable way to disable Java in IE

By Woody Leonhard | InfoWorld

Follow @woodyleonhard

Print More +1 Like

No doubt you've heard the news: Oracle released Java 7, Update 11 on Jan. 13. By the next day, exploits started appearing that took advantage of the Update 11 code. Last Friday, Adam Gowdiak, CEO of Security Explorations, reported yet another series of problems with the latest version of Java:

- 2013. Kritikus exploitok miatt le kell tiltani a Java beépülő modult

- A letiltás Firefox, Opera, Safari és Chrome böngészőben működik :)

- **Internet Explorerben nem :(**

- **Speciális registry megoldás (CERT)**

- JAVA: bankolás, Adobe Creative Suite, CrashPlan PRO mentés, LibreOffice, APEH, stb.

2005. SONY rootkit

- Rootkit másolásvédelem (XCP) a Van Zant zenei CD lemez

- Véletlenül derült ki (Mark Russinovich, Winternals)

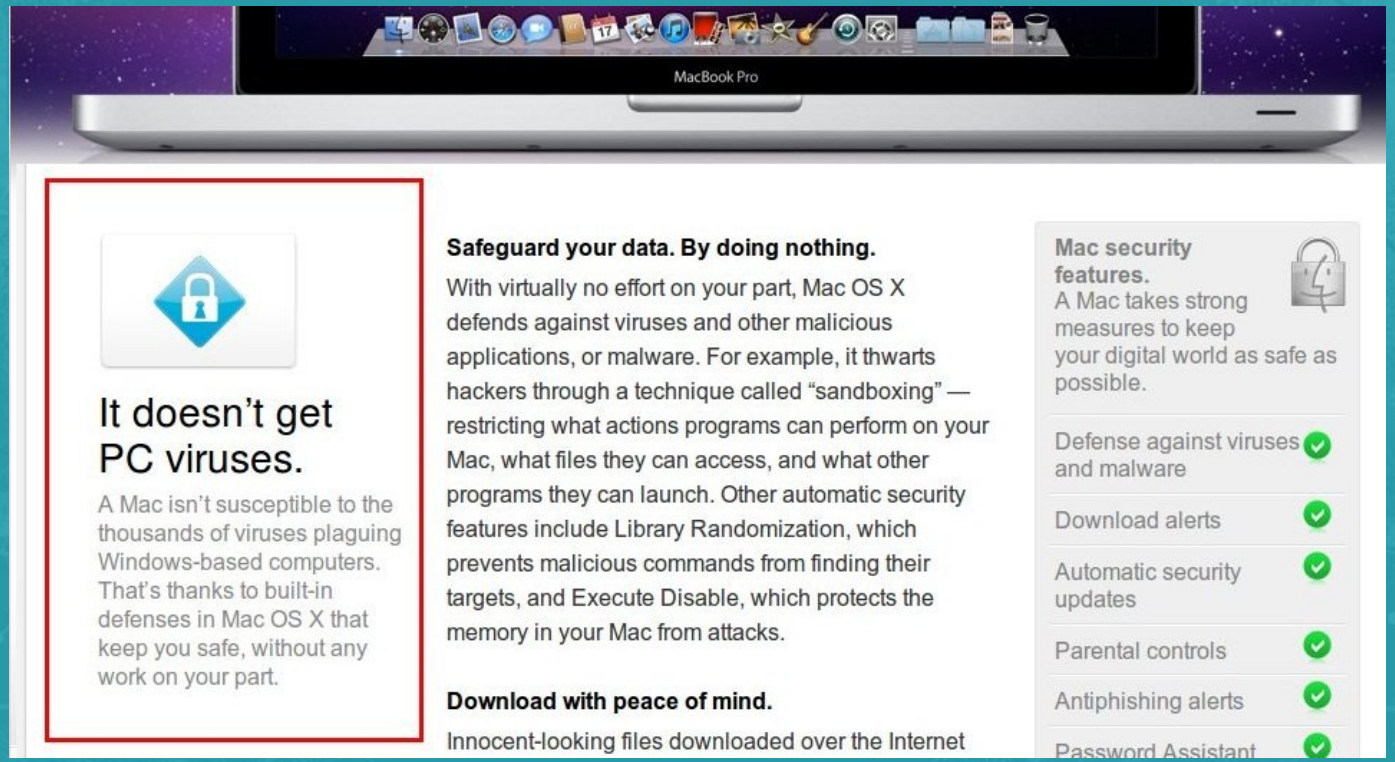
- Ismeretlen hálózati forgalmat generált Sony szerverekre

- Ki, mikor és milyen IP-címen játszotta le az albumot (Napster .mp3 per 2001.)

- **Tagadták, visszavonták**

- **Kártevők a rejtett mappában**

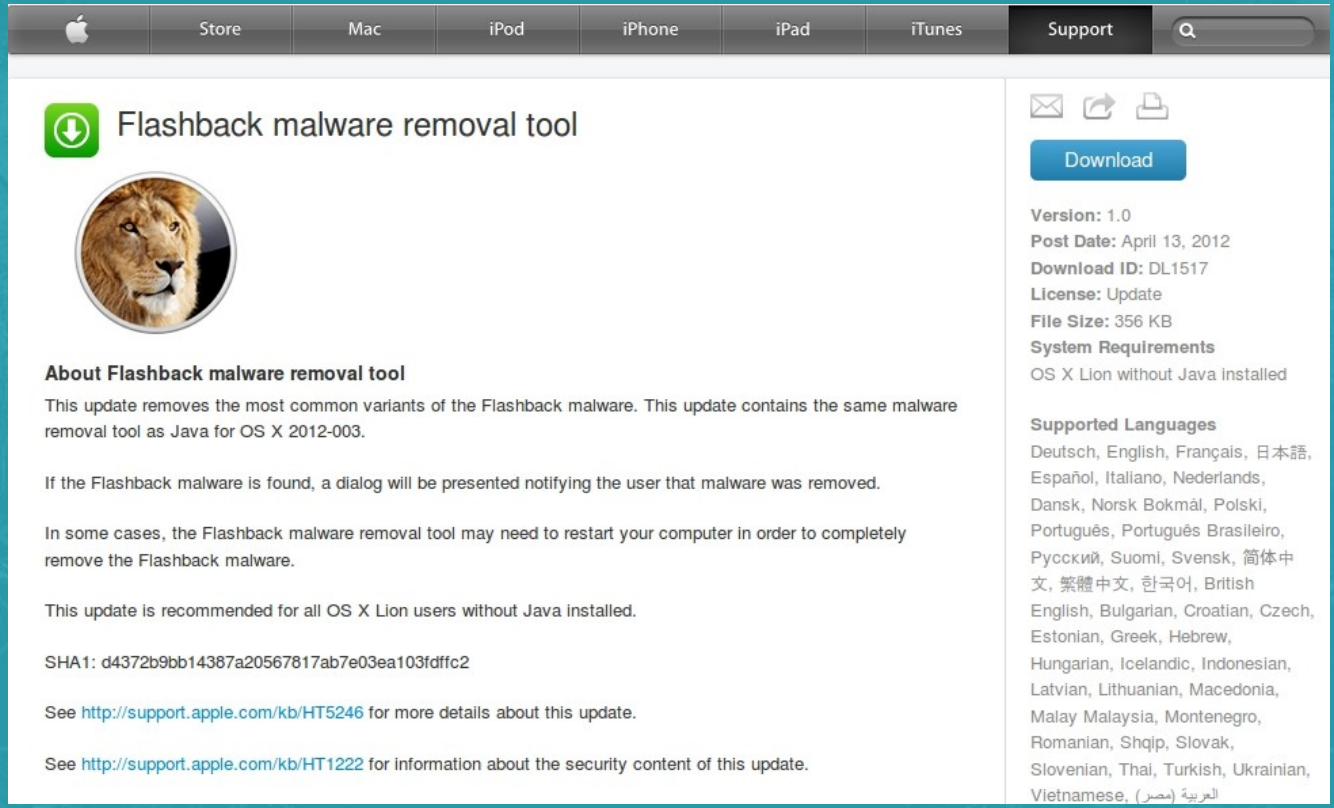
OSX operációs rendszer I.



Why you'll love a Mac: www.apple.com

-2011. "It doesn't get PC viruses" (Wayback Machine)

OSX operációs rendszer II.



2012.03. Flashback botnet OS X 600e zombi Mac (Java) rendszeren
2012.04. Flashback eltávolító eszköz – Apple biztonsági frissítés

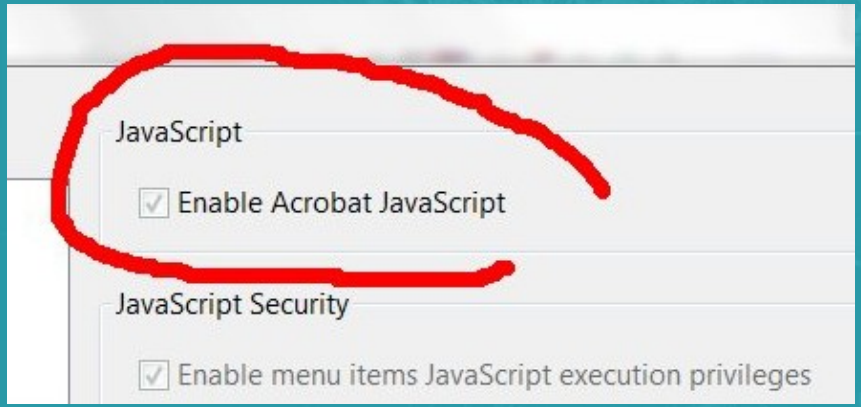
OSX operációs rendszer III.

Why you'll love a Mac: www.apple.com

2012. után - "It's built to be safe"

2008. Adobe Reader JavaScript

- 2008. Első kártékony JavaScript PDF-fájlban
- Állítólag hasznos interaktív PDF-formokban
- **Adobe Reader Win10**
- **2023. Alapértelmezetten azóta is ON**
- **Ez is 15 éve van már így**
- **Protected View kiválasztása, és ne legyen default a JavaScriptek futtatása**



Mégis miről szól mindez?

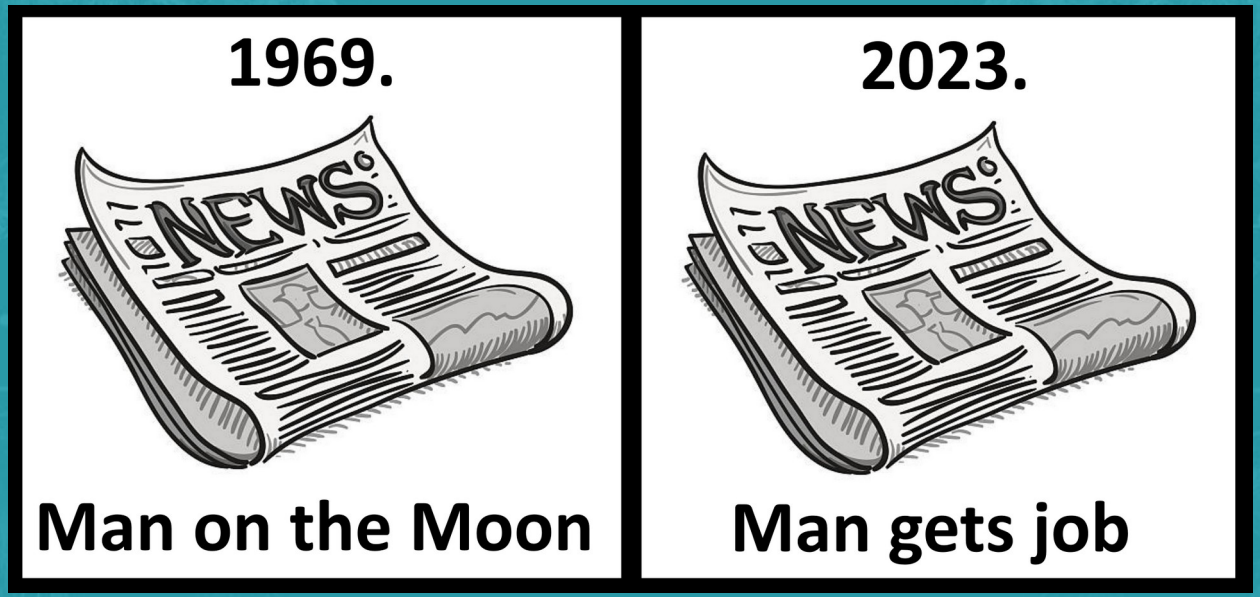
- A hozzáállásról, enélkül nincs jelentős javulás

- Az AV ipar proaktív
- A felhasználók tudatosodnak?
- A fejlesztők foltoznak, OWASP
- A sötét oldal 24/7

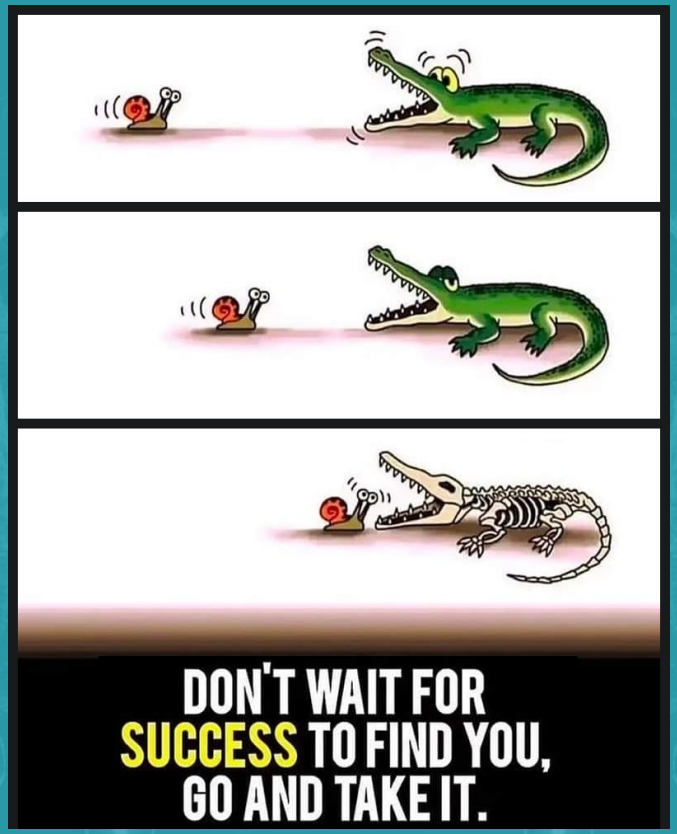
Bug bounty programok

Pwn2Own verseny Toronto 2023.

- A magas zeroday jutalom
- Pl. mobiltelefon kategória
- iPhone 14 feltörés 300e USD
- Pixel 7 feltörés 250e USD



Köszönöm a figyelmet!



info@sicontact.hu