

SICONTACT



biztonság a digitális világban



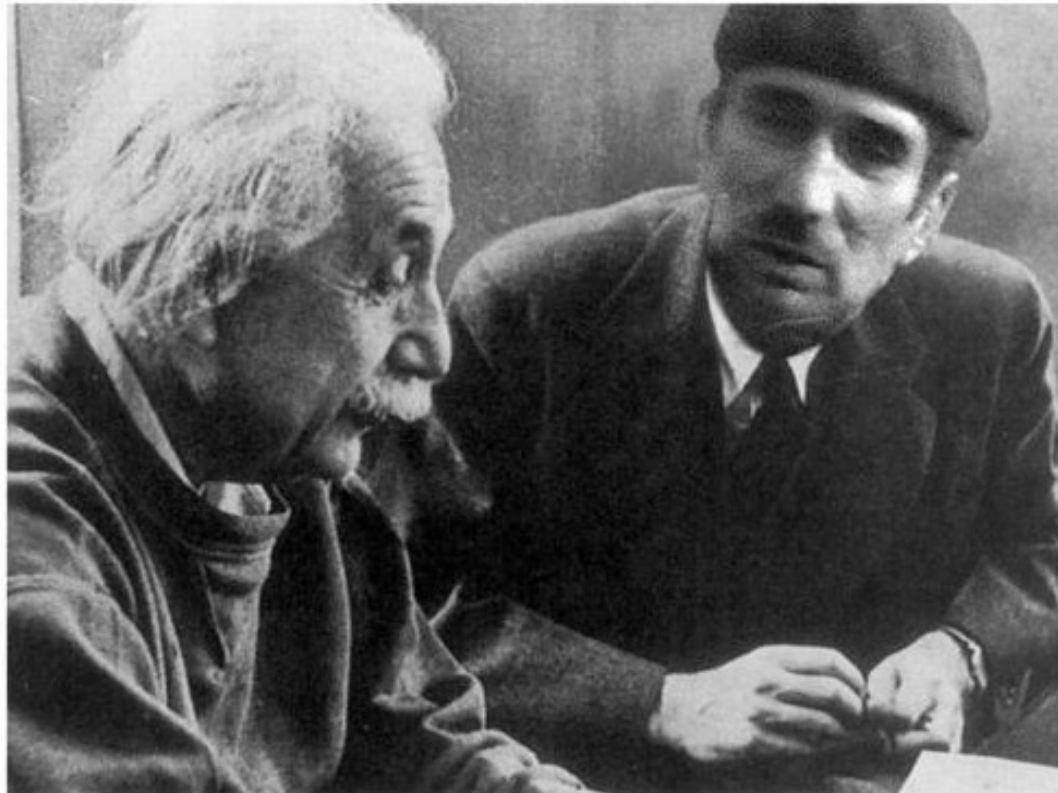
CIO HUNGARY 2019. MÁJUS 9-10.

DÖNTÉSEK ÉS KÖVETKEZMÉNYEK
A VÁLLALATI BIZTONSÁGBAN



Döntések és következmények a vállalati biztonságban

¯_ (ツ) _ /



- A vízből veszi ki a zoxigént, tetszik érteni?



Csizmazia-Darab István
Sicontact, IT biztonsági szakértő

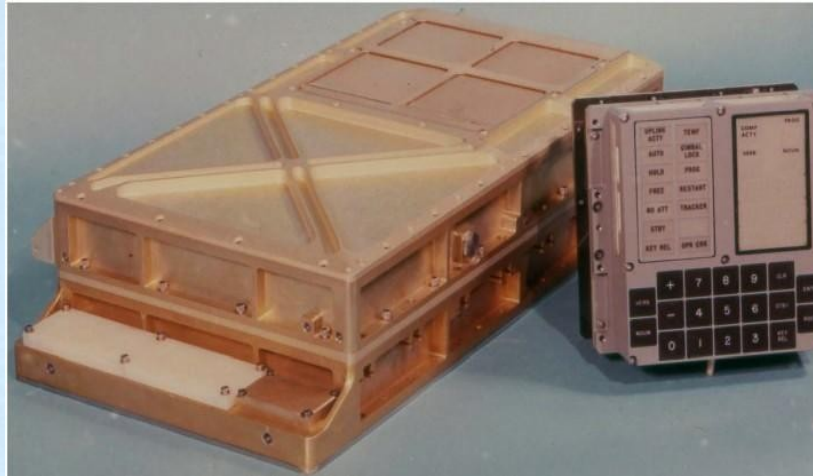






1969. Apolló 11. DSKY

- 2kB RAM
- 36 kB ROM
- 1 MHz 16 bit CPU



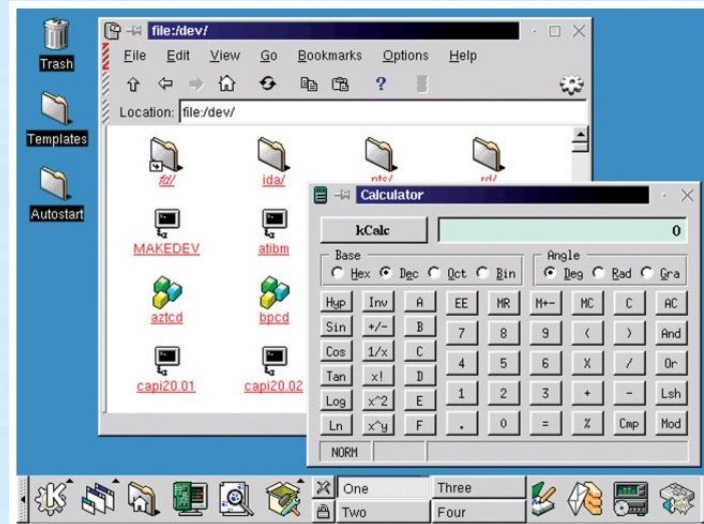
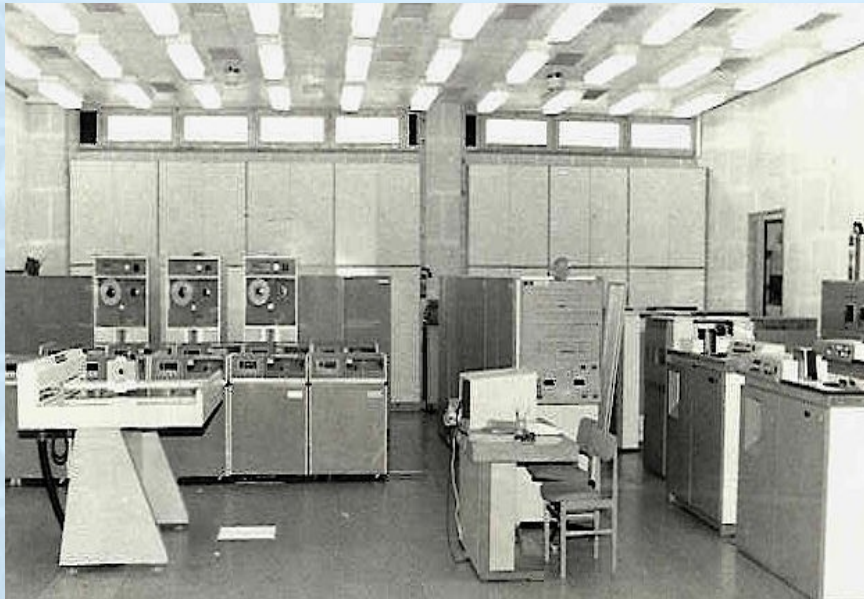
1300x gyengébb, mint iPhone 5C

2013. iPhone 5C

- 1 GB LPDDR2-1066 RAM
- 32 GB storage
- 1.3 GHz dual core
- 32-bit ARMv7-A



- 1970. R-20, R-40, ESZR, 8bit, Fortran, COBOL, PL/1
- 1981. IBM-PC XT, MS-DOS, Proper-DOS, DR-DOS,...
- 1991. Linux



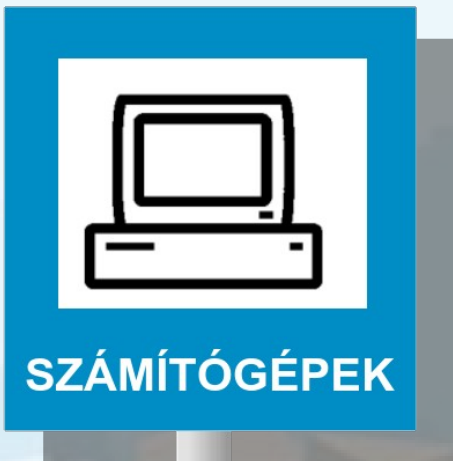


1997. Deep Blue Vs Kasparov - 4:2
259-ik, 11.38 GigaFlops



2016. AlphaGo Vs Lee Sedol - 4:1
Google DeepMind Challenge

- 2018. Summit IBM Power, 122 PetaFlops
- 2018. 7.6 mrd netező, 23.14. mrd netes eszköz (Internet World Stats, Statista)



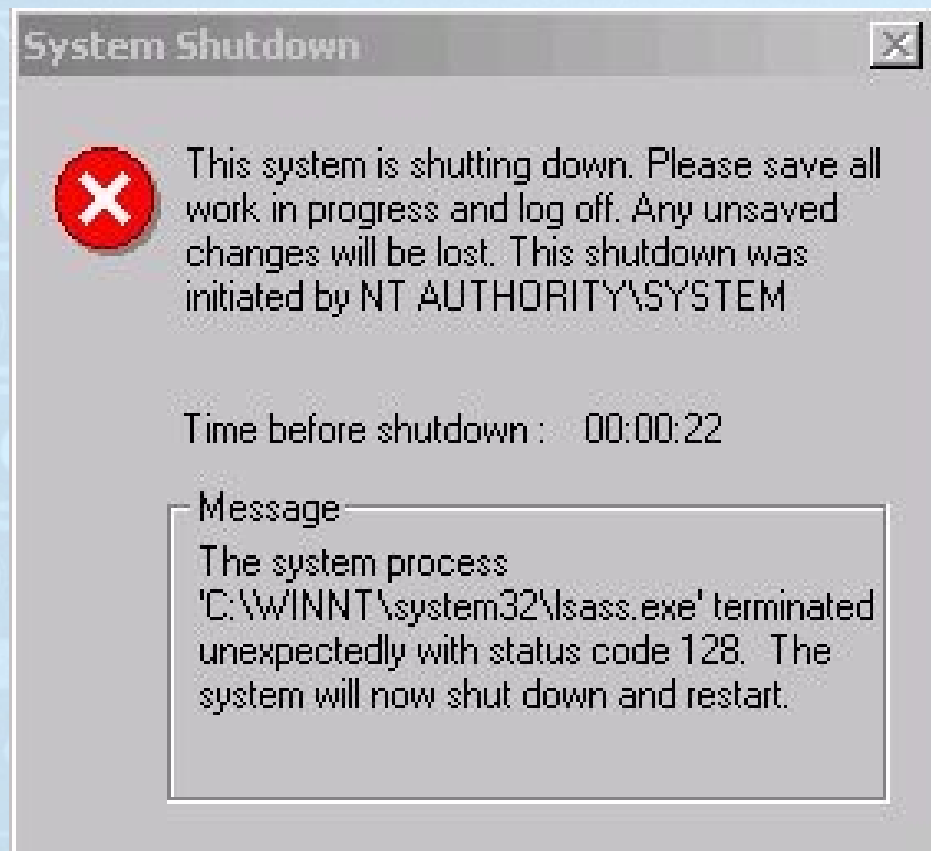


-
- A photograph of two men in dark suits and white shirts sitting at a glass table. The man on the left is smiling and gesturing with his right hand. The man on the right is also smiling and has his hands clasped. In the background, there is a white shelving unit on the left and a poster on the wall that says "Brain" and shows a red truck.

A black floppy disk is shown at an angle. A small, rectangular piece of lined paper with a yellow border is taped to the top right of the disk. On this paper, the word "BRAIN" is written in large, bold, black capital letters. Below the word, there is a small, simple drawing of a brain in green ink. The paper also has some faint, illegible handwriting and a small number "92" visible. The floppy disk itself has a large circular hole in the center and a smaller one to the right. It is resting on a red surface, which is partially visible at the bottom left.

2003. SQL Slammer flashworm

- Nincs fájl, a memóriába tölt
- Hálózati csomagban terjedt
- Az első félórában 75 ezer gép
- 750m USD összkár
- MS 2002-es javítócsomag





It doesn't get PC viruses.

A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe, without any work on your part.

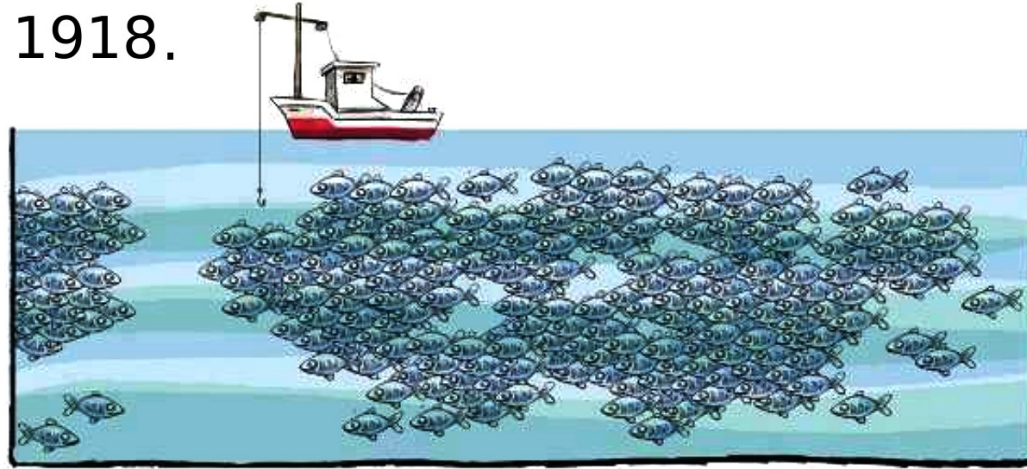


It's built to be safe.

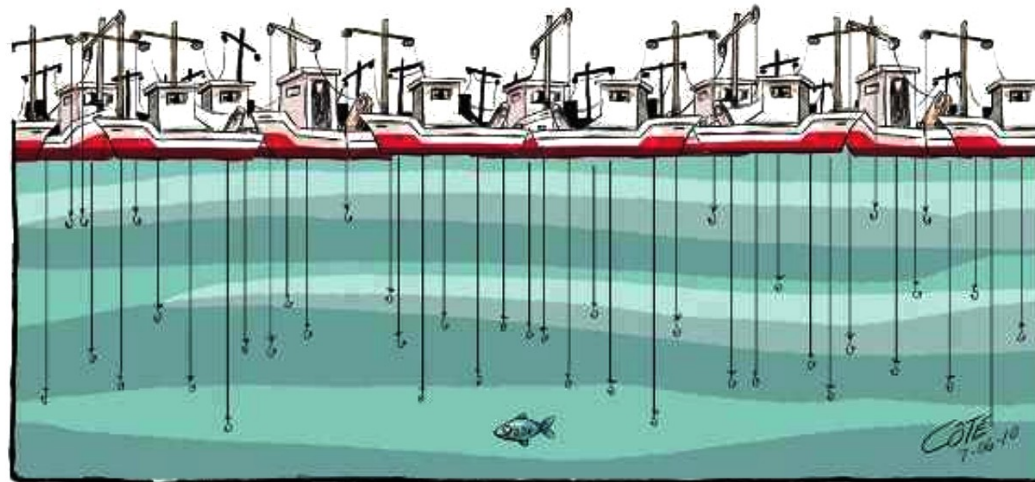
Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac.

- 2009. Power PC to Intel CPU
- 2012. március 600e Flashback botnet
- Java sebezhetőség, egyes változatok közbeavatkozás nélkül is terjedtek

1918.



2018.





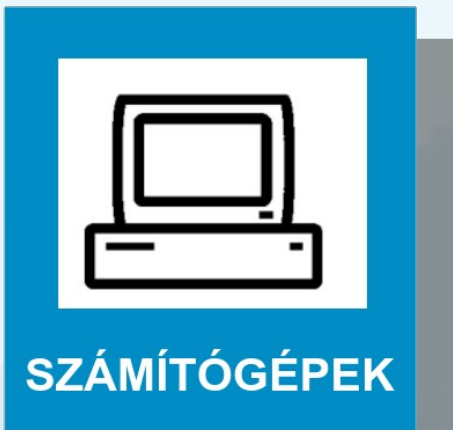
Total malware

AVTEST

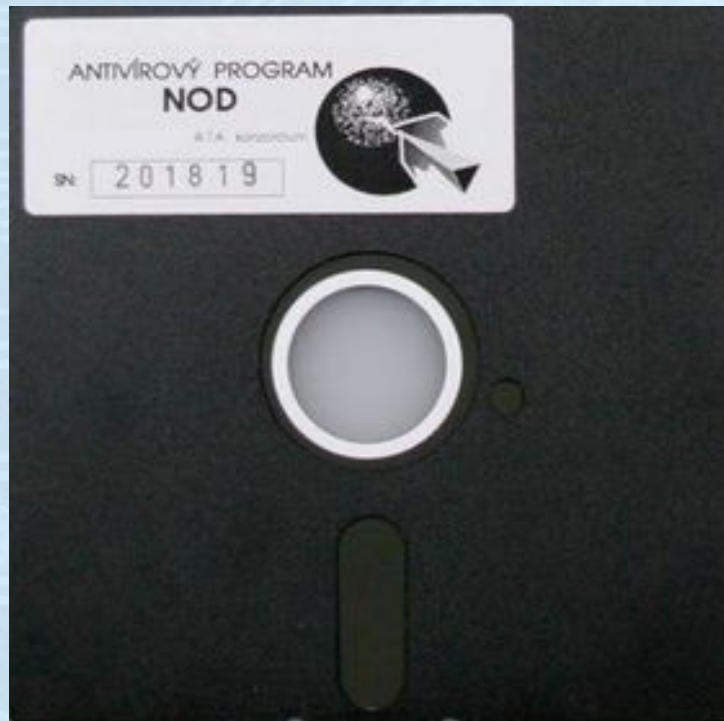


Last update: April 14, 2019

Copyright © AV-TEST GmbH, www.av-test.org

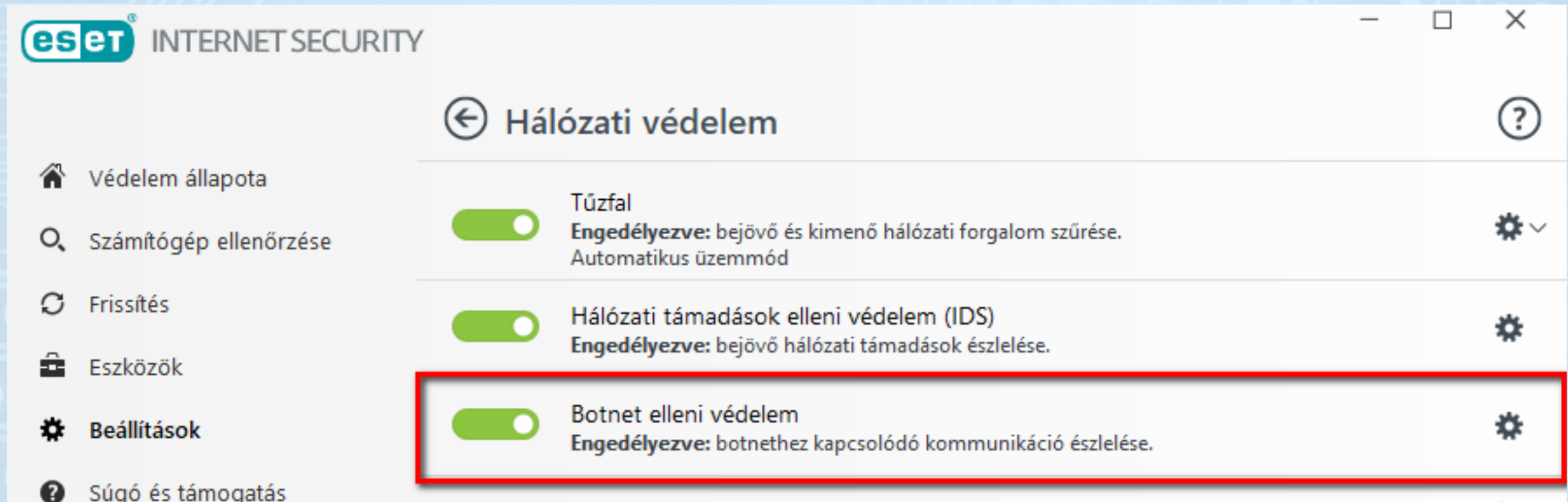




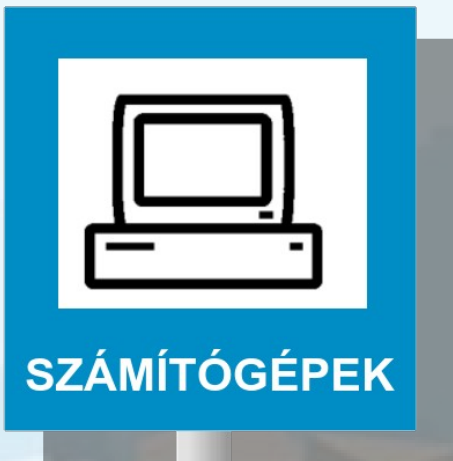


Targets	Log	Setup
Diagnostics Targets: ☒ Files ☒ Boot sectors ☒ Memory	On virus detection: ☐ Clean ☒ Offer an action ☐ Leave unchanged ☐ Rename ☐ Delete ☐ Replace	On virus detection: ☒ Offer an action ☐ Leave unchanged ☐ Rename ☐ Delete ☐ Replace
Diagnostics methods: ☒ Signatures ☒ Heuristics ☐ Runtime packers ☐ Archives	Log: ☐ Enabled ☐ Wrap log ☒ Append ☐ Overwrite	System: ☐ List all files ☒ Sound signal
Heuristic sensitivity: ☐ Safe ☒ Standard ☐ Deep	Max. length [kB]: 100 Name: nod32.log	Save Load Extensions Defaults

1987. NOD32 1.0
1990. Virnet BBS (FidoNET)



Proaktív és többretegű védelmi technológiák: URL detection, advanced memory scanner, virtuális kódemuláció, spamszűrés, tűzfal, viselkedés alapú vizsgálat, botnet, hálózat, ransomware, felhő alapú reputáció, UEFI, stb.







- 2011. Diginotar
- 2012. LinkedIn: 6.5m ügyféladat
- 2013. Adobe: 150m ügyféladat, 3.2m bankkártya adat, forráskódok
- 2013. Target: 110m ügyféladat, 40m bankkártya, 290 mUSD kár
- 2014. Sony: 20 támadás, 24 mrd USD veszteség
- 2018. Tesla: Amazon cloud, Bitcoin bányászat

1.



2.



3.



4.



5.



6.





2019. április. 04. 09:33 · Utolsó frissítés: 2019. április. 04. 09:46 · TECH

540 000 000 Facebook-felhasználó adatát "őrizgették" jelszóval sem védett szervereken

szerző:
hvg.hu



Nem kellett sokat várni, itt az újabb adatgond, amely most is Facebook-felhasználók tömkelegét érinti.

Egyre inkább helytálló az a megállapítás, amely szerint a Facebook elég gyakran vét katasztrofális hibákat, ha a felhasználói adatokról van szó. Egy hónapja sincs, hogy kiderült, az oldal titkosítás nélkül, **egyszerű szöveges formában tárolt több száz milliónyi jelszót**. Aztán alig egy napja arról érkeztek hírek, hogy a hálózat **jelszavakkal együtt kér be e-mail-címeket**.

Titkosítatlanul tárolják az adatokat a Tesla modelljei

2019. április 03. 9:04, szerda



Az autók fedélzeti számítógépeiben nincsenek védve a személyes adatok és más információk sem.

Két hacker több Tesla Model 3, valamint egy-egy Model S és Model X típusú gépkocsit is [megvizsgált](#). A szakértők kiderítették, hogy a fedélzeti számítógépek titkosítatlanul őrzik a beépített merevlemezeken a személyes adatokat (telefonkönyvek, videók, e-mail-címek stb.), valamint az olyan információkat is, amelyek a vezetői szokásokra vonatkoznak. Így aki összetöri a járművét, az számolhat azzal, hogy nem csupán az autója végzi a roncsok között, hanem az adatai is kikerülhetnek.

2019. CrowdStrike Global Threat Report, toplista

1. - 0 óra 18 perc 49 sec - oroszok
2. - 2 óra 28 perc 14 sec - észak-koreaiak
3. - 4 óra 00 perc 26 sec - kínaiak
4. - 5 óra 09 perc 04 sec – irániak



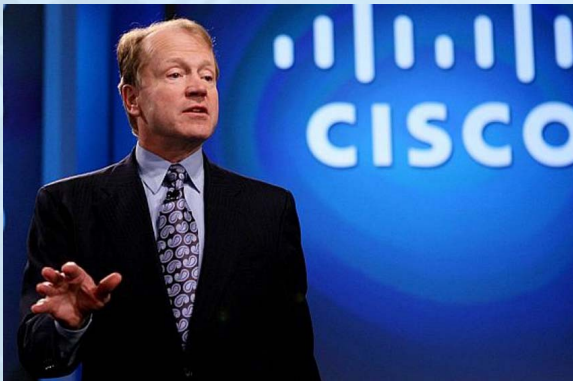
2019. Microfocus jelentés

- 2017-ben 90.1 milliárd kiber incidens naponta
- 2018-ban már 240 milliárd



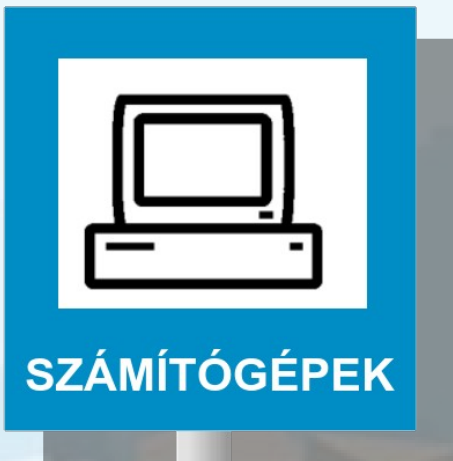
Robert S. Mueller, FBI igazgató:

"Két féle cég van, akiket már feltörték, és akiket még nem."



John Chambers, Cisco vezérigazgató:

"Két féle cég van, akik már észrevették, hogy feltörték őket, és akik még nem vették észre."



- Vállalati IT és üzleti ökoszisztéma
- IT kulcs elem az üzleti folyamatokban
- **Kockázat arányos költség kell**





- Nem érdemes spórolni a biztonságon
- Vírusvédelem + patch management + biztonság tudatosság
- Titkosítás (GDPR), mentés, logelemzés, pentest, security audit, stb.
- A proaktív és többretegű védelmi megoldások, felhővel kiegészített technológiák segítenek



↑ CIO Hungary ↑
Köszönöm a figyelmet!
csizmazia.istvan@sicontact.hu



**Ön a sárgával jelzett gépjárművet
vezeti. Hányadikként haladhat
tovább a kereszteződésben?**