# A mesterséges intelligencia véd, a felhasználó megkerüli

Csizmazia-Darab István | 2022.04.06. | SecWorld

Digital Security
Progress. Protected.


A mesterséges intelligencia véd, a felhasználó megkerüli

Csizmazia-Darab István

IT biztonsági szakértő
ESET/Sicontact

# #Tartalom

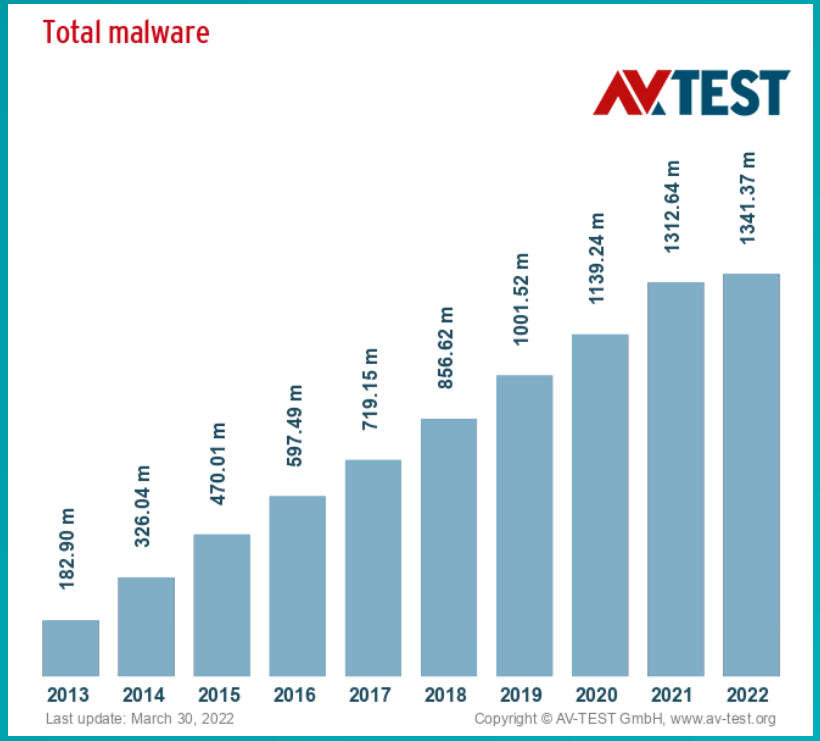
1. *Helyzetkép: támadók, védelem*
2. *A felhasználó közbelép*
3. *Social engineering és belsősök*
4. *Felkészülés, megelőzés*

# #fejlődés

- 4.95mrd internetező (World Internet Users 2022. január)

- 26mrd netes eszköz, ebből 16.4 mrd IoT eszköz (IoT Analytics)

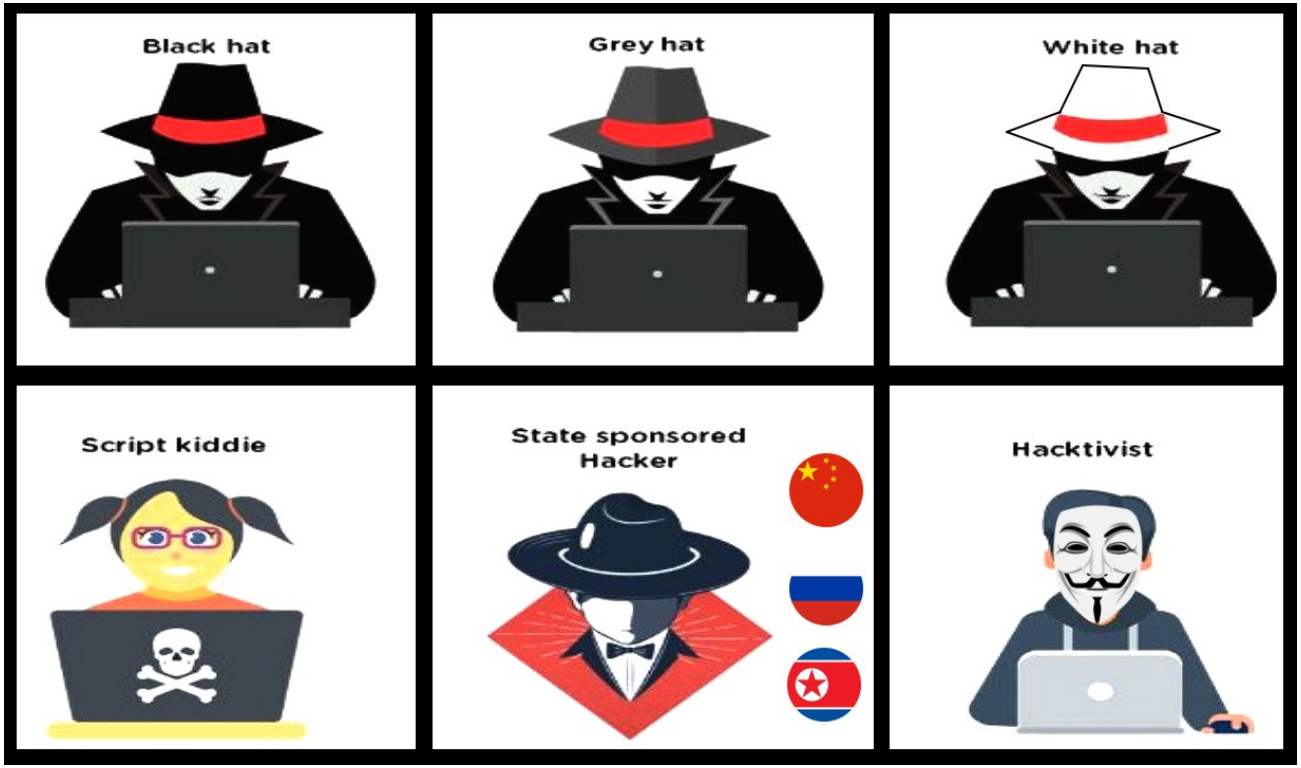
# #vírusok





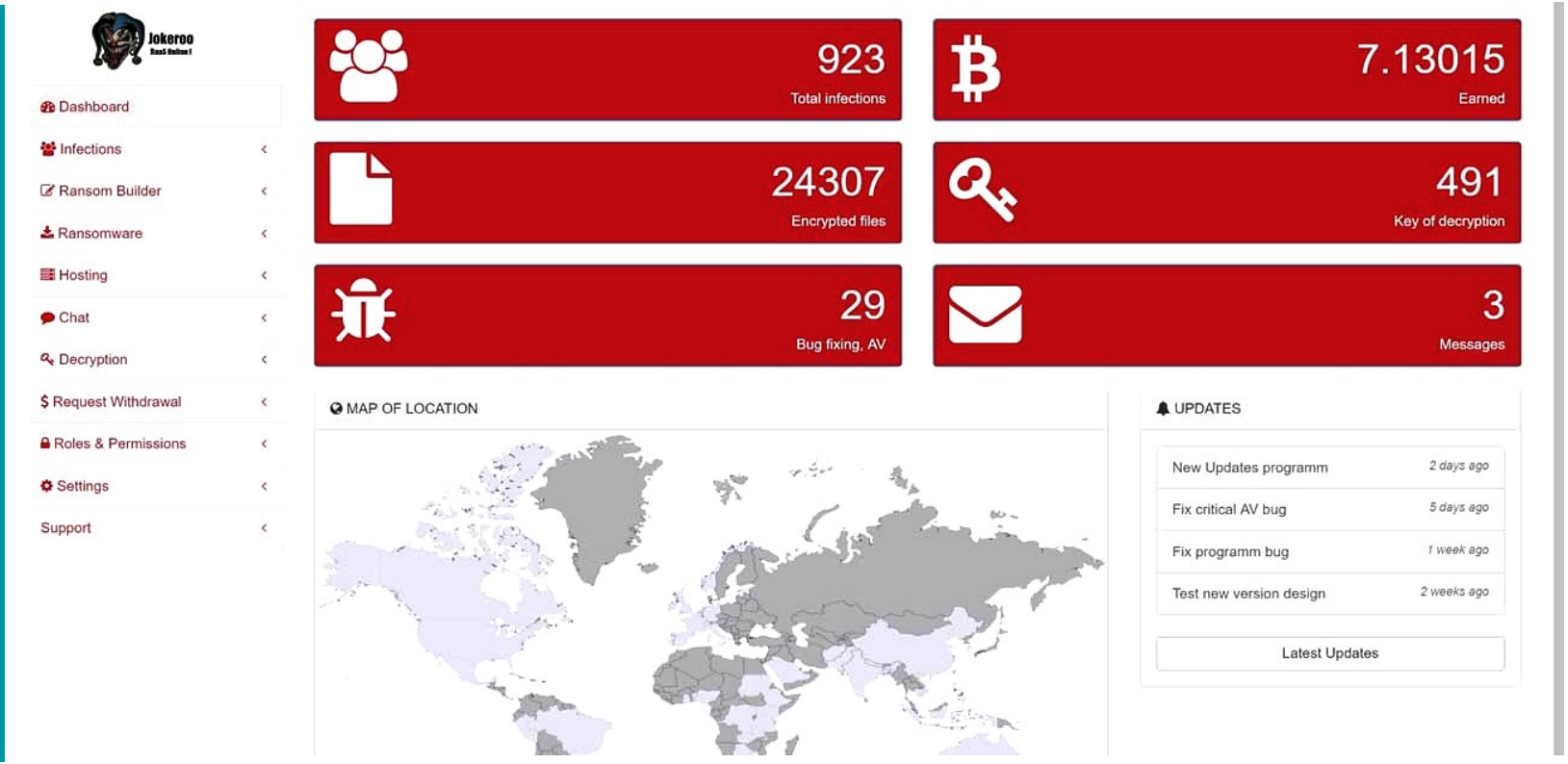
- 1986 - Brain 36 év
- 1.341 mrd egyedi kártékony kód (AVTest.org 2022. március 30.)

# #támadók



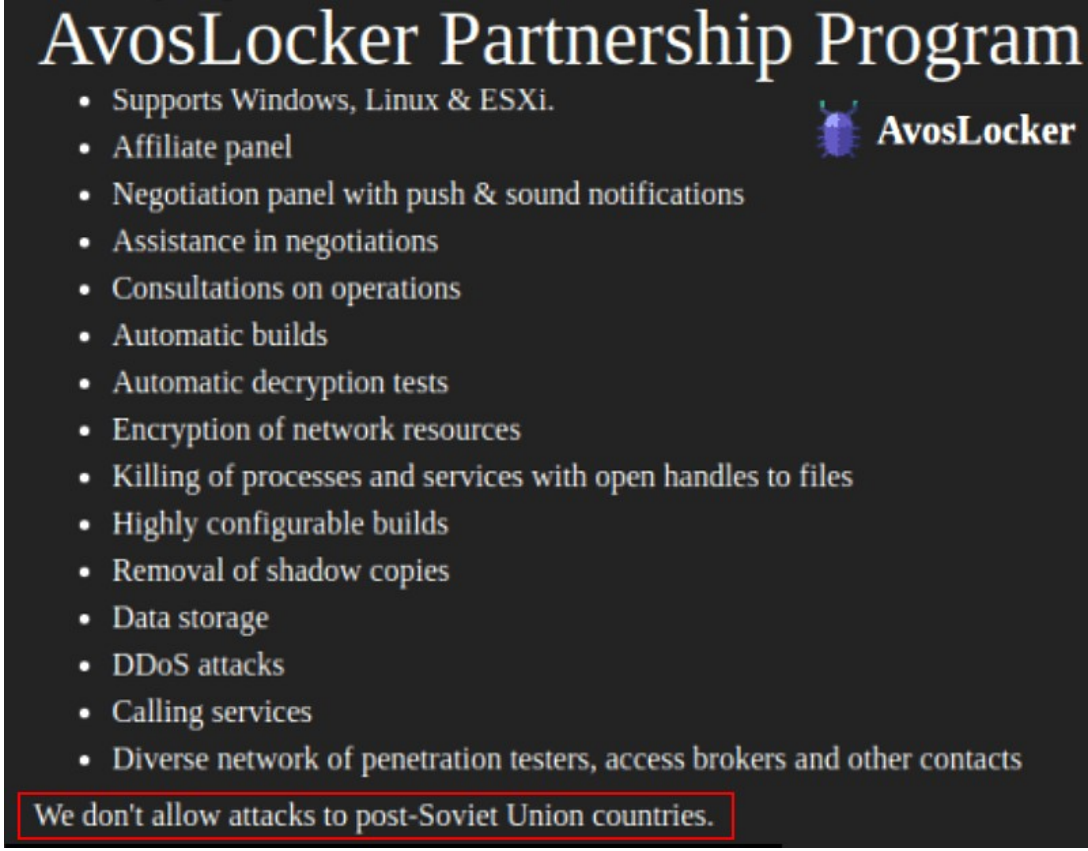

- script kiddie, hacktivist, elit hacker, állami kártevő, állami hacker, ransomware, ipari kémkedés
- automatizált eszközök, teljes bérelhető feketepiaci infrastruktúra a darkweben

# #RaaS - Ransomware as a Service




- 7/24 support, nyelvi támogatás, váltságdíj-tárgyalások kezelése, megszerzett adatok tárolása-közzététele, direkt telefonhívás

# #zsarolóvírusok




- hibrid ransomware
  titkosítás + doxing + DDoS

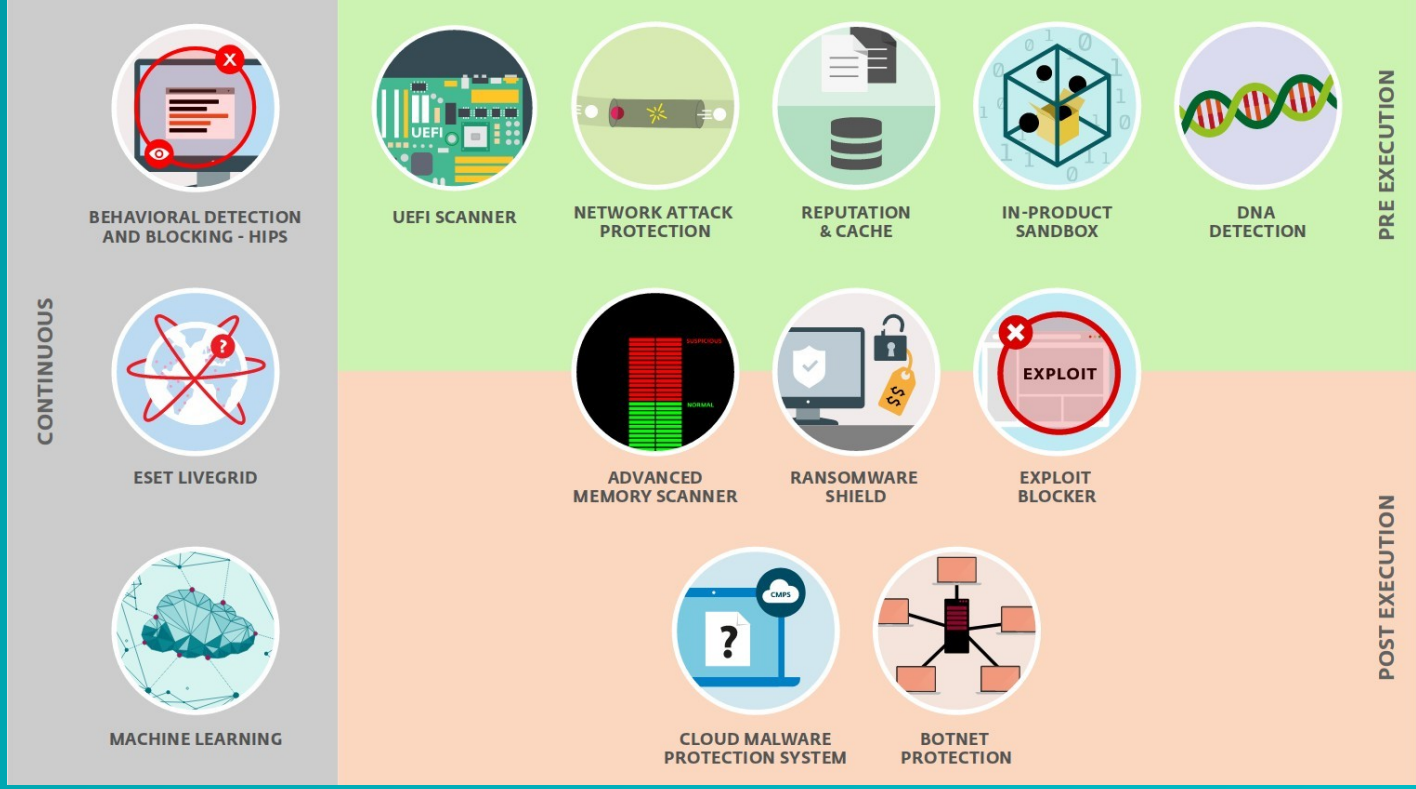
- USA pénzügyi szolgáltatók, iparvállalatok, kormányzati szervek

- ellopott adatok árverése a darkweben

# #zsarolóvírusok


- Észak-Korea – állami hackerek, nukleáris fegyverkezés
- 2021. átlagos váltságdíj 2.2m USD (Palo Alto Unit42, 144% nőtt)
- 2020. Oroszország betiltja a belföldi fizetést kriptovalutával
- És most a háborús szankciók alatt 2022-ben?

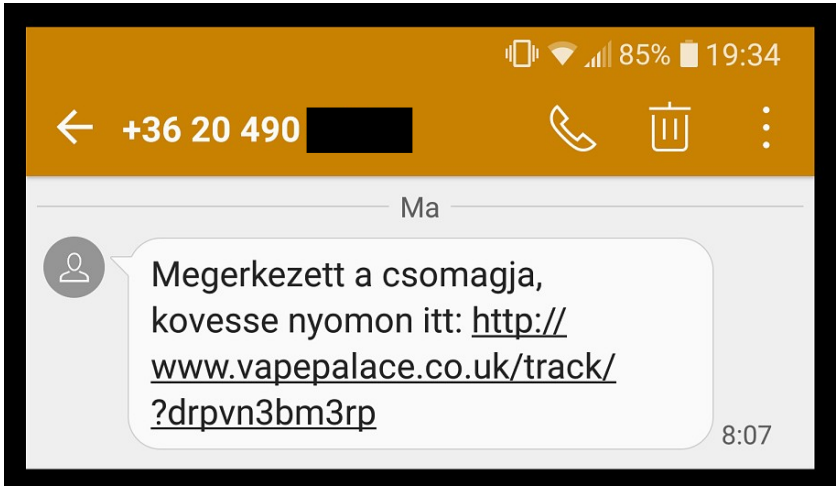
# #védelem




- Live Grid, Exploit Blocker, Botnet Protection, Antiransomware, stb.
- 1989-től adatgyűjtés-osztályozás, 1995-től gépi tanulás
- a védelemben 7 féle AI, víruslabor: automata és kézi elemzés
- ESET LiveGuard Advanced (Dynamic Threat Defense): 3 gépi tanulás + sandbox

# #PEBKAC

- összevissza telepítgetés
- engedély megadása gondolkodás nélkül
- 2021. március FedEx FluBot incidens
- "Accessibility services", 4700 SMS, banki adatok





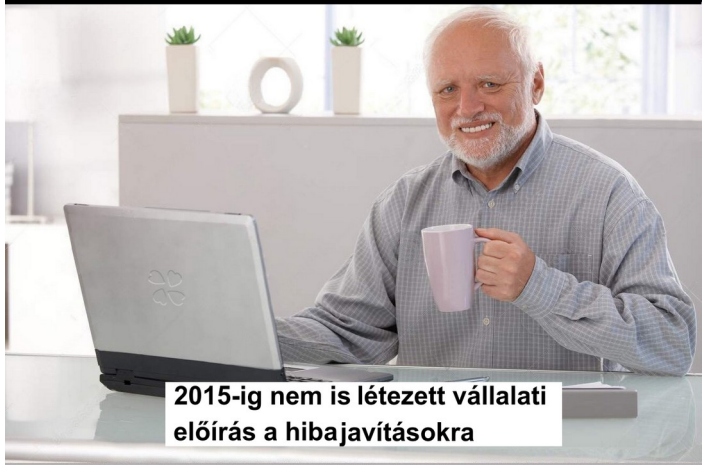
# #nem tanul, nem szorong, nem frissít

- WannaCry/WannaCryptor **2017.05.12.** VS. CVE-2017-5638 **2017.03.07.**

- azóta is globális fenyegetés: 2021-ben is 21.3% (ESET 2021. 2/3 riport)

- 2001. Nimda - 24 óra alatt 2.2 millió fertőzött gép - hiányzó frissítés

# #nem tanul, nem szorong, nem frissít

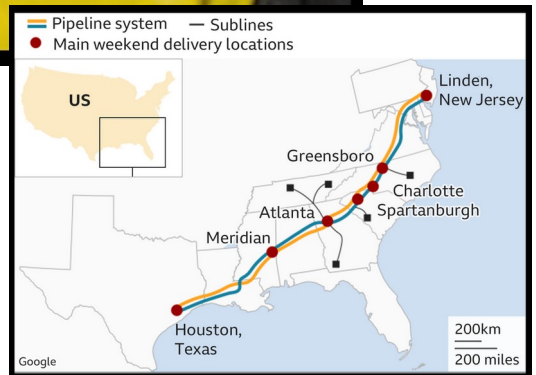





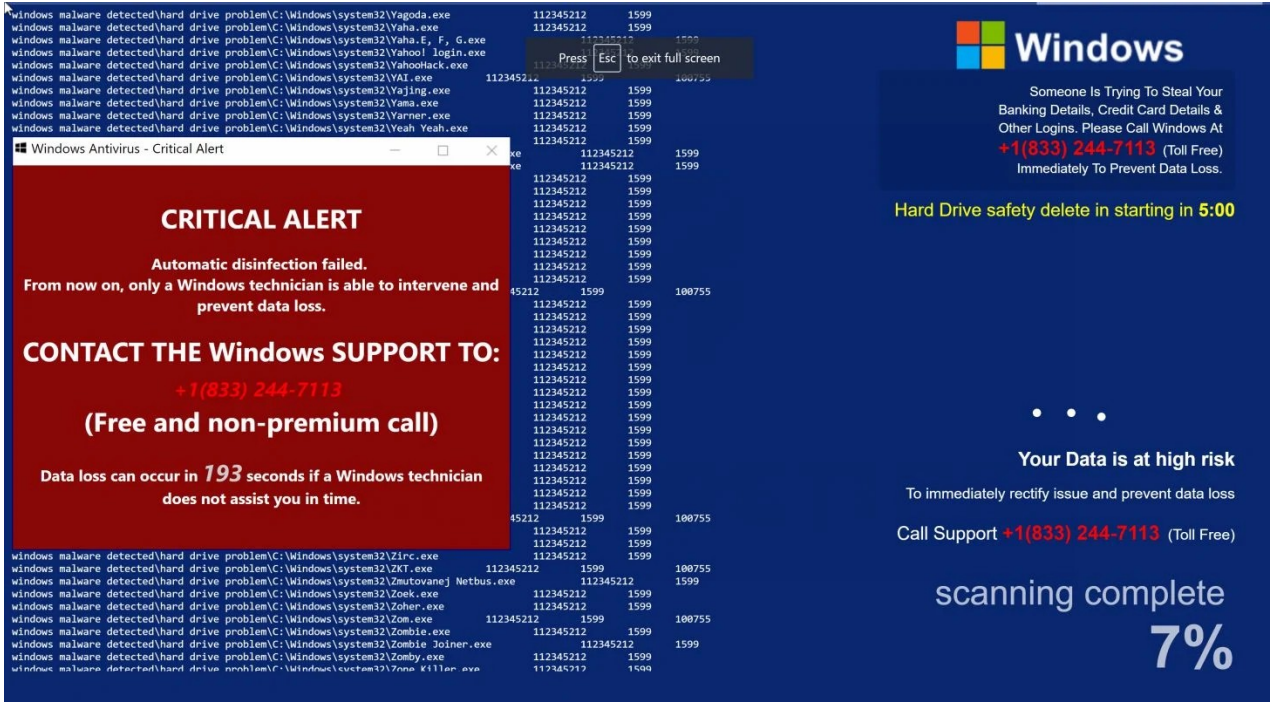
- Equifax 2017. 146m személyes adat
- Összesen 2mrd USD kár

# #nem tanul, nem szorong, nem 2FA


- Colonial Pipeline 2021. május
- Revil/Sodinokibi 4.4 mUSD
- darknetre szivárgott jelszavak
- mérnöki távmunka VPN no 2FA
- sérülő adatbiztonság:
  * sértetlenség
  * bizalmasság
  * rendelkezésre állás



# #social engineering




- fake support csalások: RAT, kémprogram

- pl. Amazon, Microsoft, Apple, PayPal

# #social engineering

- user bediktál banki adatokat a telefonba

- kérésre RAT-et telepít

- 2020. OTP, aláírási címpéldány SIM Swap

24.HU

BELFÖLD

## Egy óvatlan kattintás miatt 51 millió forintot loptak el egy budapesti házaspártól

Horváth Csaba László | 2020. 06. 08. 06:05

Kirívóan kedvező lakáshirdetéssel húztak csőbe egy budapesti családot, akik egész életük megtakarítását veszették el egy szempillantás alatt. A szélhámosok gondosan összehangolt lépésekkel, adathalászattal és SIM-cserés átveréssel szereztek hozzáférést a család bankszámlájához, ahonnan 51 millió forintot emeltek le. Noha a pórul járt házaspár is óvatlan volt, a történtek a Telekom felelősségét is felvethetik. A rendőrség nyomoz, az OTP Bank kivizsgálta az ügyet, és kártalanította ügyfeleit.

24.HU

BELFÖLD KORONAVÍRUS

## Telefonját blokkolva loptak el 30 milliót az OTP ügyfelétől, majd jött a koronavírus

Horváth Csaba László | 2020. 03. 31. 05:53

Attilának egyelőre ismeretlen módon jutottak hozzá a bankszámlájához, a járvány miatt pedig az ügyintézés is lelassult. A csaló köddé vált, a rendőrség nyomoz, az OTP Bank szerint ők nem hibáztak ugyan, de kárpótolták ügyfelüket. A 24.hu-nak nyilatkozó IT-biztonsági szakértő szerint valószínűleg SIM-kártya csalás történt.

# #boss attack

- Business E-mail Compromise, MS 2021. - céges e-mail csak 20%-a MFA

Sep 3, 2019, 04:42pm EDT | 55 714 views

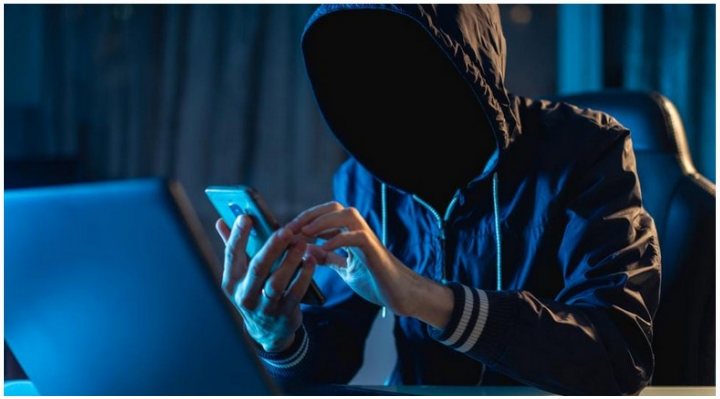
Forbes

## A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

**Jesse Damiani** Contributor

Consumer Tech

*I run Postreality Labs, a new media art advisory & curatorial studio.*



**It's the first noted instance of an artificial intelligence-generated voice deepfake used in a scam.**

Phone scams are nothing new, but the mark usually isn't an accomplished CEO.

According to a new report in *The Wall Street Journal*, the CEO of an unnamed UK-based energy firm believed he was on the phone with his boss, the chief executive of firm's the German parent company, when he followed the orders to immediately transfer €220,000 (approx. $243,000) to the bank account of a Hungarian supplier.

- 2019. RealTalk program: DeepVoice hangszintetizálás
- 220e EUR (72m HUF) brit energetikai cég
- német CEO kért brit CEO-tól utalást egy magyar beszállító számlájára

# #a bennfentes

- belső érintett, gondatlanság, sértett vagy zsarolható alkalmazott

- 34% insider threat (Swiss Cyber Institute)

- bennfentes toborzás

- pl. Lockbit, Netwalkwer

- céges RDP, VPN, levelezés, vállalati hozzáférések

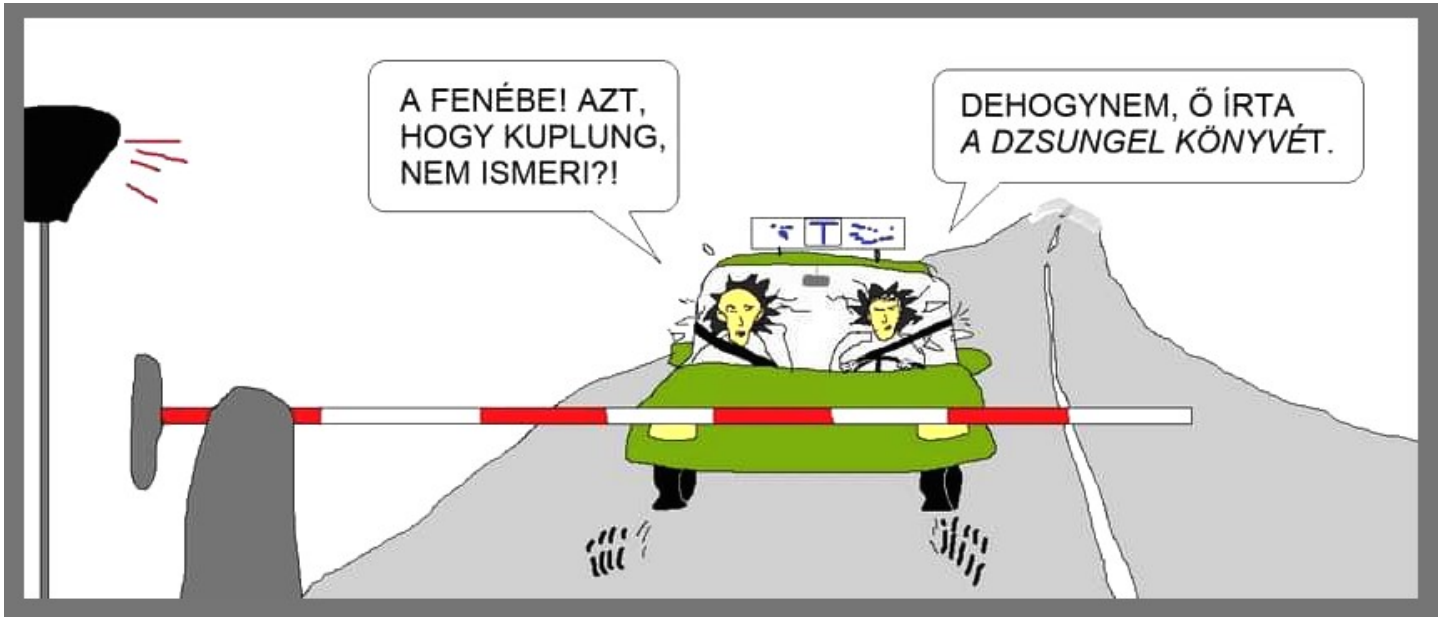
- pénzjutalom + "teljes anonimitás"

# #megoldás (főnév), vízszintes 8 betű

- rendszeres biztonsági mentés, automatizált patchmenedzsment, naprakész vírusvédelem, biztonságos hálózati beállítások, erős jelszavak és hitelesítés, 2FA/MFA alkalmazása, biztonsági policy, adminisztrátori jogosultságok korlátozása, érzékeny adatok titkosítása, hálózatok szegmentálása, folyamatosan fejlesztett védelem, pentest, audit, SOC, stb.

# #biztonságtudatosság

- Security awareness, biztonsági szabályzat, cégpolicy
- 2010. Busher Stuxnet – USB kulcs
- **rendszeres képzés, tréning**




- mesterséges és természetes intelligencia :-)

# Köszönöm a figyelmet!

info@sicontact.hu

Digital Security
**Progress. Protected.**