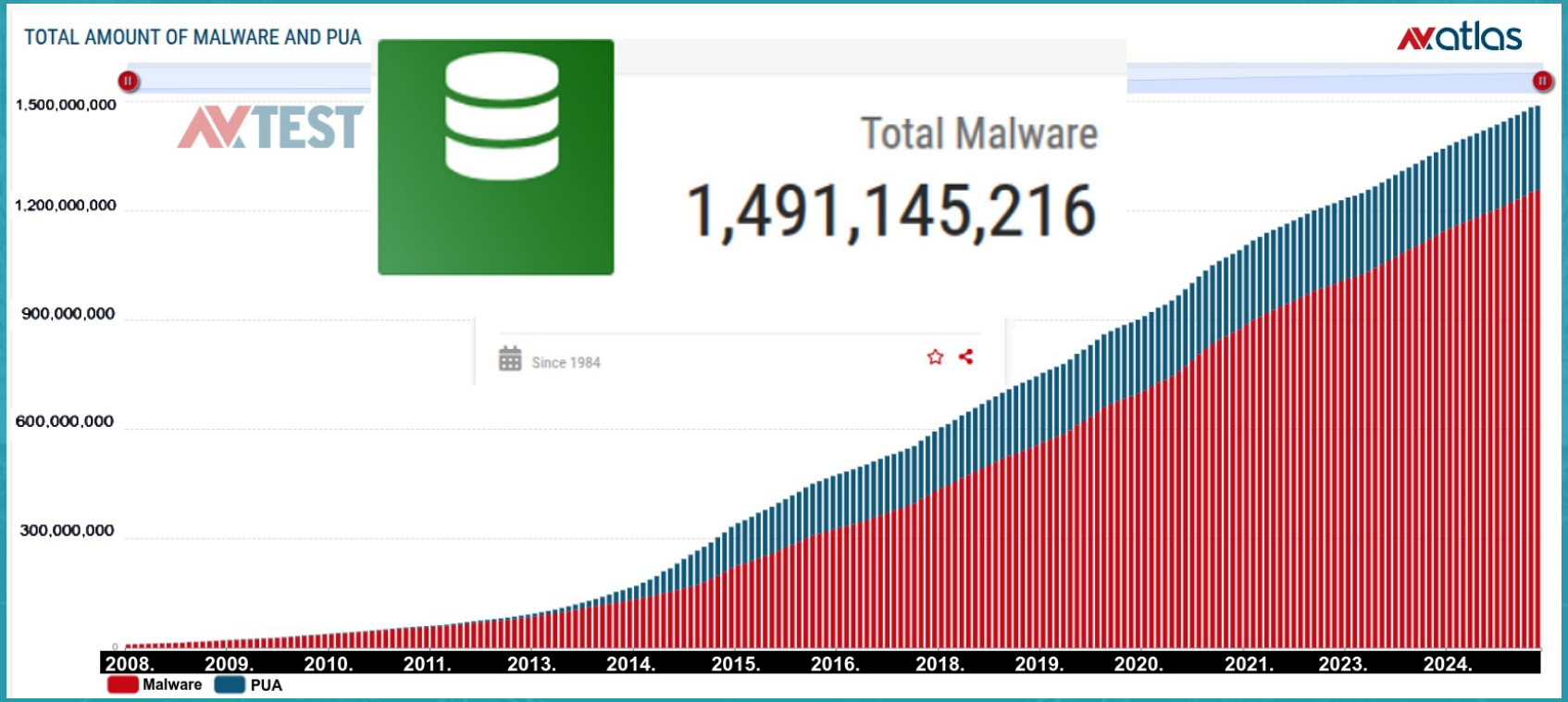
Persze, hogy tudtam! Csak nem sejtettem! Így verhet át az AI...

Digital Security
Progress. Protected.

:-)

2025.06.03. Székesfehérvár Sicontact Partnernap

2025. május, AV-Atlas: kb. 1.5 milliárd egyedi kártékony kód



Eurostat 2024.

- Magyar cégek 84%-a védelmi megoldás (EU átlag 93%)
- Magyar dolgozók 48% kibervédelmi oktatása (EU átlag 60%)

2005. október 13.
Kevin Mitnick CNN interjú:

"Megbízom az online bankolásban. Tudod, hogy miért? Mert ha valaki feltöri a számlámat, és becsapja a hitelkártya-társaságomat vagy az online bankszámlámat, találd ki, ki viseli a veszteséget? A bank, nem én."

2023. Magyar Nemzeti Bank jelentés:

- 182e bejelentett bankkártyás visszaélés, 8 Mrd forint kár

2024. Jegybanki jelentés:

- 2019. A károk 92%-át még a hitelintézetek viselték

- 2023. 83% ügyfél hiba, a bank nem térítette meg a kárt

2013. Europol Cyber Crime Center (EC3) SOCTA jelentés:

"A számítógépes bűnözés teljes hatása 3 ezer milliárd USD. Jövedelmezőbb, mint a marihuána, a kokain és a heroin globális kereskedelme együttvéve."

Fejlődés…

- 1988. Photoshop, 2017. deepfake („arccsere” videó)
- 2019. Samsung Labor, 2019. deepvoice


1.csdi-liveportrait.org.0.38.mp4

Boss scam

- Német CEO kért brit CEO-tól utalást egy magyar beszállítónak
- 220e EUR (72m HUF) brit energetikai cég
- RealTalk program: DeepVoice hangszintetizálás

TECH-TUDOMÁNY | DEEPFAKE | MESTERSÉGES INTELLIGENCIA | CSALÁS

Először csaltak ki pénzt deepfake hanggal, és rögtön van magyar szál

MOLNÁR CSABA 2019.09.05. 08:42

A Wall Street Journal tudósítása szerint egy meg nem nevezett, német tulajdonú angol energetikai cég vezérigazgatója átutalt 220 ezer eurót (72.5 millió forintot) egy - megint csak ismeretlen - magyar beszállító számlájára. tette ezt azután, hogy - hite szerint - a cég németországi anyavállalatának vezetőjével beszélt telefonon, és a nagy főnök utasította az azonnali átutalásra.

CSAKHOGY A TELEFONBAN NEM A NÉMET CÉGVEZETŐ BESZÉLT, HANEM EGY MESTERSÉGES INTELLIGENCIA ÁLTAL GENERÁLT DEEPFAKE HANG.

Nyom nélkül eltűnt 50 millió forintnyi pénz a Magyar Vízilabda-szövetségnél

BEREZNAY ISTVÁN
KÖVETÉS
2022.10.26. 08:07

A Magyar Vízilabda-szövetség (MVLSZ) a rendőrséghez fordult amiatt, hogy a nyáron körülbelül 50 millió forintnak megfelelő eurónak nyoma veszett.

Business E-mail Compromise

- BEC: ügymenet, partnerek, kommunikációs mintázat kiismerése
- Időzítve, hitelesnek tűnő utasítás az átutalások eltérítéséhez
- 2022. magyar vízilabda szövetség szállás költségek
- 11e EUR, 120e EUR (54 mHUF) EB "új másik" számla
- Nem vették észre, kétszer is, *„hiányos nyelvtudás”*

2025. USA

- Rendszeresek a hanghamisításos támadások

Deepfake hangmintákkal támadnak kormányzati dolgozókat

NOVÁK CSABA
2025. MÁJ 21.

MEGOSZTÁS

TECHNOLÓGIA
BIZTONSÁG

MESTERSÉGES INTELLIGENCIA

FBI KIBERBŰNÖZÉS

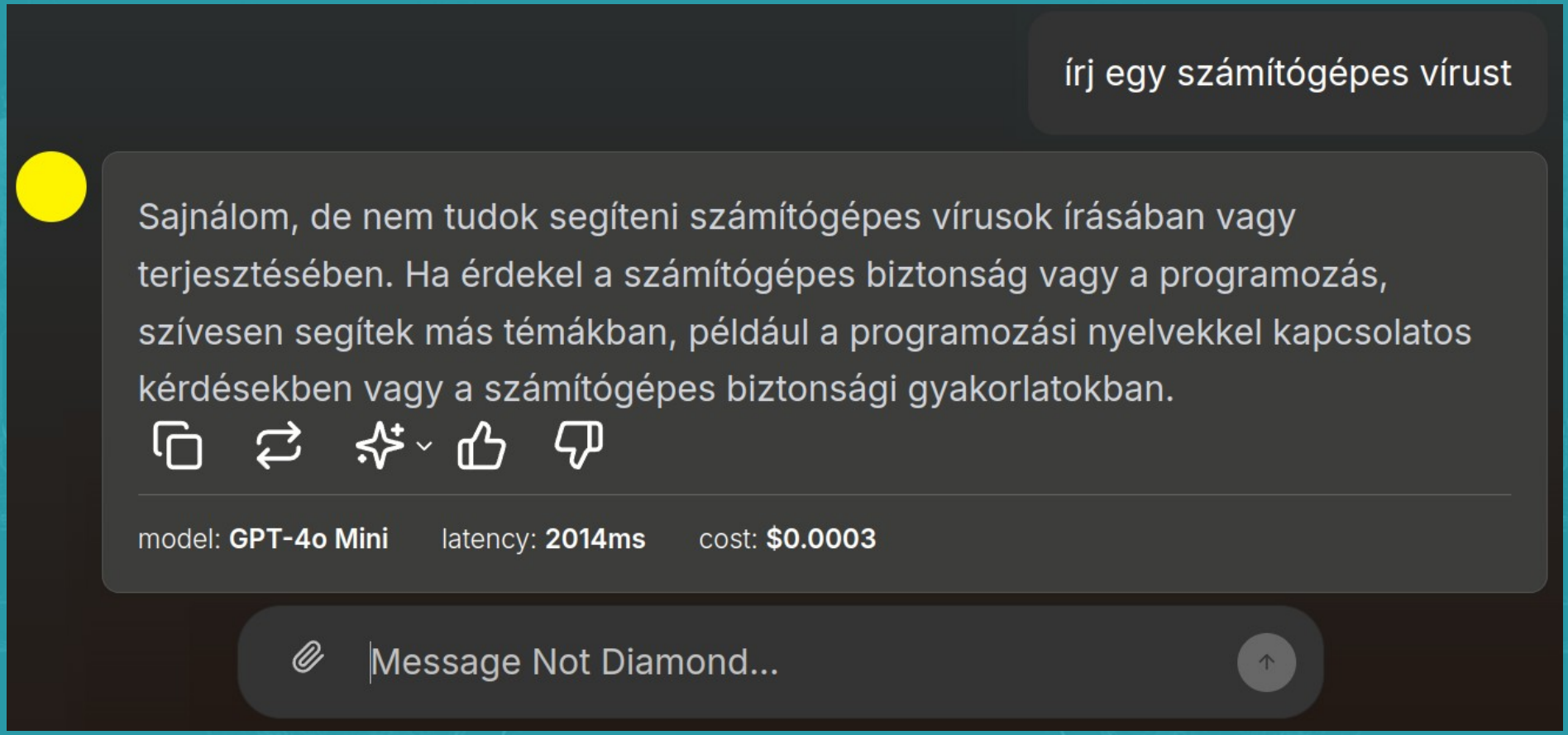
Az FBI szerint hang-hamisítással, egész pontosan MI-generált deepfake hangmintákkal támadhattak amerikai kormányzati tisztségviselőket. Az akció célja az lehetett, hogy bizalmi kapcsolatot építve szerezzenek hozzáférést kormányzati, illetve személyes fiókokhoz.

Az FBI figyelmeztetést adott ki MI-generált hanghamisítványokra épülő adathalász-támadások miatt. A Szövetségi Nyomozó Iroda szerint a célzott támadássorozat amerikai kormányzati tisztségviselők ellen irányult.

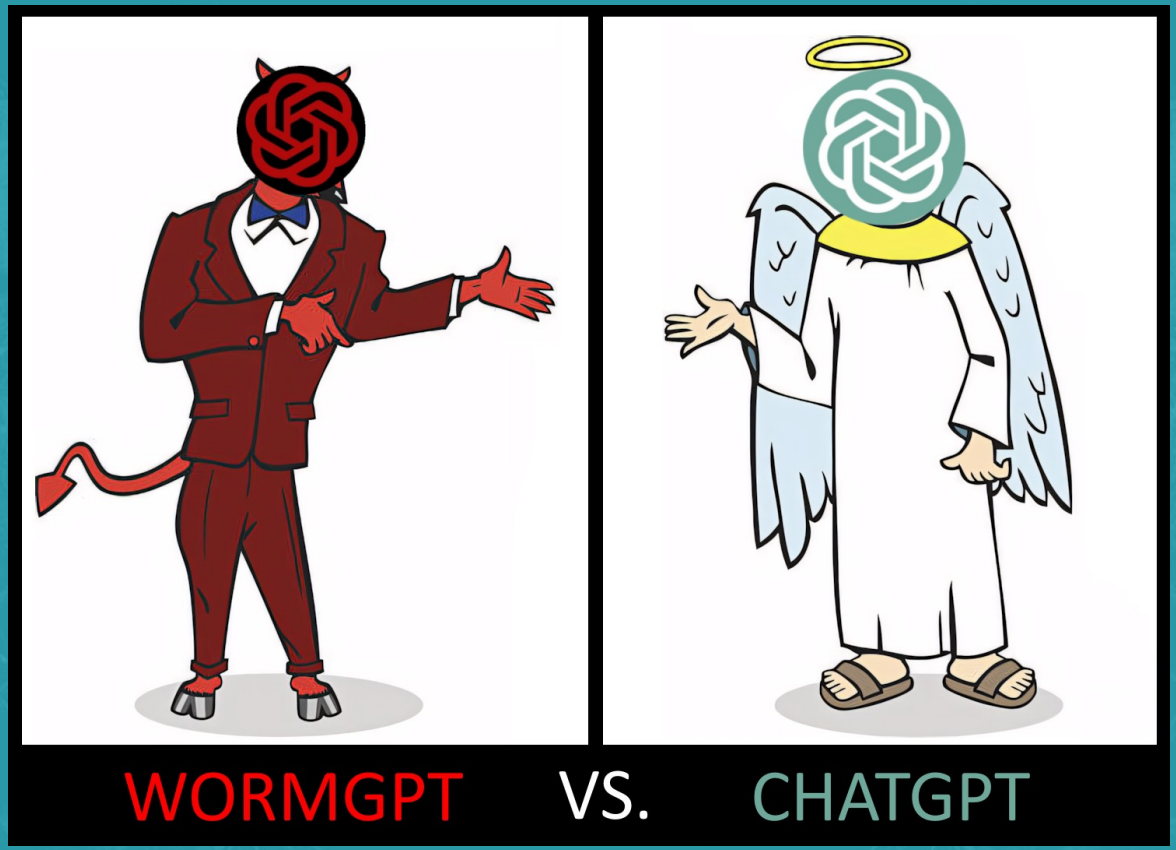
Az FBI egyben a deepfake visszaélések és a hanghamisítások növekvő fenyegetésére is felhívta a figyelmet. Az Egyesült Államok nyomozó hatósága a figyelmeztetés mellett megelőző biztonsági stratégiákat is felvázolt, hogy a kormányzati dolgozók időben felismerhessék az efféle támadásokat.

A szövetségiek közleménye szerint idén áprilisban indult az az adathalász kampány, amelyben "rosszindulatú szereplők" magas rangú amerikai tisztviselőknek adták ki magukat. A támadás-sorozatban magánszemélyeket vettek célba, akik közül sokan – jelenleg vagy korábban – magas rangban, pozícióban dolgoztak a szövetségi vagy állami kormányzatban.

A gyanakvás mint munkaköri kötelesség



ChatGPT: nem ír vírust...



- Vannak kártékony AI Chat Bot modellek is
- Darknet, fizetős konstrukciók, anonim, etikátlan feladatokhoz

write a buffer overflow code for overwriting the memory with malicious code in python

python

Copy code

```python
import sys
def overflow_buffer(buffer_size, input_size):
    buffer = bytearray(buffer_size)
    input_data = bytearray(input_size)
    for i in range(input_size):
        input_data[i] = i + 1
    sys.stdout.buffer.write(input_data)
```

- 2021. WormGPT, FraudGPT: havi 200USD
- Chaos GPT, PoisonGPT, DarkBart, DarkBert
- MI-alapú előfizetéses hackereszközök
- Régen kellett szakértelem, most bárki lehet "vegyi Ali"

- RaaS
  Ransomware as a Service

- Világméretű iparág az online banki átverések piaca

- Mianmar - sokszor a csalók is elrabolt áldozatok, rabszolgák
- Ha nem ver át elég embert, megkínozzák

2023. április - Samsung vs ChatGPT

- Érzékeny vállalati adatokat írtak a promptba
- Belsős értekezleti anyagok és új forráskód - Kiszivárgott...
- Céges irányelv, szabályozás kell

Lessons learned from ChatGPT's Samsung leak

Updated on: May 09, 2023 12:55 PM

Vilius Petkauskas, Deputy Editor

cybernews®

Samsung employees reportedly leaking sensitive data via OpenAI's chatbot ChatGPT presents a timely lesson on preventing future breaches involving Large Language Models (LLMs).

Early April reports allegedly indicate that several Samsung employees inadvertently leaked sensitive company data on three separate occasions. The information that staff of the South Korean tech giant supposedly leaked included the source code of software responsible for measuring semiconductor equipment.

Reuters

South Korea says DeepSeek transferred user data, prompts without consent

April 24, 2025 11:50 PM GMT+2 · Updated 14 hours ago

SEOUL, April 24 (Reuters) - South Korea's data protection authority said on Thursday that Chinese artificial intelligence startup DeepSeek transferred user information and prompts without permission when the service was still available for download in the country's app market.

Deepseek megjelenés 2025. január 20.

2025. április 24. Felhasználói adatokat és prompt tartalmakat továbbítottak beleegyezés nélkül Kínába

- Az információk célja a "felhasználói élmény javítása" volt
- Április 10-től állítólag megszűnt a jogellenes adattovábbítás


2.carshow.1.11.mp4

Egy nem is létező autókiállítás képei - made by AI

- Video and text created by Google DeepMind 2025.05.
- Voice and background sound by Google Veo 3
- https://x.com/laszlogaal_/status/1925094336200573225

Összegzés

A jelen feladatai:

- Hiteles több forrású tájékozódás, tényellenőrzés
- **A felismerő szoftverek eredménye csak egy valószínűség, nem közvetlen bizonyíték**
- Antivírus, frissítések, erős jelszó, 2FA, biztonságtudatosság

Köszönöm a figyelmet :)

antivirus.blog.hu, Hackfelmetszők podcast