Kibertámadások, amelyek tönkretehetik a cégünket

XXXI. ORSZÁGOS KÖNYVVIZSGÁLÓI KONFERENCIA

ESET Digital Security
Progress. Protected.

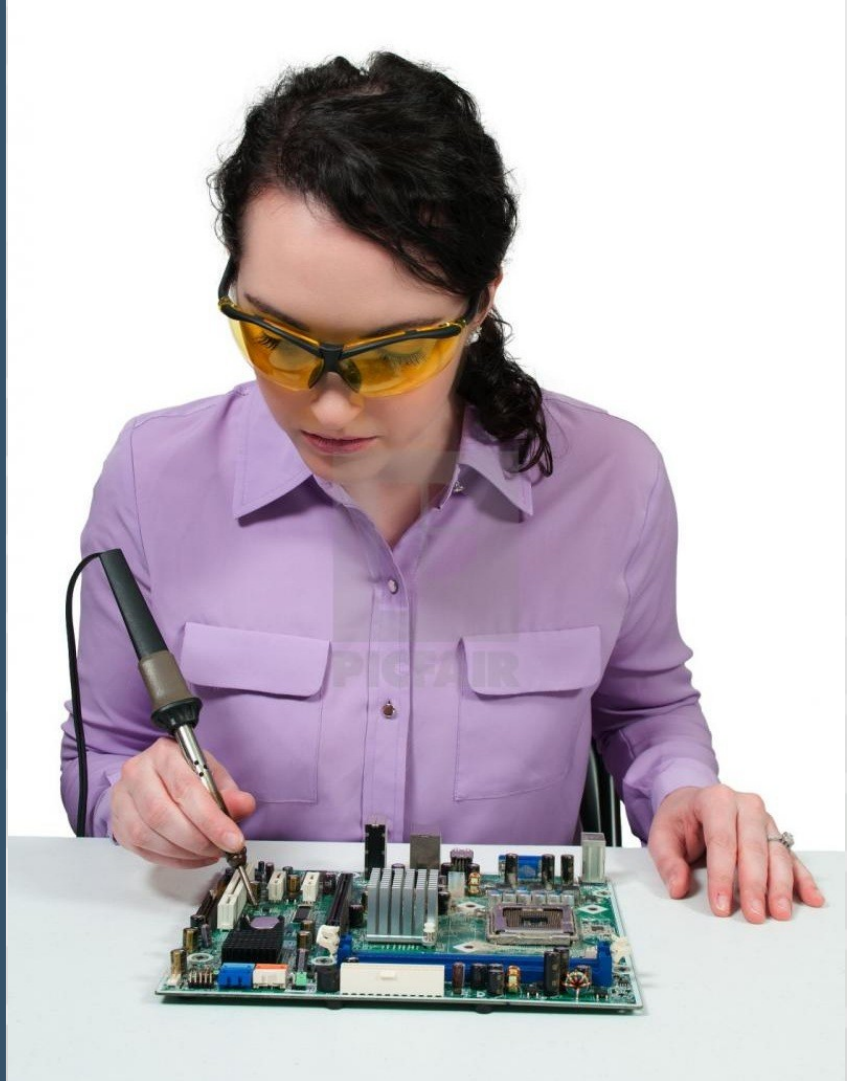
2023. szeptember 13.

Csizmazia-Darab István

[Rambo]

IT biztonsági szakértő, ESET/Sicontact

TARTALOM



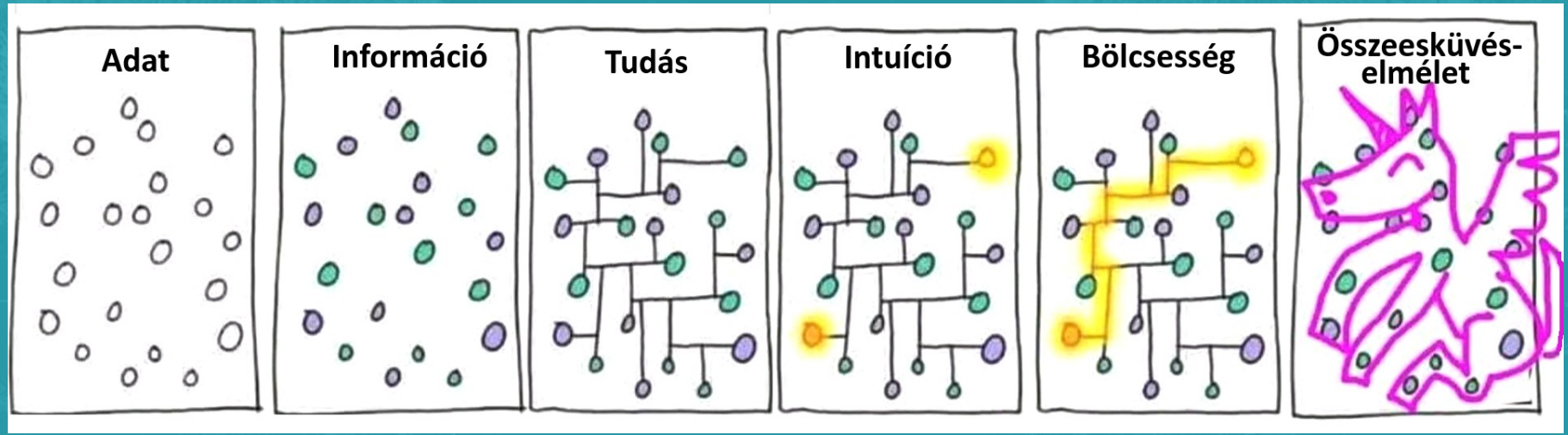
- A jövő itt van, és sose lesz vége

- Más kárán tanulni

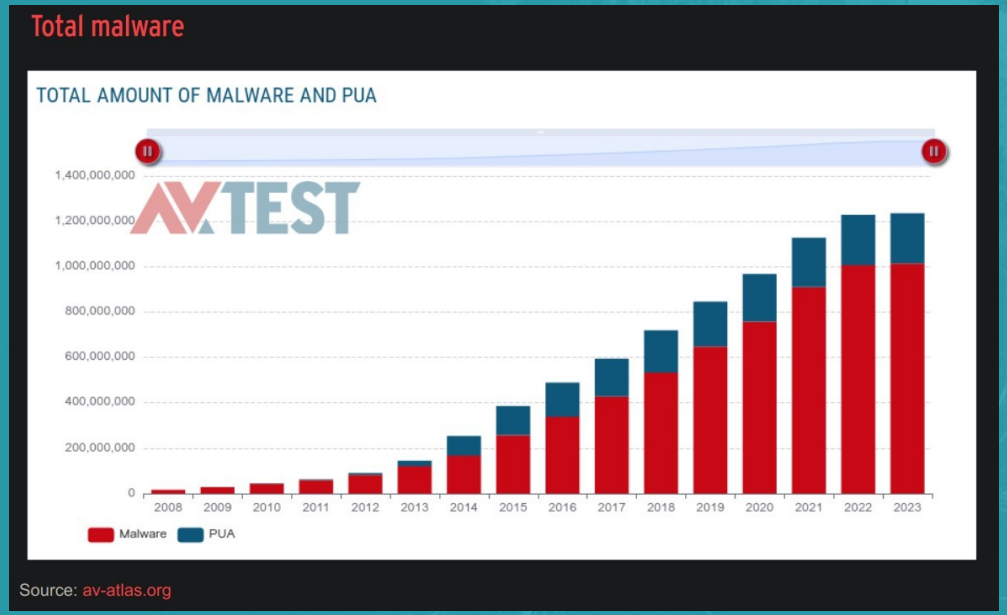
- Megelőzés, védekezés

Technológiai szingularitás:

"A mesterséges intelligencia megjelenése miatt a technológiai fejlődés és a társadalmi változások annyira felgyorsulnak, amit korábbi generációk képtelenek felfogni vagy megbízhatóan kezelni."



Vírusok, kártevők 1986.



- 1.21mrd egyedi kártékony kód (AV-Test.org)
- 207e biztonsági rés (CVE-Mitre Exploits cve.org)
- 5.18mrd netező (Statista.com)
- 12.5mrd feltört, ellopott jelszó (Haveibeenpwnd.com)

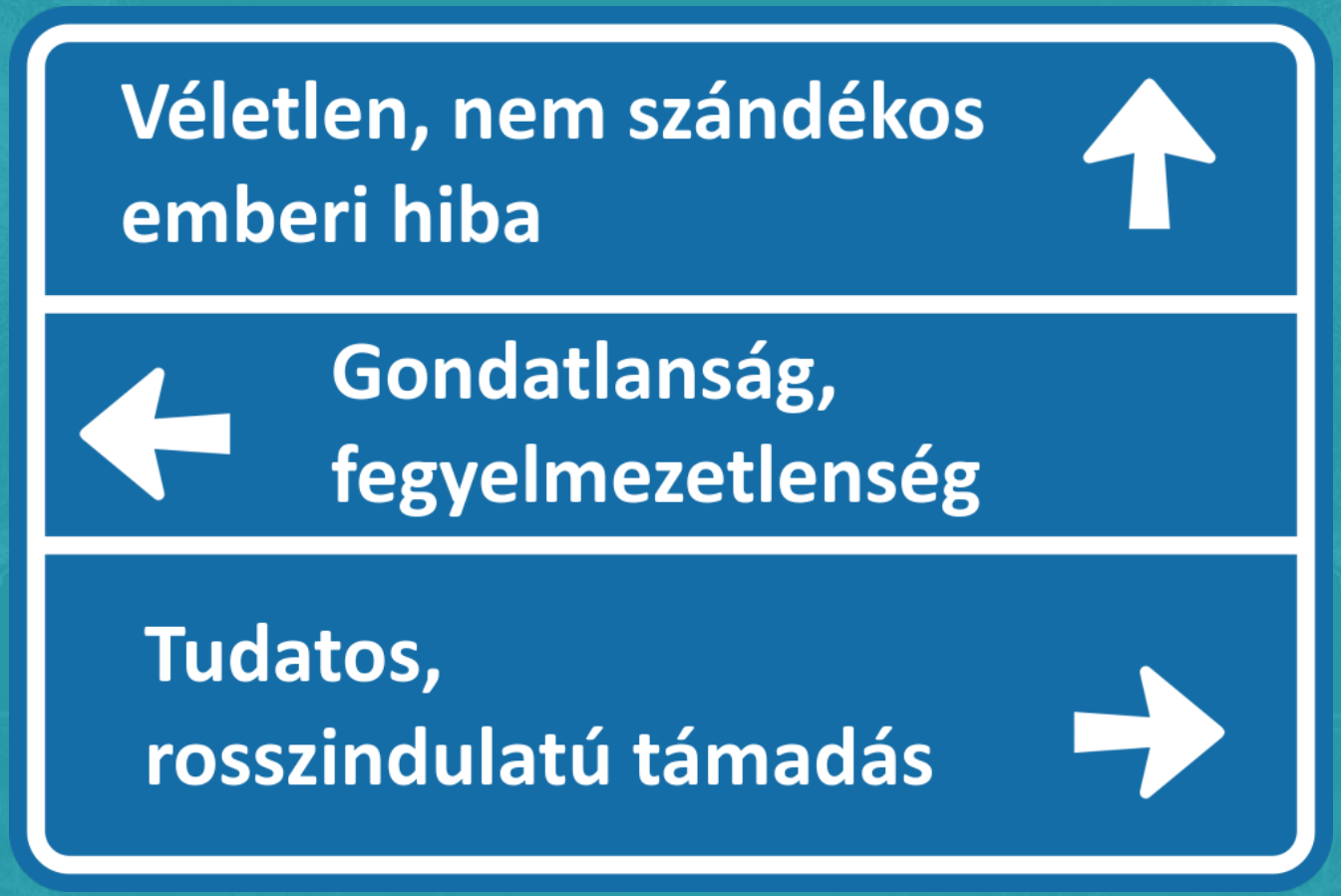
Ransomware 2013-20??

- Állomány titkosítás, váltságdíj
- Doxing: adatlopás, kiszivárogtatás, darknet, GDPR
- Működő modell: RaaS, kulcsrakész megoldások, 7/24 support

2021. Colonial Pipeline csővezetékrendszer

- USA keleti part, több hetes üzemanyaghiány, pénzügyi veszteség
- 4.4m USD (1.3mrd HUF) váltságdíj, de a visszafejtő lassú volt
- Saját korábbi biztonsági mentések
- Távmunkás mérnökök, kompromittált vezérlési jelszó, 2FA nélkül

Az alkalmazotti hibák 3 leggyakoribb oka



1. Véletlen, nem szándékos emberi hiba

Mulasztás, hibás beállítások (pl. RDP), ellopott-elvesztett adathordozók, nem törölt leselejtezett eszközök), stb.

1. Véletlen, nem szándékos emberi hiba

Hertfordshire-i Egyetem, 200 használt USB (100 USA, 100 UK)
- 20 olvasható
- 135 free recovery szoftver percek alatt, 44 azonosítható tulajdonos
- 34 célszoftverrel visszaállíthatatlanul törölve
- 1 eszközön volt csak titkosítás
- Bizalmas vállalati és jogi dokumentum, adóbevallás, fizetési ívek, készpénzről és lőfegyverekről készült fényképek, házkutatási parancs, meztelen fotók névvel és elérhetőséggel

2. Gondatlanság, fegyelmezetlenség

Szakmai ismeretek hiánya, figyelmeztetések semmibevétele, BYOD, ShadowIT, jelszavak mentése a böngészőben, OpenRelay
- Programozási mulasztások: bruteforce védelem, input ellenőrzés, jelszóhash sózás, cleartext jelszó lista, patch management, stb.

2. Gondatlanság, fegyelmezetlenség

2017.03.07. Critical
CVE-2017-5638

The Register®
Biting the hand that feeds IT

Missed patch caused Equifax data breach

Apache Struts was popped, but company had at least TWO MONTHS to fix it

By Simon Sharwood, APAC Editor 14 Sep 2017 at 02:09 10 SHARE ▼

Equifax has revealed that the cause of its massive data breach was flaw it should have patched weeks before it was attacked.

The company has updated its www.equifaxsecurity2017.com/ site with a new “A Progress Update for Consumers” that opens as follows:

- USA 3 nagy hitelminősítő ügynökségének egyike
- Incidens május 13-tól július 30-ig, felfedezés csak július 29-én
- Adózási- és béradatok, hitelinformációk, munkaügyi adatok
- 143m személyes adat (USA total: 325m), 209e hitelkártya adat
- Nem volt céges policy és kijelölt felelős a hibajavításokra

3. Tudatos, rosszindulatú támadás

- A megkérdezett szervezetek 74%-a tartja legjelentősebb oknak a belső fenyegetéseket

3. Tudatos, rosszindulatú támadás

2015.05. JP Morgan Chase korábbi munkatársa, FBI letartóztatás
- Peter Persaud árulta az ügyfelek bizalmas számlainformációit

2021. LockBit sértett bennfentes munkavállalók toborzása
- Pénzjutalom céges RDP, VPN, levelező szerver hozzáférésért
- Anonimitás ígérete a belsős besúgónak

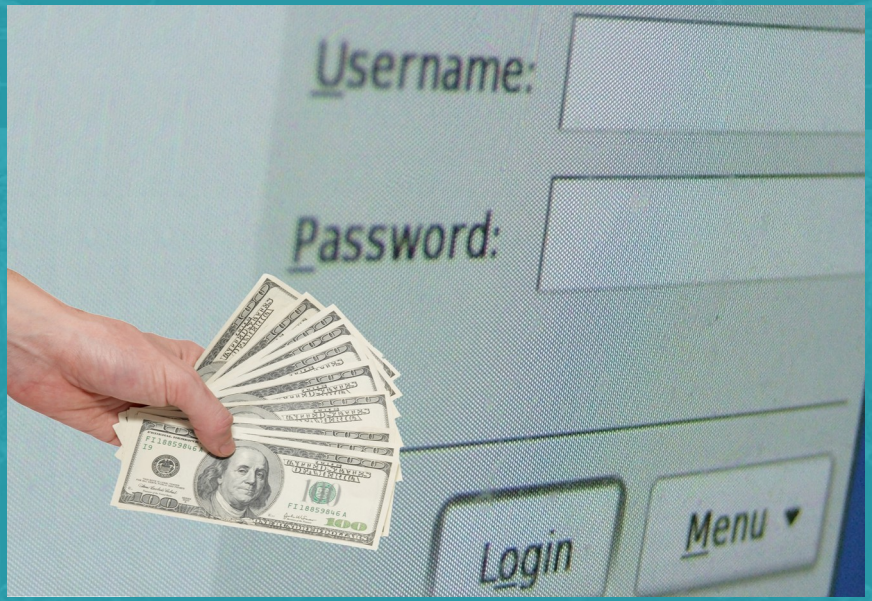
Távozó munkavállalók I.

A távozók 45%-a töröl, letölt, továbbküld vagy kiszivárogtat!

- A szervezetek 43% nincs szabályzat, ami tiltja, hogy távozáskor magukkal vigyék a munkahelyi adatokat
- UK: csak a vállalatok 47%-a vonja vissza az épületi hozzáférést
- Csak 62% kéri vissza a vállalati eszközöket a kilépett dolgozóktól

Távozó munkavállalók II.

- **Sailpoint felmérés:** az elbocsátott brit munkavállalók 14%-a már 100 fontért (40e HUF) eladná korábbi céges jelszavait



- **HelpNetSecurity jelentés:** a korábbi IT munkavállalók 25%-a a régi jelszavával azóta is hozzáfér az előző cégbeli hálózathoz

- sőt 16%-nak az összes korábbi munkahelyéhez van élő hozzáférése

Social engineering (Kevin Mitnick, 1963-2023)

- A felhasználó hiszékeny, gyanútlan, kíváncsi...

"Egy vállalat több százezer dollárt költhet tűzfalakra, behatolásjelző rendszerekre, titkosítási és egyéb biztonsági technológiákra, de ha a támadó fel tud hívni valakit a vállalaton belül, aki bediktálja neki a jelszavát, akkor a technológiára költött pénz lényegében elpazarolt."

Színre lép a mesterséges intelligencia

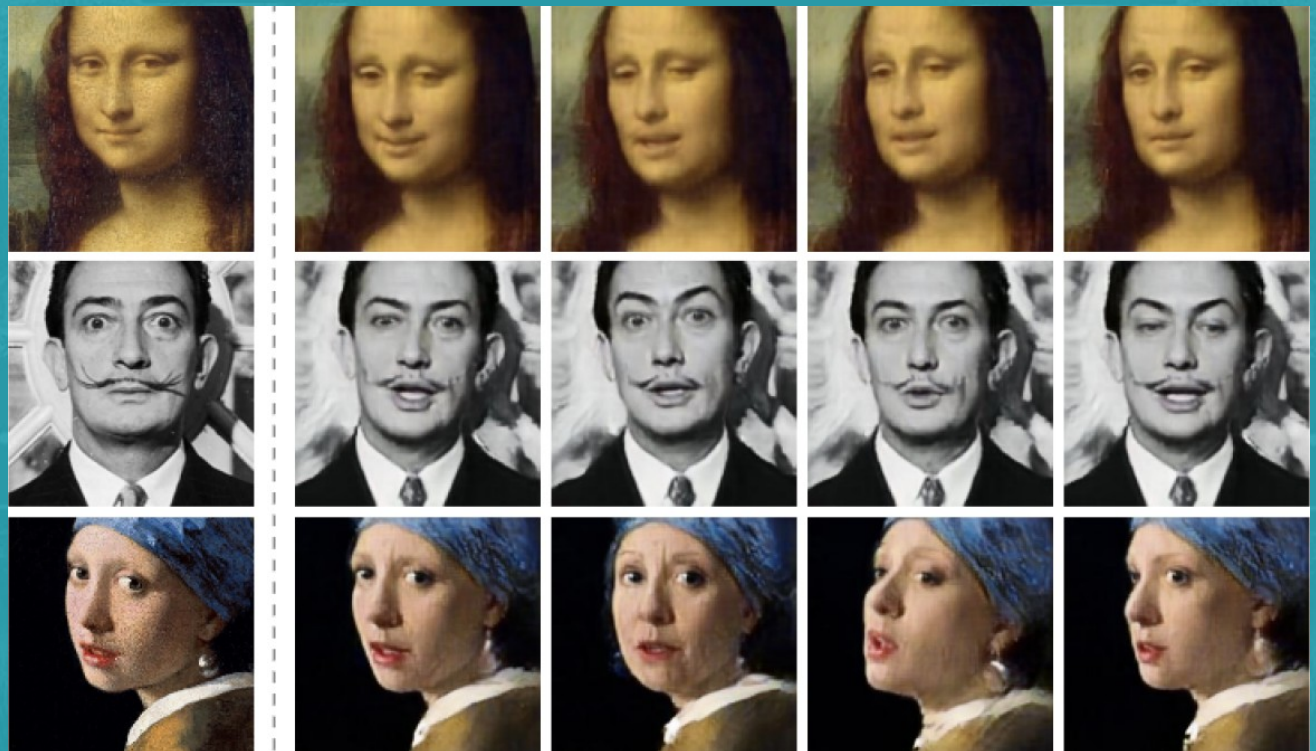
Színre lép a mesterséges intelligencia I.

1990. Whale vírus DOS - titkosított, polimorf, mutálódik
1997. Deep Blue VS Kasparov - 4:2
2016. AlphaGo VS Lee Sedol - 4:1 Google DeepMind Challenge
2016.03.23. Tay M$ chatbot, 24 óra, Hitlert élteti, lekapcsolják
2018. Vanda TELEKOM chatbot

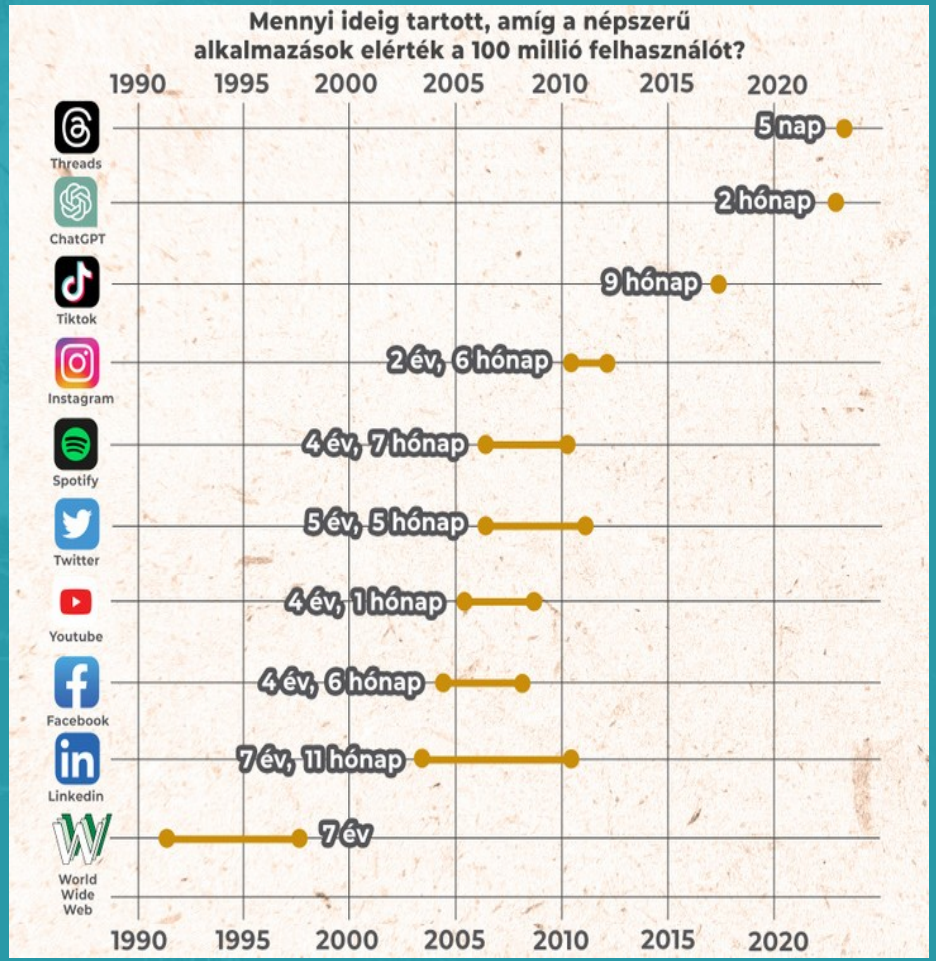
A jövő itt van, és sose lesz vége

Színre lép a mesterséges intelligencia II.

- 1988. Photoshop, 2018. deepfake, 2019. Samsung, 2019. deepvoice
- Deepfake “arccsere” video Photoshop, fake news
- Látszólag egy ismerősünk is könyöröghet pénzért
- ElevenLabs AI Voice cloning, EU+USA hangazonosítás=ujjlenyomat



Színre lép a mesterséges intelligencia III.



- 2022. ChatGPT - 2 hónap

2023. április - Samsung

- Belsős értekezleti anyagok és új forráskód

- Bizalmas anyagokat itt készítettek, javítgattak

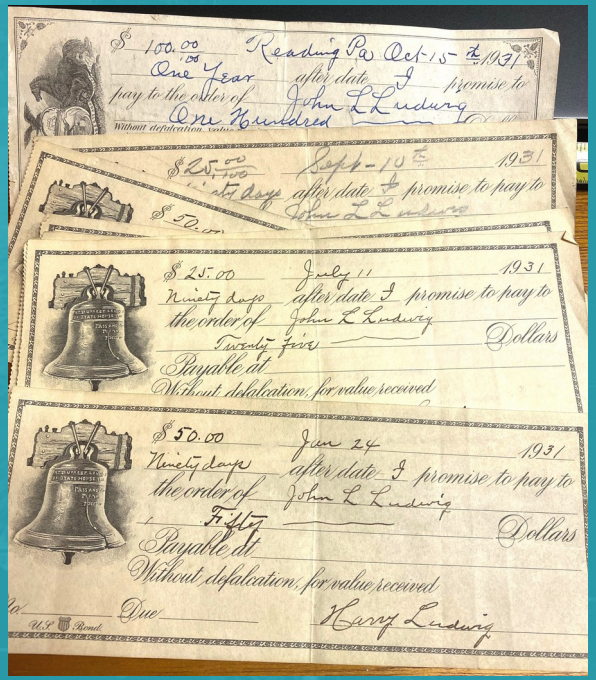
- Kiszivárgott...

A jövő itt van, és sose lesz vége

Színre lép a mesterséges intelligencia IV.

- 2022. Crayion AI generator - témáról festmény, fotó generálás
- Midjourney - ősember, Trump, pufidzsekis Pápa, Leonardo
- 2023. NVIDIA már tárgyi modellt is képes generálni 3D printhez

Business E-mail Compromise I.



- Egyre több célzott és testre szabott támadás
- Boss transfer trükk: a támadó a cég CEO-jának adja ki magát
- Azonnali bizalmas tranzakciókat hagyat jóvá
- Phishing, smishing, vishing, quishing

Business E-mail Compromise II.

2019. brit energia cég

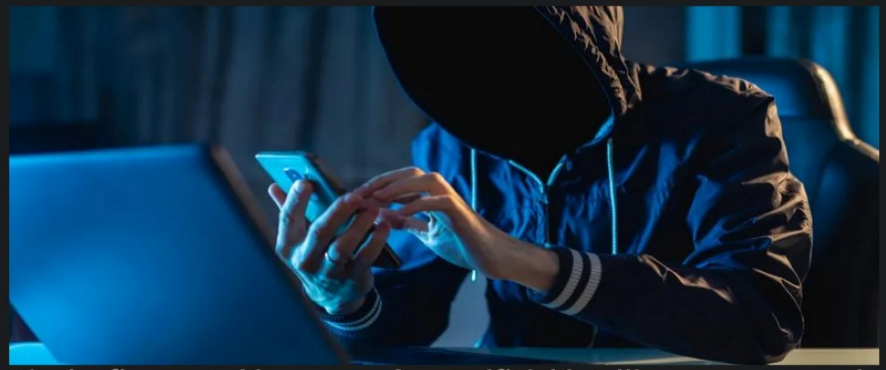
- Brit CEO 220e EUR (72m HUF) utalt egy magyar beszállító számlájára
- Hallotta a német CEO hangját a telefonban
- RealTALK voice cloning: akcentus, hanglejtés, sebesség
- Azonnal továbbutalták egy mexikói számlaszámra

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

Jesse Damiani Contributor ⓘ
I run the Reality Studies newsletter & Postreality Labs consultancy

Forbes Follow

Sep 3, 2019, 04:42pm EDT



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

Business E-mail Compromise III.

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

Más kárán tanulni

Krízis kommunikáció - 2011. DigiNotar Hollandia

- Iráni hekkerek hozzáfértek a tanúsítványokat kibocsátó rendszerhez
- Hónapokig nem is vették észre
- Csak belső vizsgálat, nem értesítették a partnereket:
  "az incidens hatása minimális"
- Több száz hitelesnek látszó hamis tanúsítványt állítottak ki a nevükben
- A kitudódás után a hamis tanúsítványokat vissza kellett vonni
- Még abban az évben csődbe mentek

Megelőzés, védekezés I.

- Fizikai és IT védelem

- Jelszavak és tárolásuk,
  pl. ESET Smart Security Premium

- Hozzáférési jogosultság korlátozás, 2FA, MFA
  pl. ESET Secure Authentication

- Titkosítás
  pl. ESET Endpoint Encryption
  Központi menedzsment

Megelőzés, védekezés II.

- Automatizált patchmenedzsment
  pl. ESET Vulnerability & Patch management (Complete és Elite comag részeként)

- Rendszeres biztonsági mentés külső adathordozóra

- Folyamatos DLP
  (Data Loss Prevention)
  pl. Safetica Protection

Megelőzés, védekezés III.

- Adatvédelmi szabályzat
- BYOD és ShadowIT szabályozás
- Pénzügyi kontroll protokoll
- Biztonságtudatossági képzések

Köszönöm a figyelmet!

info@sicontact.hu

www.eset.hu