CIO HUNGARY

2021.09.1-2.

Durva incidensek a karanténos távmunka idején...

Csizmazia-Darab István

IT biztonsági szakértő, ESET/Sicontact

csizmazia-darab.istvan@sicontact.hu

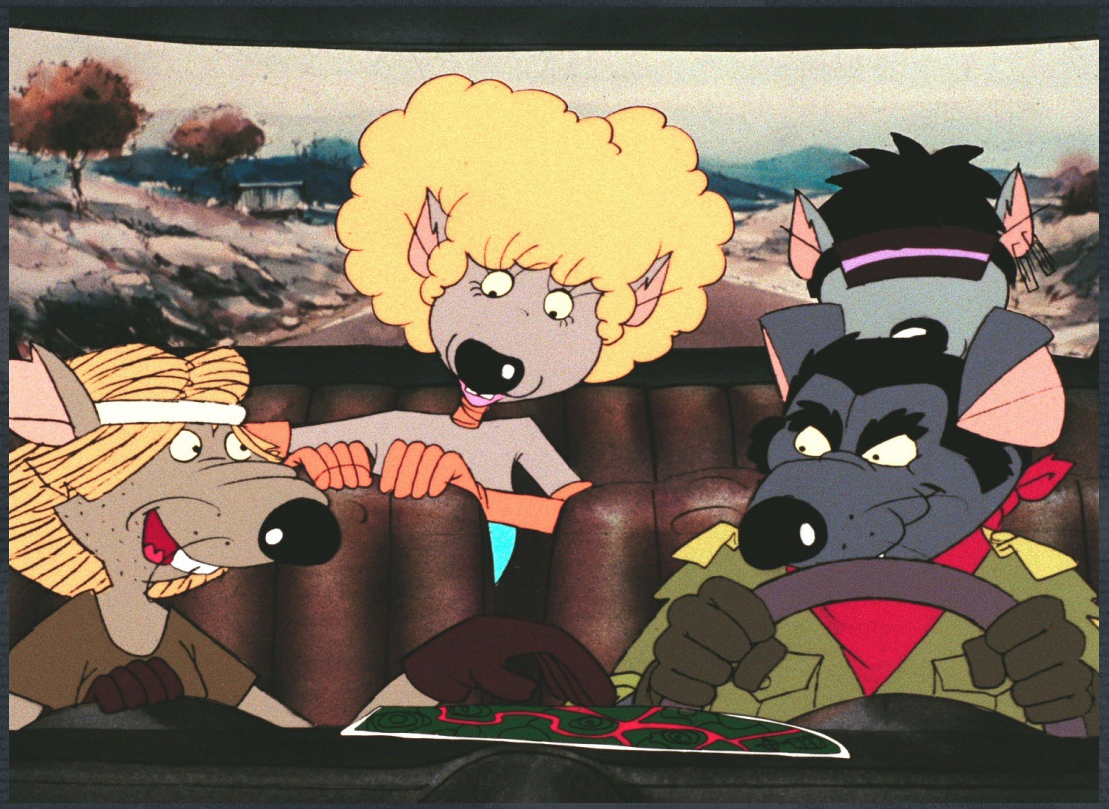
Ide a dohánnyal, vagy ízekre pofoztatom magam!
És ezt nyugodtan vehetik fenyegetésnek!

2008. USA: több pénz a kiberbűnözésből, mint a drogkereskedelemből: 105 Mrd USD

Mi történt magával, Safranek?
A borotválkozásnál megvágtam magam, uram.

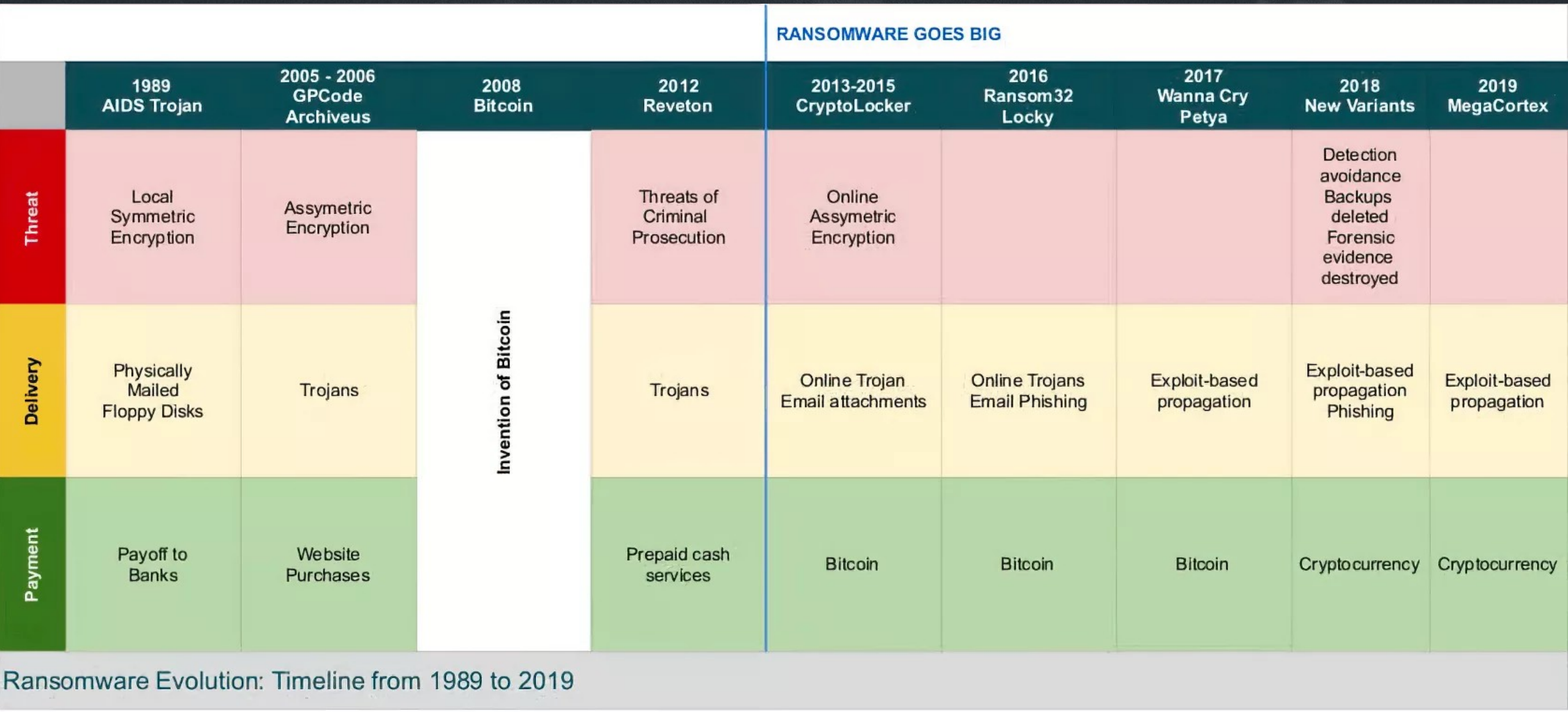
- 2013. Cryptolocker
- igazi veszteség okozása
- nyereséges üzleti modell
- 2015. óta OSX és Linux is (KeRanger, Linux.Encoder)
- azóta is a leggyakoribb veszély

A harmadik törvény, a jó gengszter mindig álcázza magát.



- erős, egyedi titkosítás: 1024, 2048 RSA kulcs
- később még erősebb ECC (Elliptical Curve Cryptography)
- C&C szerver rejtett TOR hálózat, "lenyomozhatatlan" Bitcoin, kriptovaluták
- kevés univerzális helyreállító, pl. AV letöltési oldalakon
- gyűjtemény www.getcryptostopper.com/ransomware-decryptors/

Siker esetében szabad reménykednem némi külön-jutalomban?



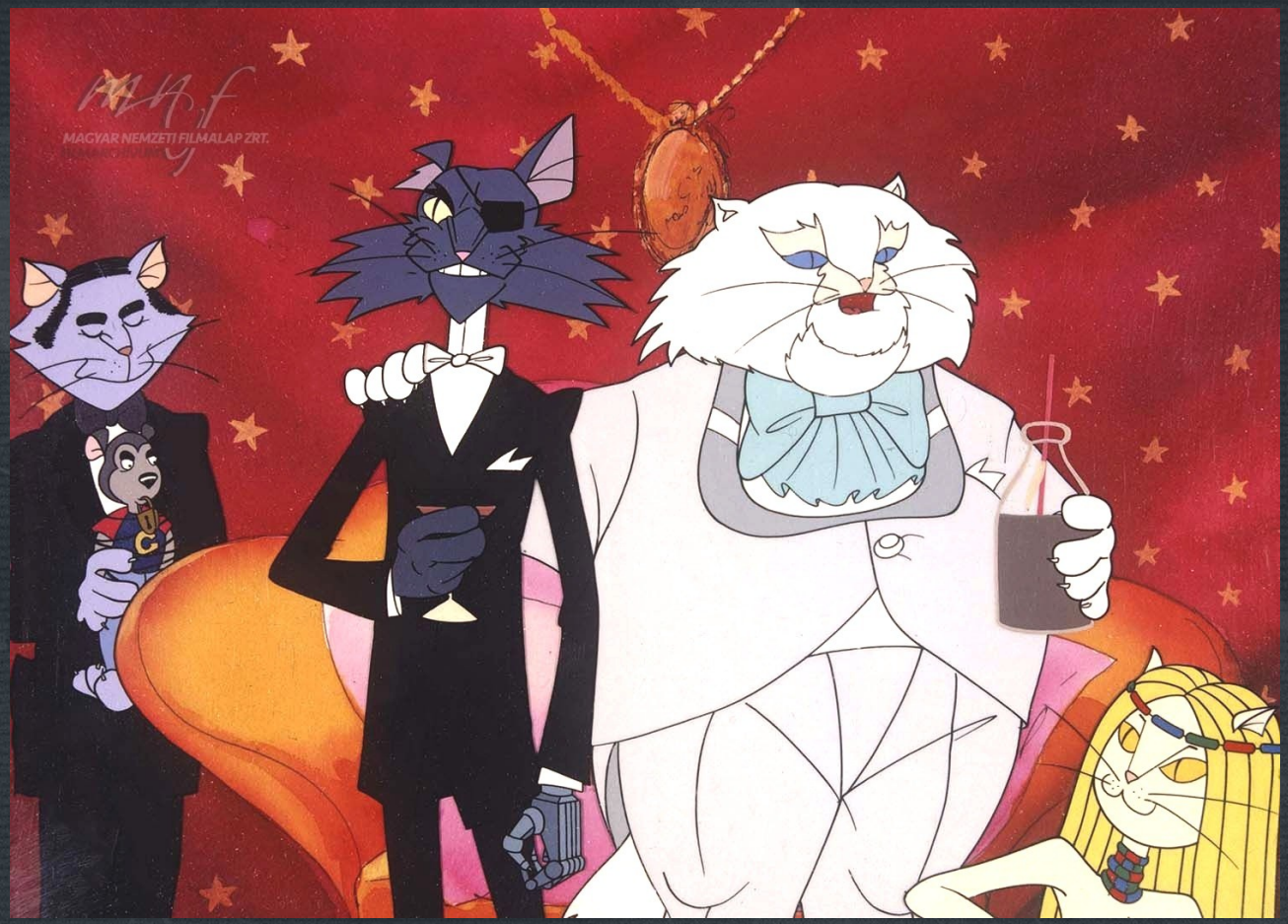
Ransomware Evolution: Timeline from 1989 to 2019

Ha akcióba lép ez a gang, Ön hátradõlhet miszter,
nálunk nem lesz semmi gikszer...

Célkeresztben - akikre a legtöbbször lőnek

- kórházak, állami intézmények, hivatalok
- COVID alatt tesztközpontok, kutatóintézetek, gyógyszeripar, minden IS ;-)

Kivel kötünk üzletet?



- Grál lovag VS. bűnöző - vajon kapunk feloldókulcsot?
- FBI állásfoglalás
- tudunk-e tárgyalni, alkudni?

Lúzerek, Darwin díjasok
Na gyerünk Safranek, ne tettesse magát hülyébbnek, mint amilyen!

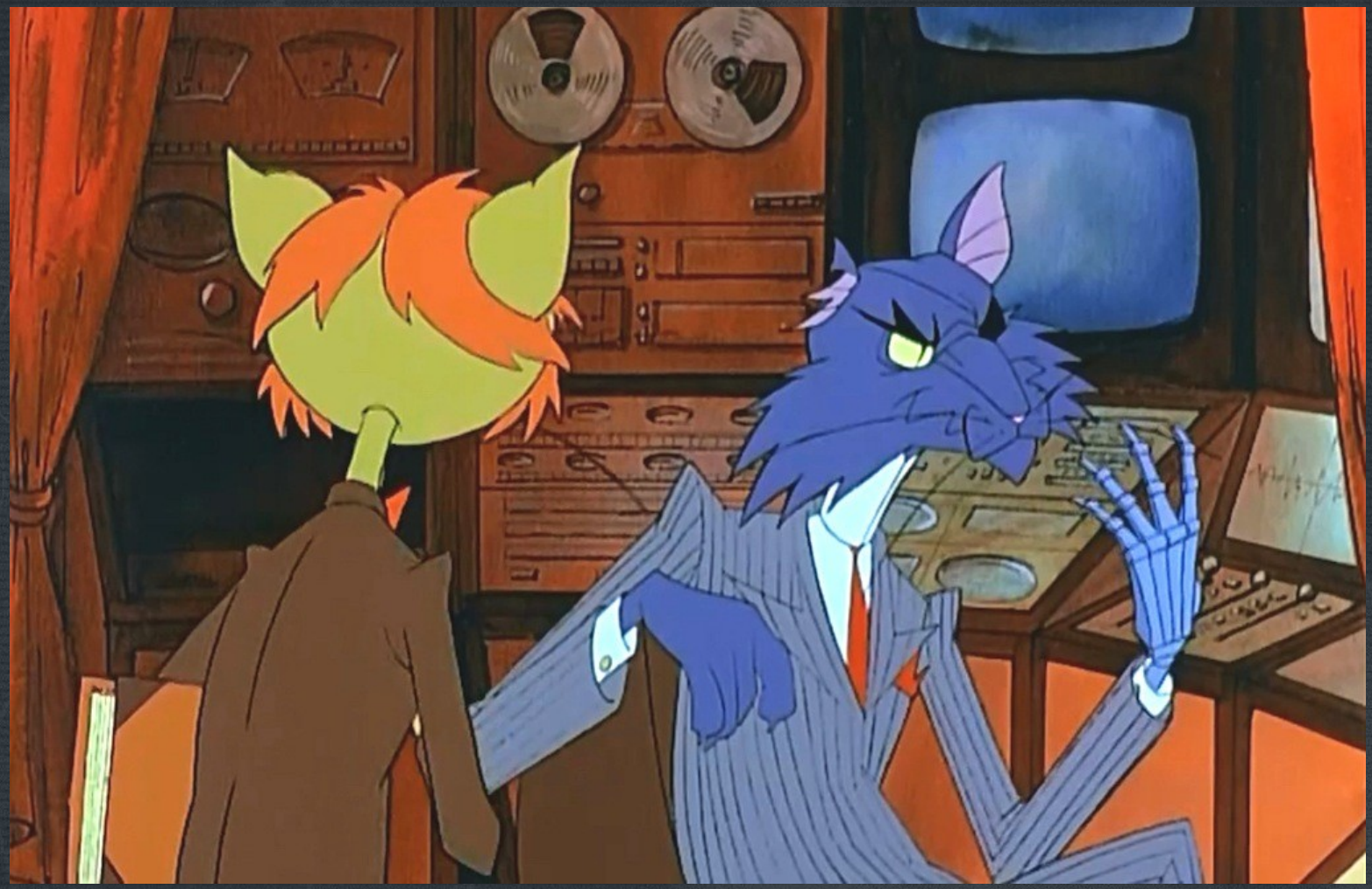
- 2013. Swansea rendőrőrs: mi az a BTC? majd FBI

- 2014. Goodson ügyvédi iroda (Észak-Karolina) csőd

- programhibás zsaroló vírusok

- 2015. Power Worm: 2 BTC (akkori 220 eHUF)

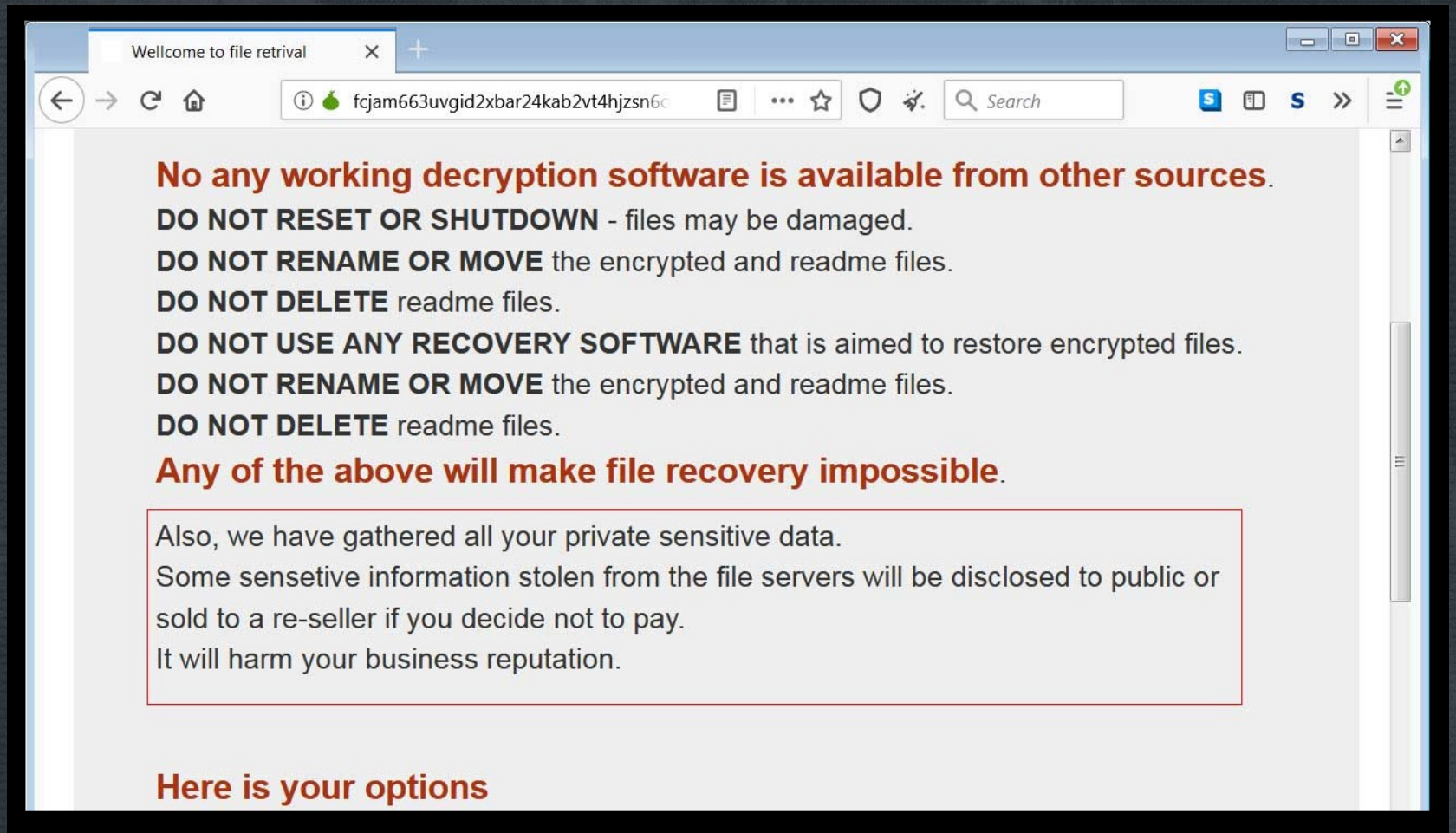
Mennyibe is került ez nekünk, Safranek?
Öööö...izé....há....öt....négy...hé... Két millió.



2021-es felmérés szerint a helyreállítás költsége átlag 10x-e a váltságdíjnak

Emelkedik a tét - Publikussá tétel, tárgyalás a GDPR háta mögött

- Doxing - néha csak blöff az adatlopás
- Nagy a látencia!
- 2020. Lockheed-Martin, SpaceX, Tesla, Boeing, Honeywell - GOTO public
- 2020. CWT Business Travel Management Company (30e PC, 2 TB adat) 4.5 mUSD



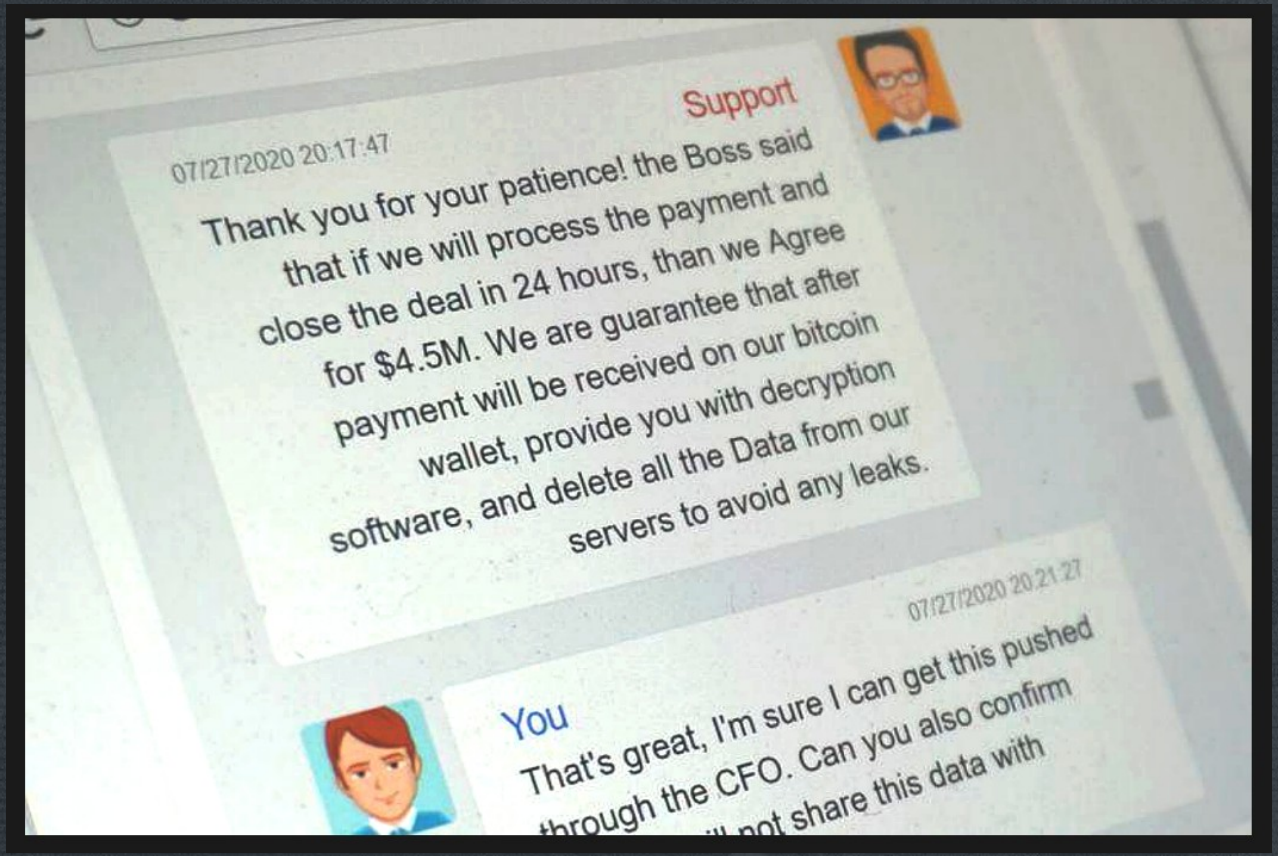
Ki kéne valamit találni, mert a végén mehetünk vissza a balettba ugrálni!

Hogy kerültünk ide:

1.) Túl sok a sebezhetőségünk
2.) Az amerikai szervezetek kezdtek fizetni - váltságdíjat fizetni illegálisnak kell(ene) lennie
3.) A kriptovaluták megkönnyítik a pénzmosást
4.) Oroszország, Kína, Irán és Észak-Korea

Biztosítás
Nem kapsz két óriási pofont, ha megmondod, hová ment az autó gazdája.

- sokszor a technikai védekezés és megelőzés helyett teszik
- kontraproduktív
- sokszor ransomware brókerek tárgyalnak (CWT)
- pl. Dr.Shifro nevű orosz "kiberbiztonsági tanácsadó cég" – valójában felhajtó

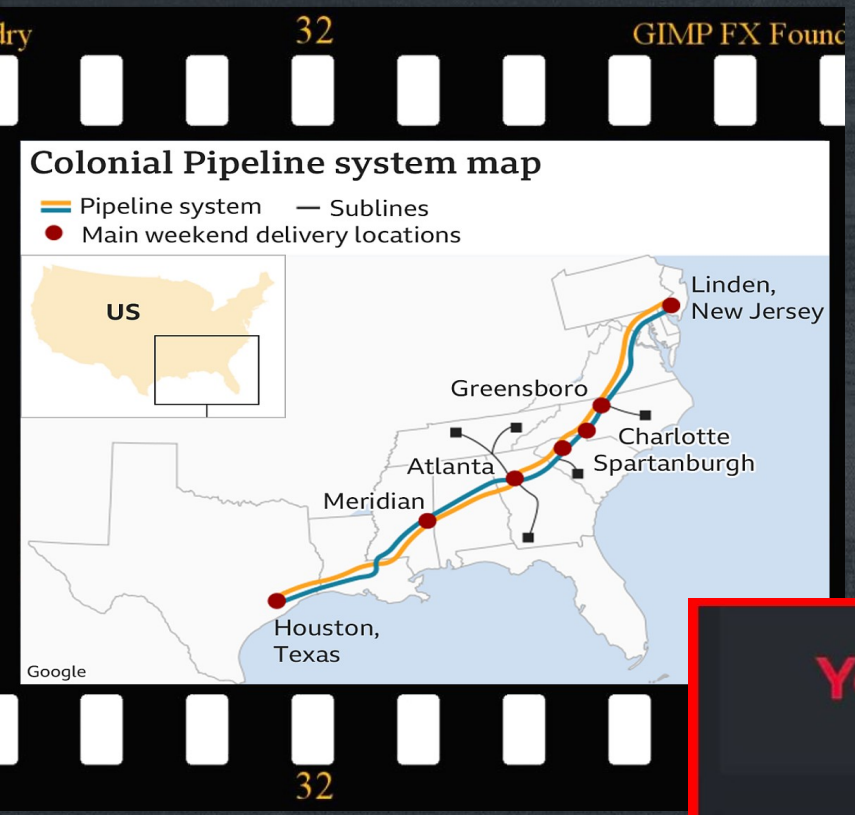


Colonial Pipeline

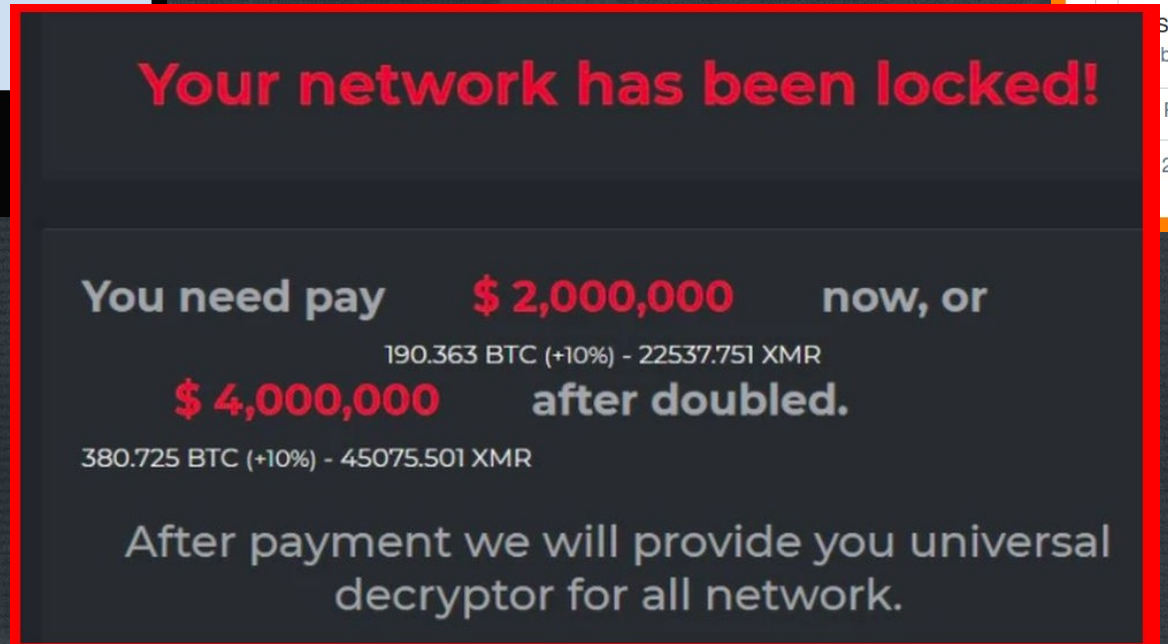
- Ede, de bedezodoroztad magad
- Mit lopsz küklopsz, gipsz klipszet lopsz küklopsz?
- Cukrozott csibecombcsontba szúrt Moszkvics kisbusz luxus slusszkulcs

Na de hogy Sodinokibibkikkikkk...!?

Valami újabb baleset, Safranek? Borotválkoztam, uram.
No, de a keze... Abban volt a borotva, uram.



Colonial Pipeline VS. DarkSide



Digitális Mohács, lépéééés iiindulj!

- Napi 100 millió gallon (kb. 378 millió liter) kapacitású olajvezeték

- a texasi Houston és New York között

- 100 GB ellopott bizalmas adat

- 4.4 millió dollár (1.27 mrd HUF)

Mellékhatások tekintetében…
Colonial Pipeline VS. Elon Musk

Forbes

Mar 24, 2021, 03:47am EDT | 102 013 views

Elon Musk Reveals Tesla Will Increase $1.5 Billion Bitcoin Holdings, Boosting The Price

Billy Bambrough Contributor
Crypto & Blockchain
I write about how bitcoin, crypto and blockchain can change the world.

Tesla TSLA +1% chief executive Elon Musk—whose tweets regularly move the bitcoin price (as well as other cryptocurrencies)—has revealed people can now buy a Tesla car with bitcoin.

The bitcoin price has soared by more than 700% over the last 12 months, taking the combined value of ... [+] COINBASE

- Bitcoinnal is lehet Teslát venni…

- árfolyam: alé hopp!

De vajon ő tudja-e, hogy mi tudjuk, hogy ő tudja, hogy mi tudjuk, hogy ő..

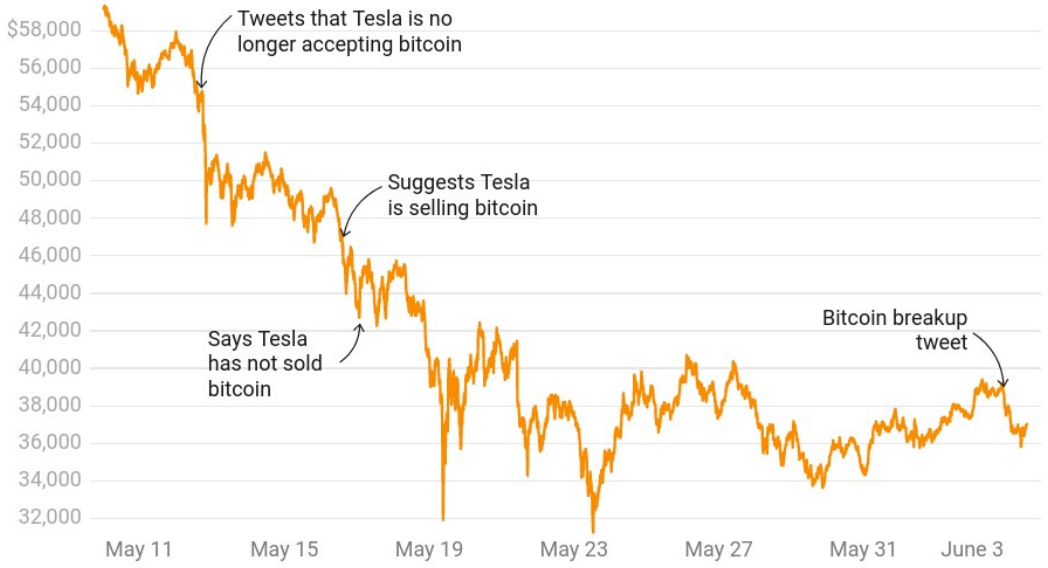
When Elon Musk tweets, crypto prices move

How Elon Musk affects bitcoin prices, in one chart.

By Rani Molla | @ranimolla | Updated Jun 4, 2021, 11:00am EDT

With a single tweet, Tesla CEO Elon Musk can move the crypto market. | Christophe Gateau/Picture

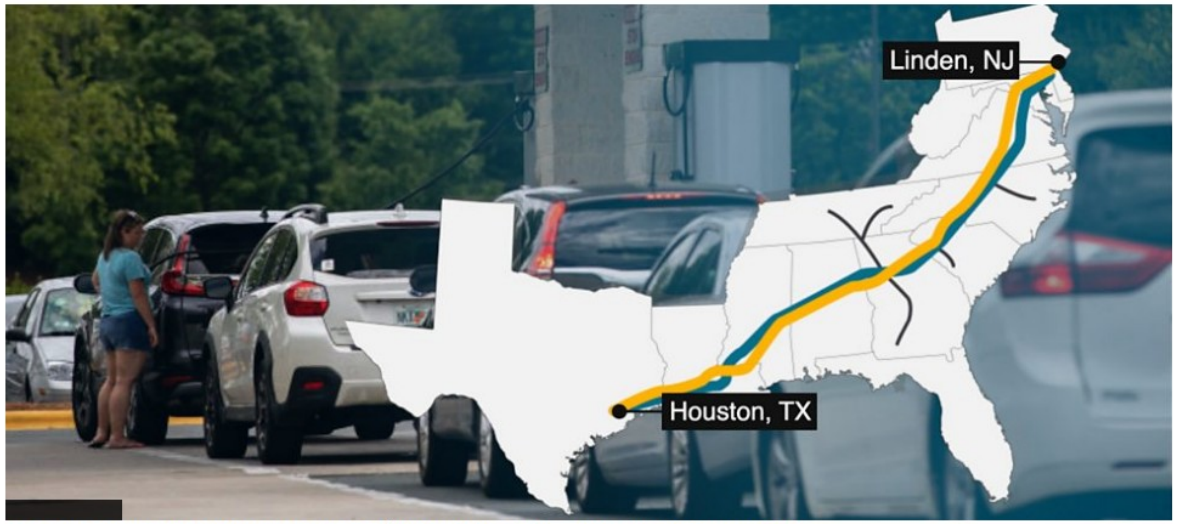
How Elon Musk's tweets have moved bitcoin prices



NEWS BBC

Home | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health

Colonial Pipeline: US recovers most of ransom, justice department says



The US has recovered most of the $4.4m (£3.1m) ransom paid to a cyber-criminal gang responsible for taking the Colonial Pipeline offline last month.

DarkSide - which US authorities said operates from eastern Europe and possibly Russia - infiltrated the pipeline last month.

- Colonial 2021.05.07-én kifizette 4.4 mUSD-t
- Bocsika, de mégsem szeretjük a Bitcoint...
- árfolyam: ajaj zsupsz...

Mi nem enni bátor egérke. Nem.
Mi csak kiszívni szép piros vérét.

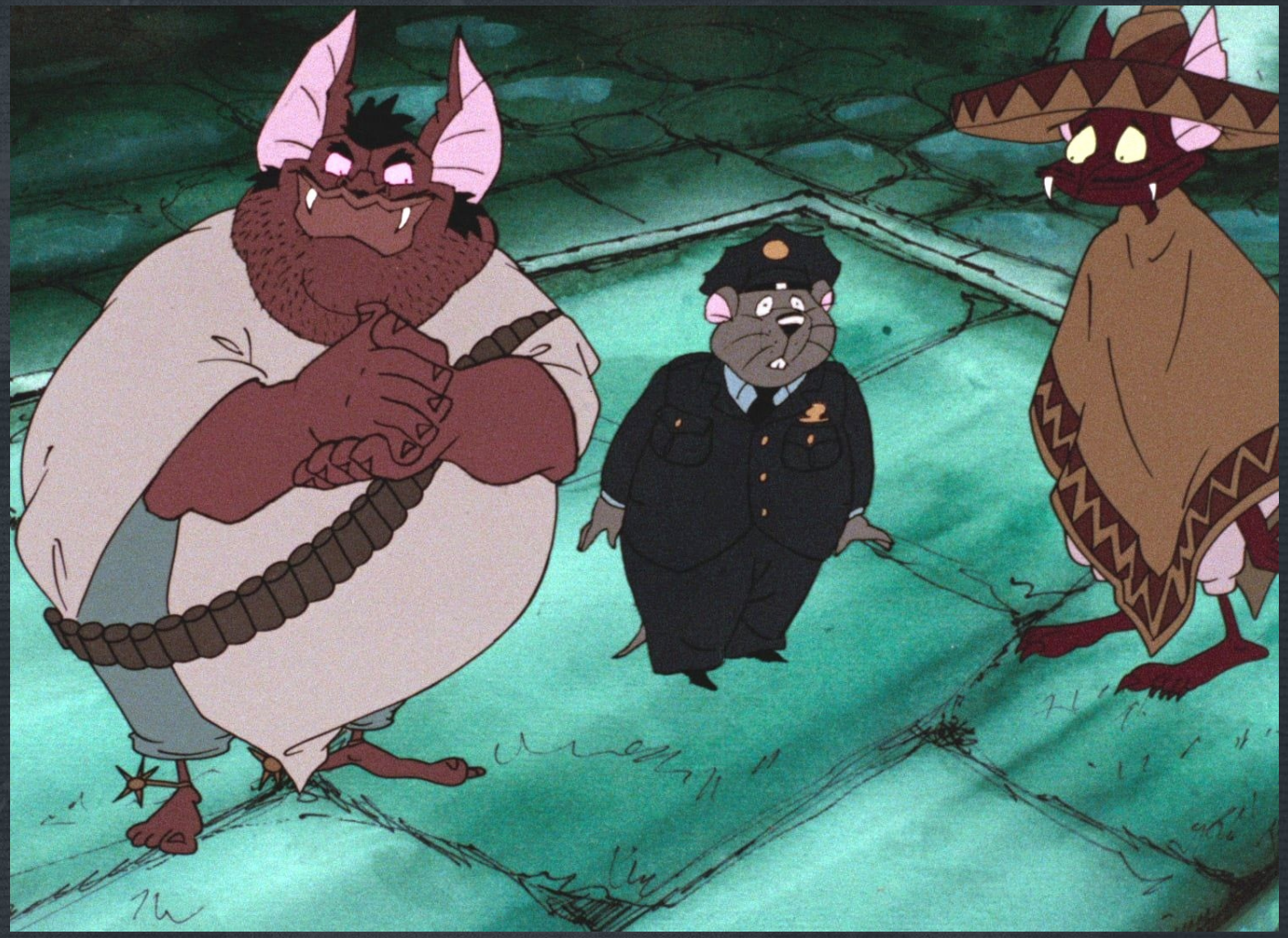
JBS VS. REvil (Ransomware Evil)

- JBS a világ egyik legnagyobb húsfeldolgozó vállalata

- világszerte több, mint 250 000 alkalmazott

- USA és ausztrál informatikai rendszerek, káosz, áruhiány

- 2021. június - 11 mUSD (3.17 mrdHUF) kriptovaluta



Nyomják meg a piros gombot, és nyugodjanak békében!

Kaseya felhőszolgáltató VS. REvil (Ransomware Evil)

- 2021. július - 70 mUSD váltságdíj

- alkudozás 50 mUSD-re univerzális kulcsért

Nagy rabló maga, öregem!
Kösz a bókot, de önt senki se múlja felül, Mr Teufel!

- 2020. a ransomware bandák 350 mUSD bevétel, +311%

- 2019. váltságdíj átlag 84 eUSD (26 mHUF)

- 2020. váltságdíj átlag 154 eUSD (46 mHUF)

Én szeretem önt, Mr. Teufel.
Helyes! A beosztott szeresse főnökét! Ez cégünk egyik alapelve...

2015. január Sailpoint felmérés

- Az elbocsátott dolgozók 14%-a 100 fontért (40 ezer HUF) eladná korábbi céges jelszavait

A robotegér a legkisebb nyíláson át is képes behatolni,
így eljuthat a legtávolabbi létesítményekig is.

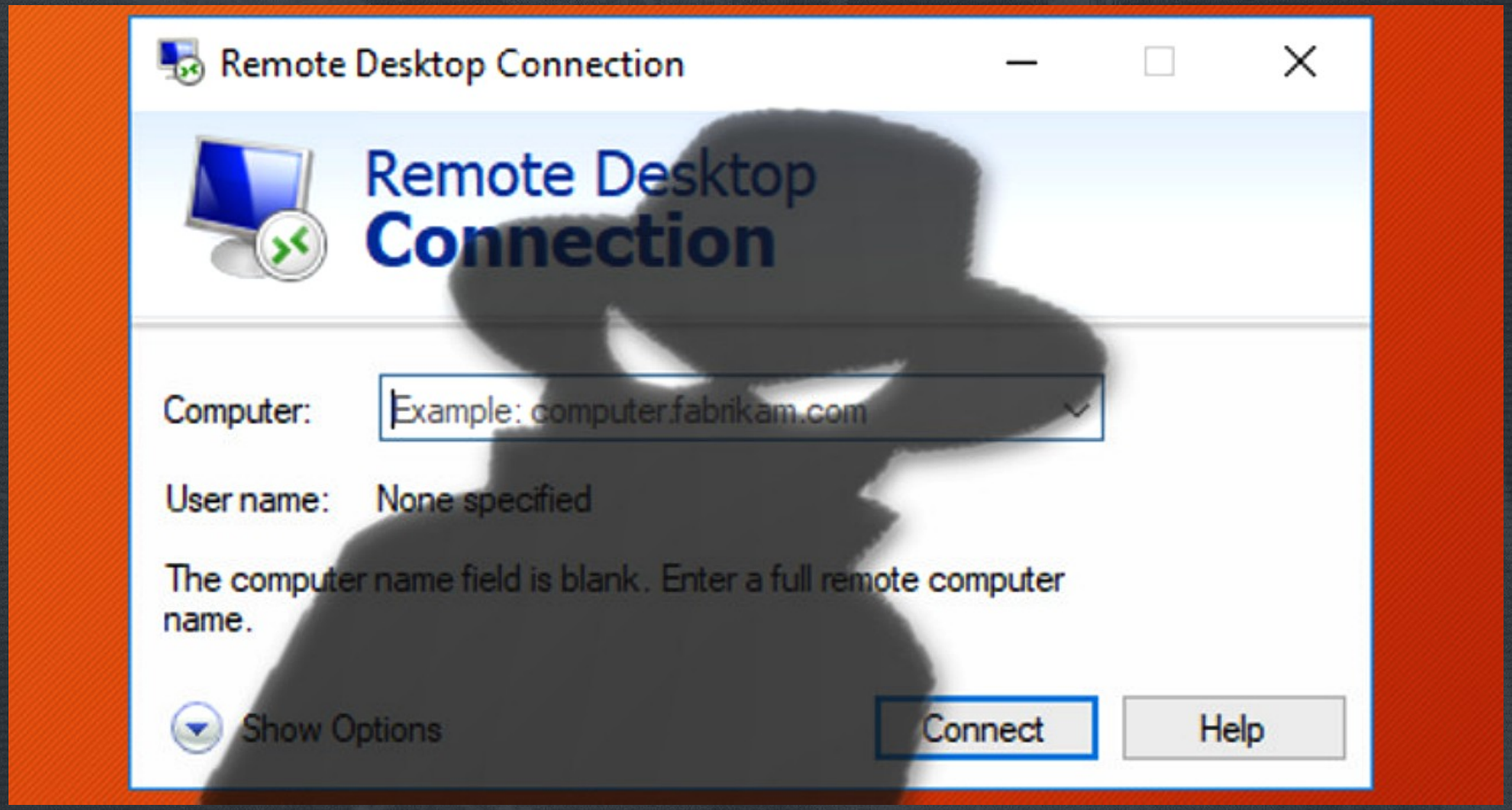
2021. augusztus

A Lockbit 2.0 kódot terjesztő banda sértett munkavállalókat, bennfenteseket toboroz

"Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc. Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID: xxxx"

Védekezés, megelőzés
Grabowski, megsebesült? Nem szokásom.

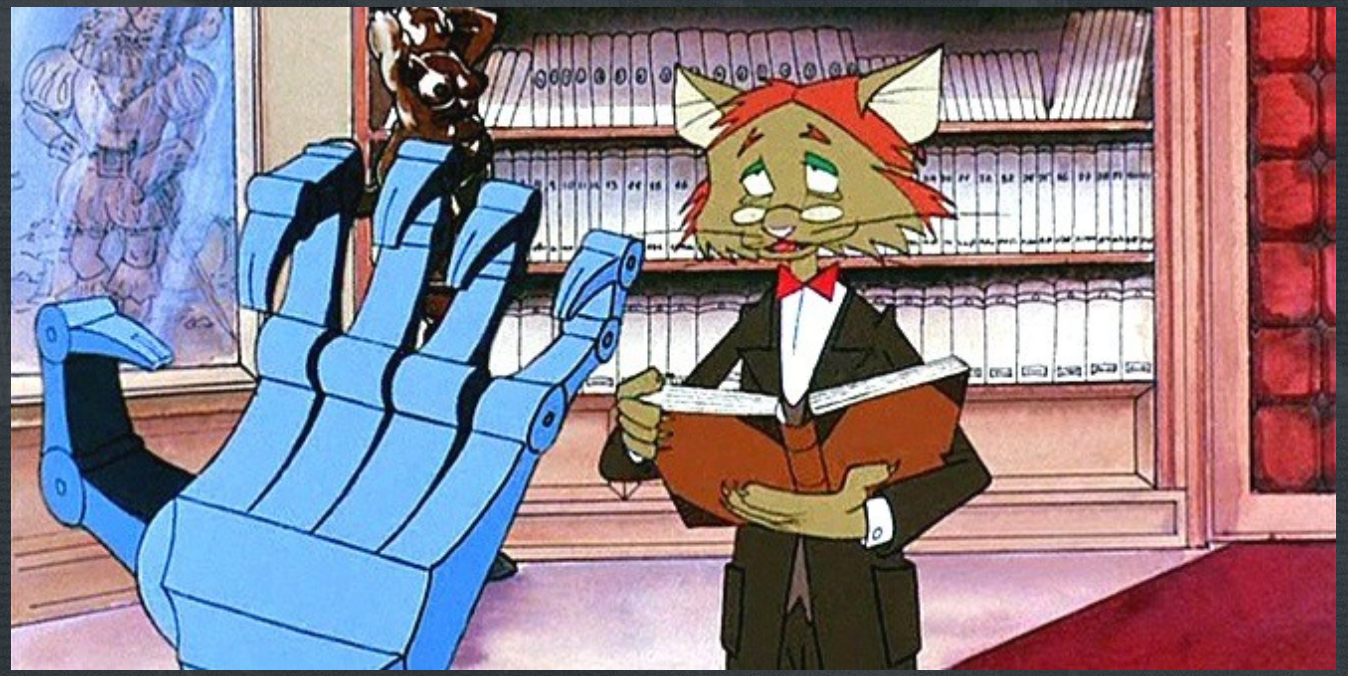
- frissítés, napi biztonsági mentés, RDP, AV, 2FA/MFA, settings, jelszavak, policy, adminisztrátori jogosultságok korlátozása, biztonságtudatosság, érzékeny adatok nyugalmi állapotban történő titkosítása, képzések, hálózatok szegmentálása, stb.



Maga melyiket választaná Safranek?
Ő... hát... khm... izé... Nem értem a kérdést Uram.

CEO és CTO támadás előtt:

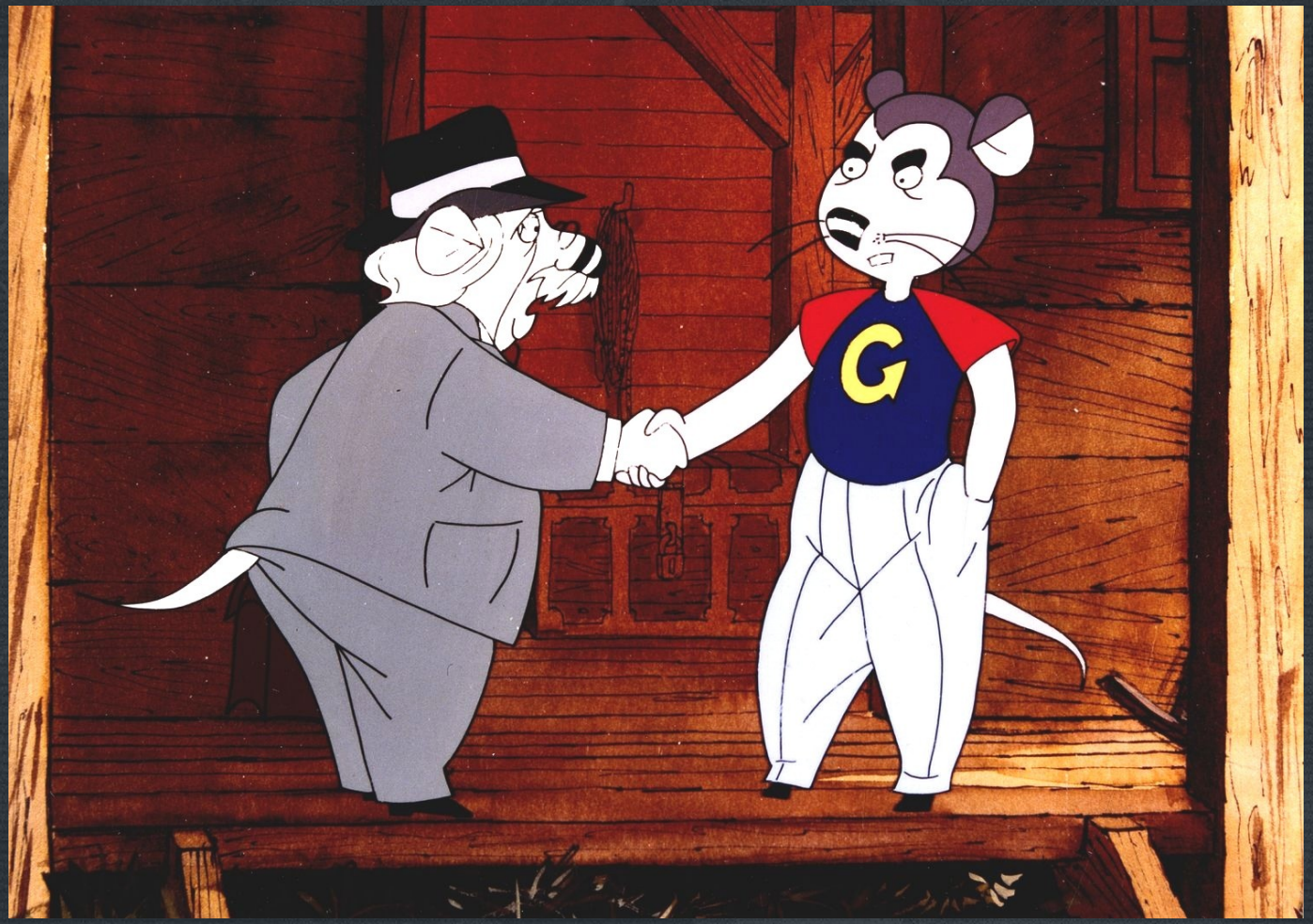
CTO: kéne 2 millió dollár a védelem erősítésére!
CEO: jó jó jó, majd a következő management board ülésen szóba hozom...



CEO és CTO támadás után:

CTO: kéne 2 millió dollár a védelem erősítésére!
CEO: tessék 200 ezer, és máskor hamarabb szólj ám, ez az egész a ti hibátok!

Köszönöm a figyelmet!



info@sicontact.hu