CYBERSECURITY
EXPERTS ON YOUR SIDE

2021. április 13.

RANSOMWAREK HÁBORÚJA

Csizmazia-Darab István
IT biztonsági szakértő, ESET/Sicontact

csizmazia-darab.istvan@sicontact.hu

"A Sötét oldal nem erősebb, csak simább, könnyebben járható."

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


Színre lép az Erő sötét oldala

2013. Cryptolocker

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

Az Erő sötét oldalának hatalmát használva

- erős, egyedi titkosítás: 1024, 2048 RSA kulcs

- később még erősebb ECC (Elliptical Curve Cryptography)

- C&C szerver rejtett TOR hálózat

- "lenyomozhatatlan" Bitcoin

- kevés az univerzális helyreállító, pl. AV letöltési oldalakon

- gyűjtemény:
  https://www.getcryptostopper.com/ransomware-decryptors/

"Nemcsak elhivatottságra van itt szükség, de hideg fejre is."

- Kivel kötünk üzletet? Grál lovag VS bűnöző. Vajon kapunk feloldókulcsot?

- FBI állásfoglalás

- tudunk-e tárgyalni, alkudni?

Célkeresztben - akikre a legtöbbször lőnek

- kórházak, állami intézmények, hivatalok

- COVID alatt tesztközpontok, kutatóintézetek, gyógyszeripar

"Gyengeségeidből okulhatsz a legtöbbet"

Lúzerek, Darwin díjasok

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

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

- "Tedd vagy ne tedd, de ne próbáld!"

- programhibás zsaroló vírusok

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

"Vannak helyek, amiket a sötét oldal hosszú ideje tartó jelenléte áthat"

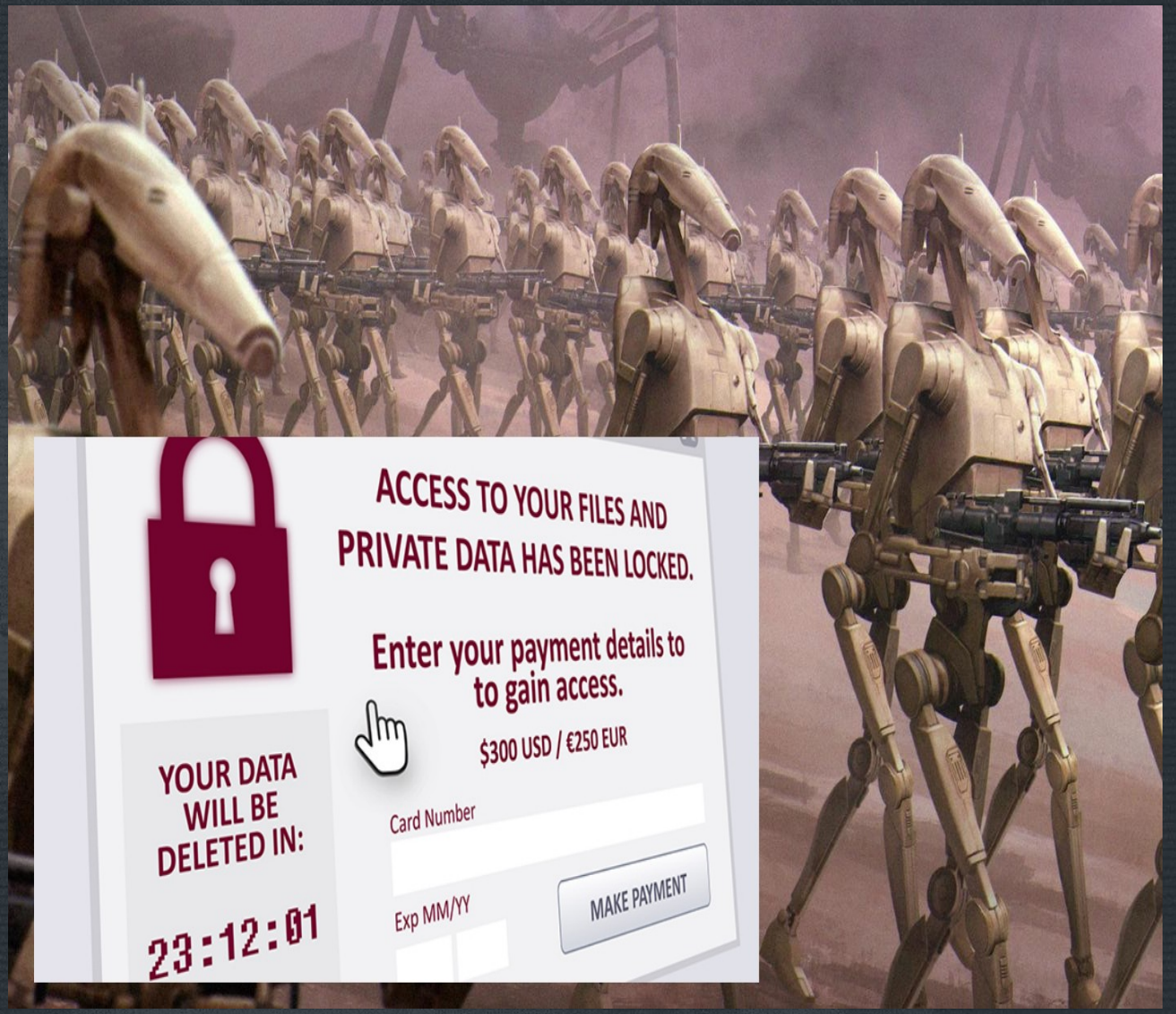
2015. SamSam "vállalati" zsarolóvírus

- sok előkészítő észrevétlen felderítő munka

- tökéletes időzítés pl. támadás hétvégén, ünnepeken, zsarolás az év végi hajrában

- egyedi "testre szabott" váltságdíj helyreállítási költségnél kevesebb, a céges nyereséghez igazodó

- folyamatosan új exploitok beépítése



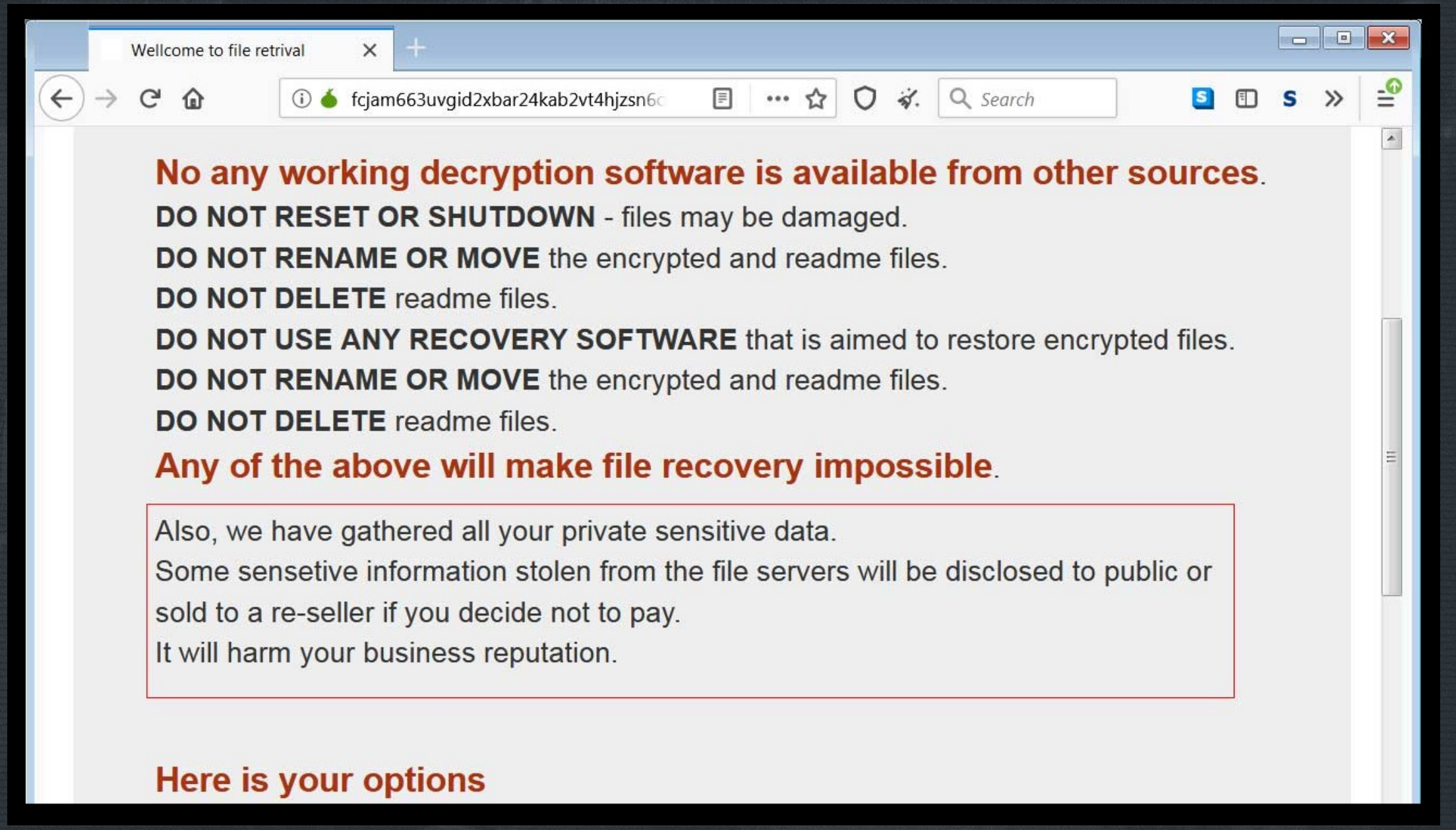
"Szétroppantottam a Galaxis gerincét…
Néha szét kell roppantani valamit, hogy újjáépíthessük."

- 2018. két iráni gyanúsított letartóztatása

- summa 6m USD (19mrd HUF) váltságdíj, 30 mUSD okozott kár

- később új szereplők: Ryuk, RagnarLocker, BitPaymer, MegaCortex

Sith elmetrükk - Emelkedik a tét



Publikussá tétel, tárgyalás a GDPR háta mögött

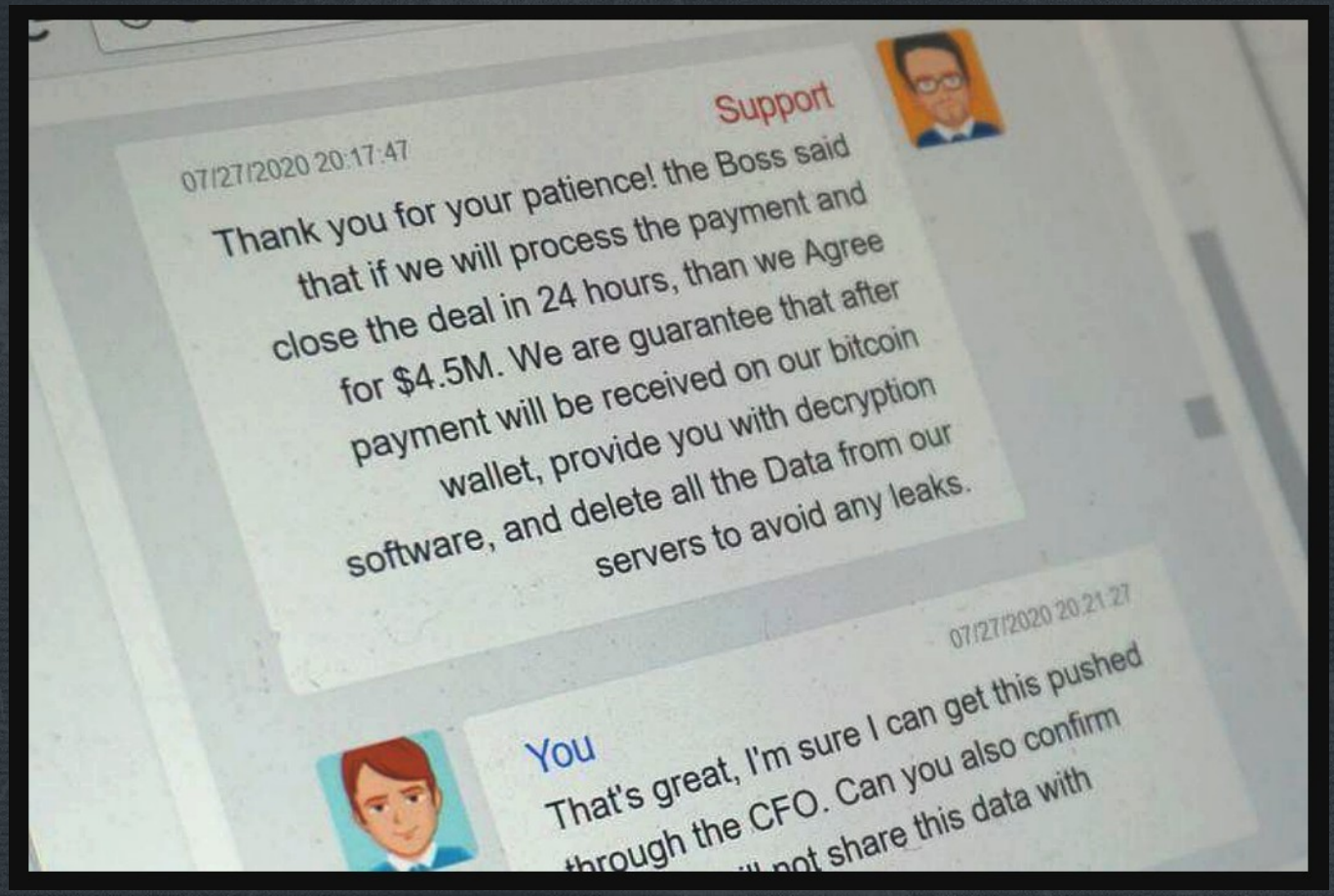
- néha csak blöff az adatlopás

- 2020. Lockheed-Martin, SpaceX, Tesla, Boeing, Honeywell - GOTO public

- 2020. CWT Business Travel Management Company (30e PC, 2 TB adat) 4.5 mUSD

"Nem ezek azok a droidok, amiket keresnek."

Biztosítás, biztonság?

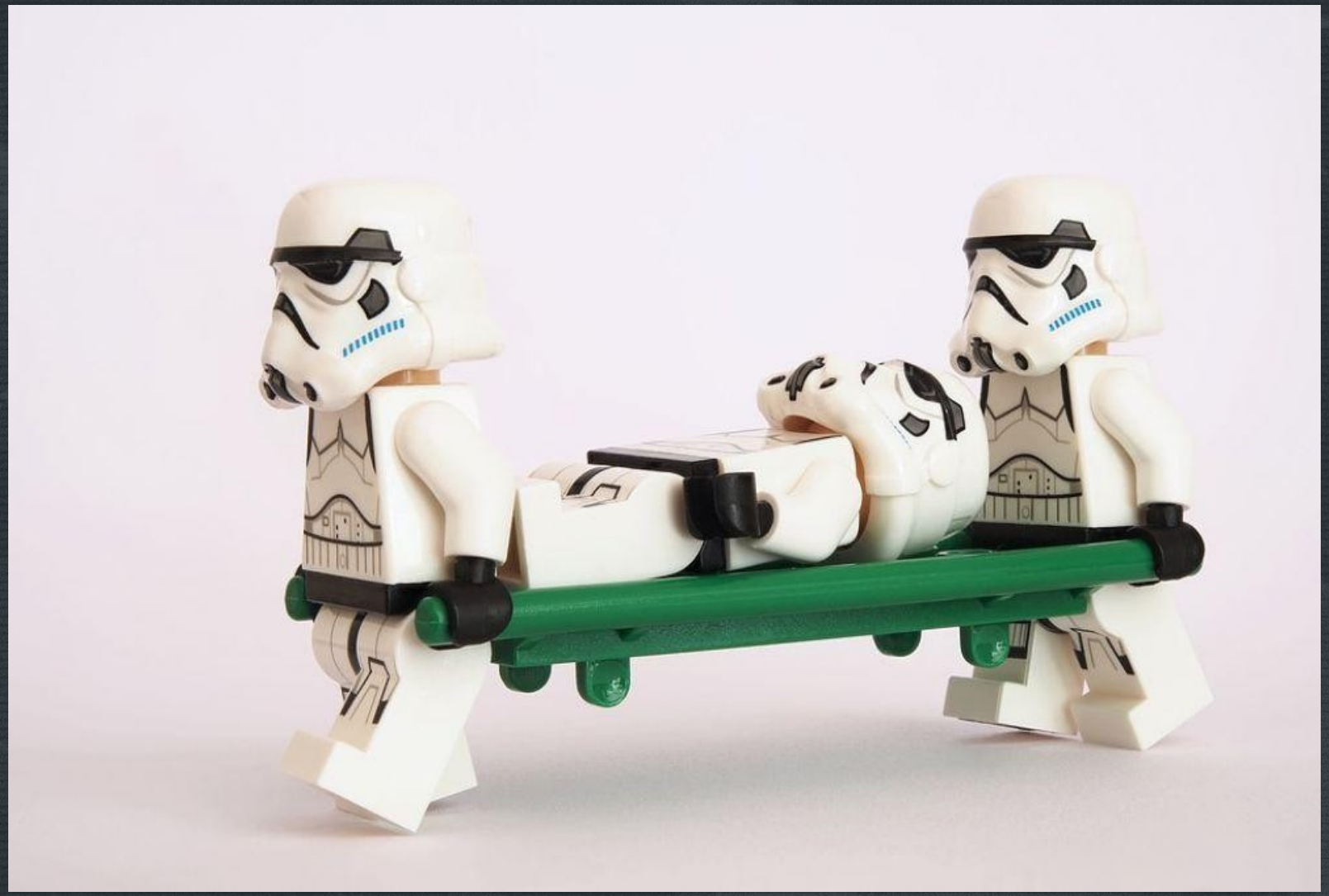


- sokszor a technikai védekezés és megelőzés helyett teszik, kontraproduktív

- ransomware brókerek a Jedik és a Sötét oldal szolgálatában

- pl. Dr.Shifro nevű orosz "kiberbiztonsági tanácsadó cég”

Mibe fáj nekünk mindez?



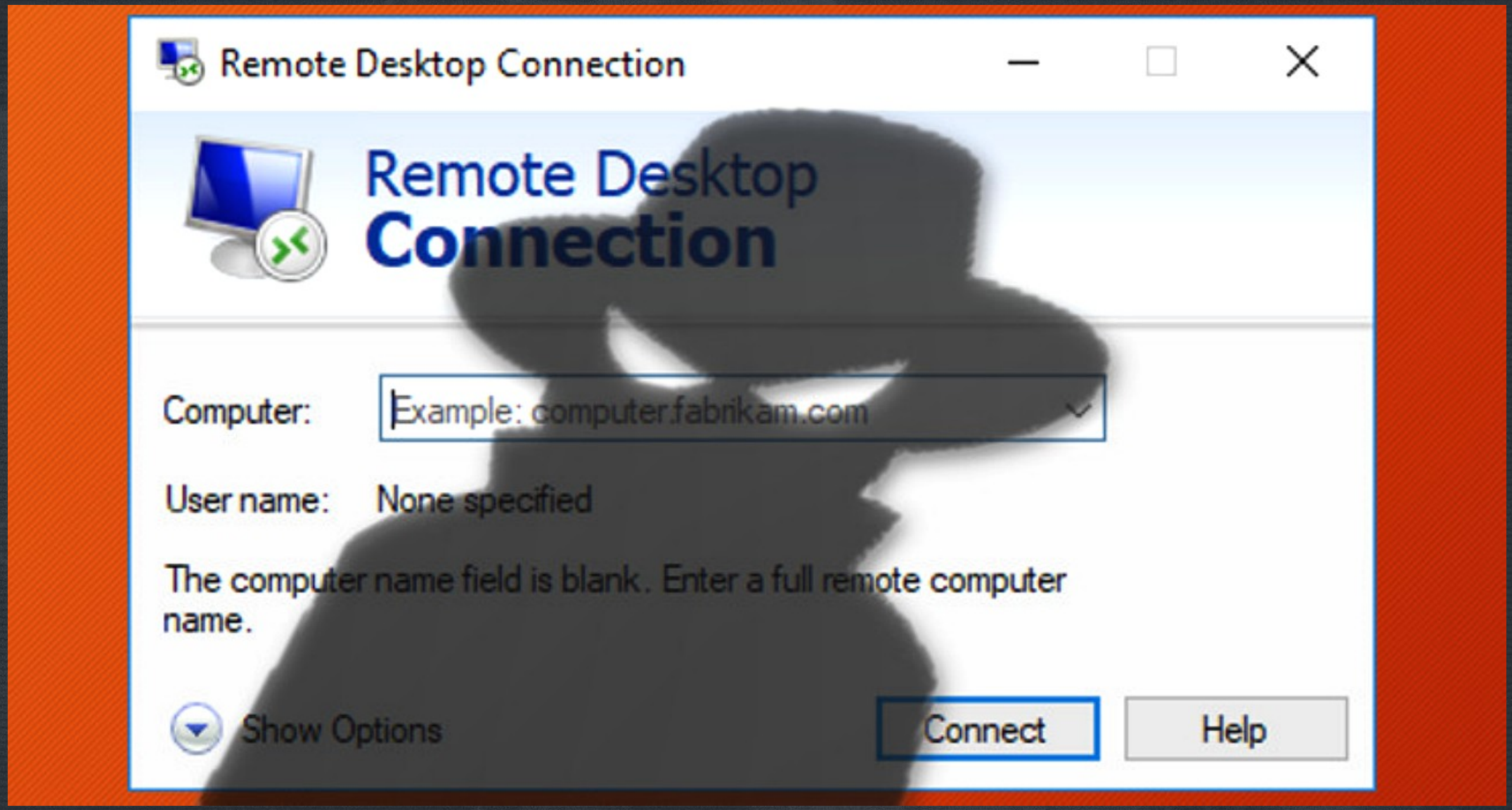
"Soha nem szabad lebecsülni az Erőt, nagy hatalma van"

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

- 2019. váltságdíj átlag 84 eUSD (26 mHUF)

- 2020. váltságdíj átlag 154 eUSD (46 mHUF)

"A félelem tudata megóvhat, ha nem nő túl rajtad."



Az Erő legyen velünk

- Védekezés, megelőzés
- frissítések
- mentések
- RDP és egyéb settings
- AV
- jelszavak, MFA/2FA
- policy
- biztonságtudatosság

Köszönöm a figyelmet!