HTE
KIBERSZABÁLYOZÁSI
MINIKONFERENCIA
2024. március 19. | Budapest

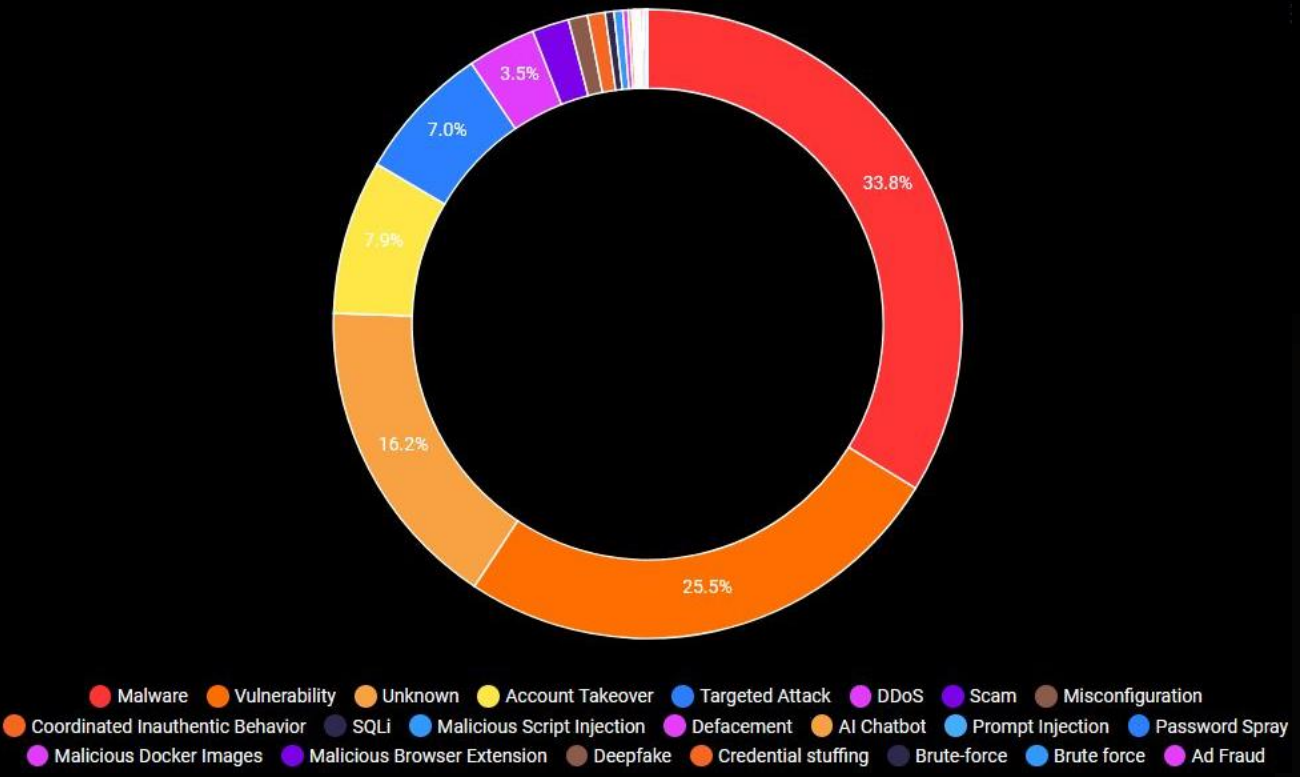
HTE 75 ÉV
1949-2024

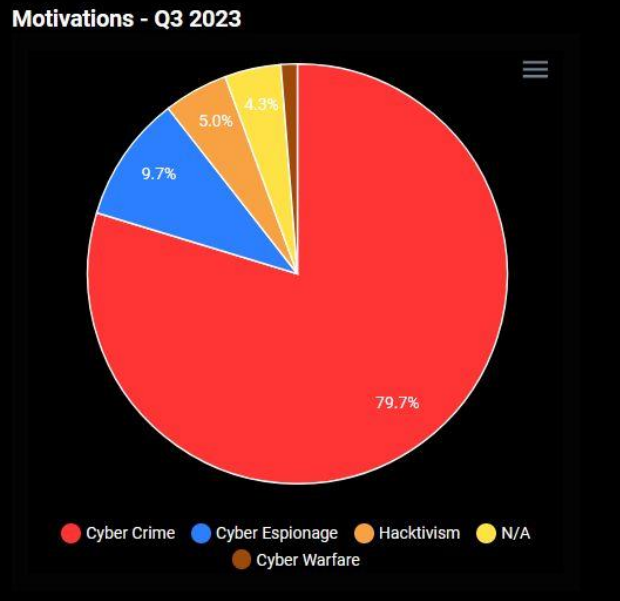
Incidenskezelési esettanulmányok a SWAT életéből

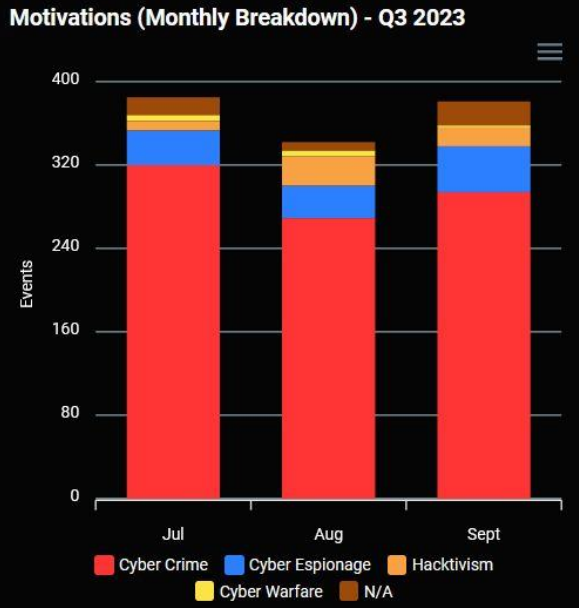
… azaz miért van szükség biztonsági minimumokra

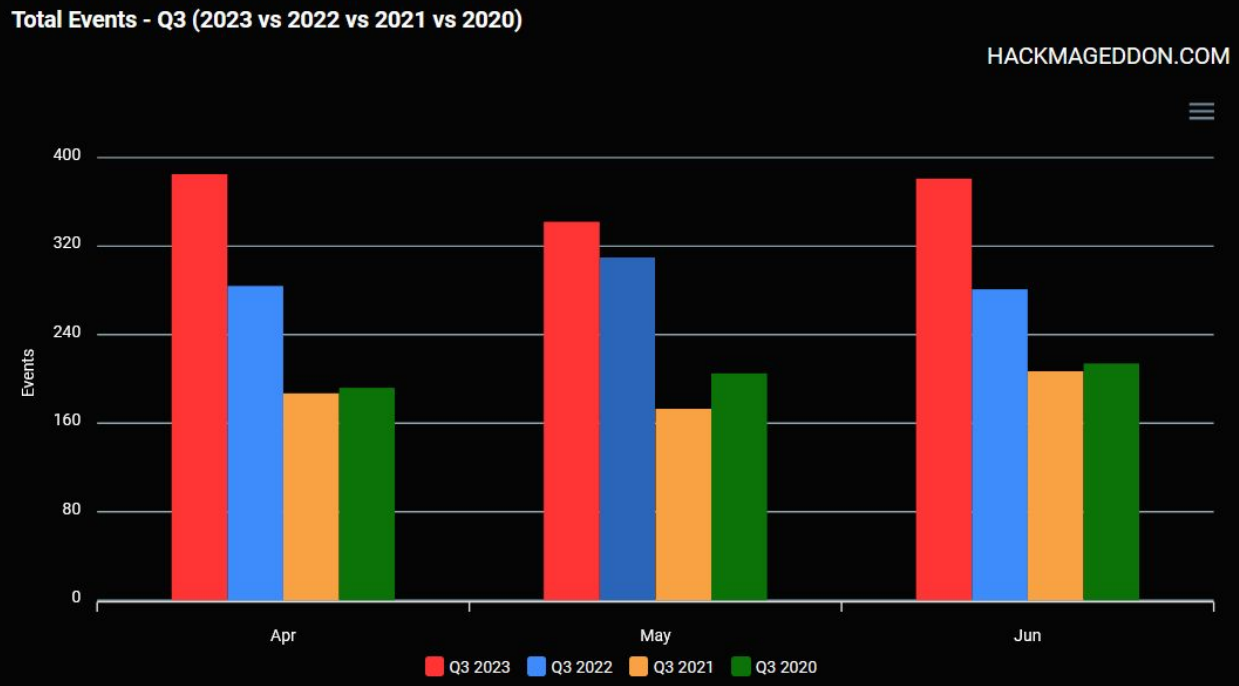
1,108
EVENTS

12.18
EVENTS/DAY









CTRL

CYBER THREAT RESILIENCE TEAM BY T

Legfőbb fenyegetettségek

Zsarolóvírusok

- Lopás, titkosítás, DDoS és nyomásgyakorlás
- RaaS

Account takeover

Business e-mail compromise

DDoS

Támadás felhőben lévő végpontok ellen

SWAT – Security Weapons And Tactics

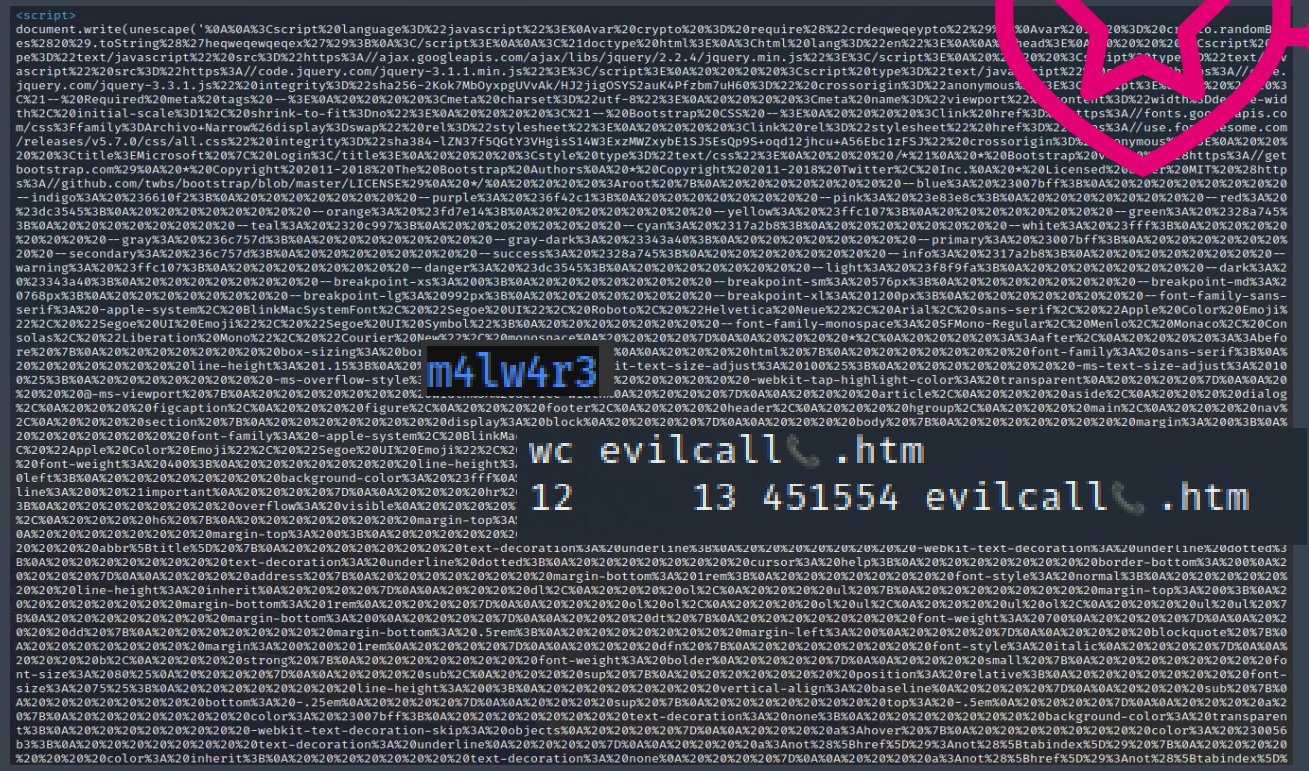
Gyors, hatékony és eredményes reagálás a krízist okozó kibertámadásokra

Biztonsági és infrastruktrális szakértelem teljes Telekom-TRI tudással

Akár kommunikációs, compliance tanácsadás, túsztárgyalás...

Konstrukciók:

- Eseti segítség krízishelyzet kezelésében
- Havidíjas konstrukció

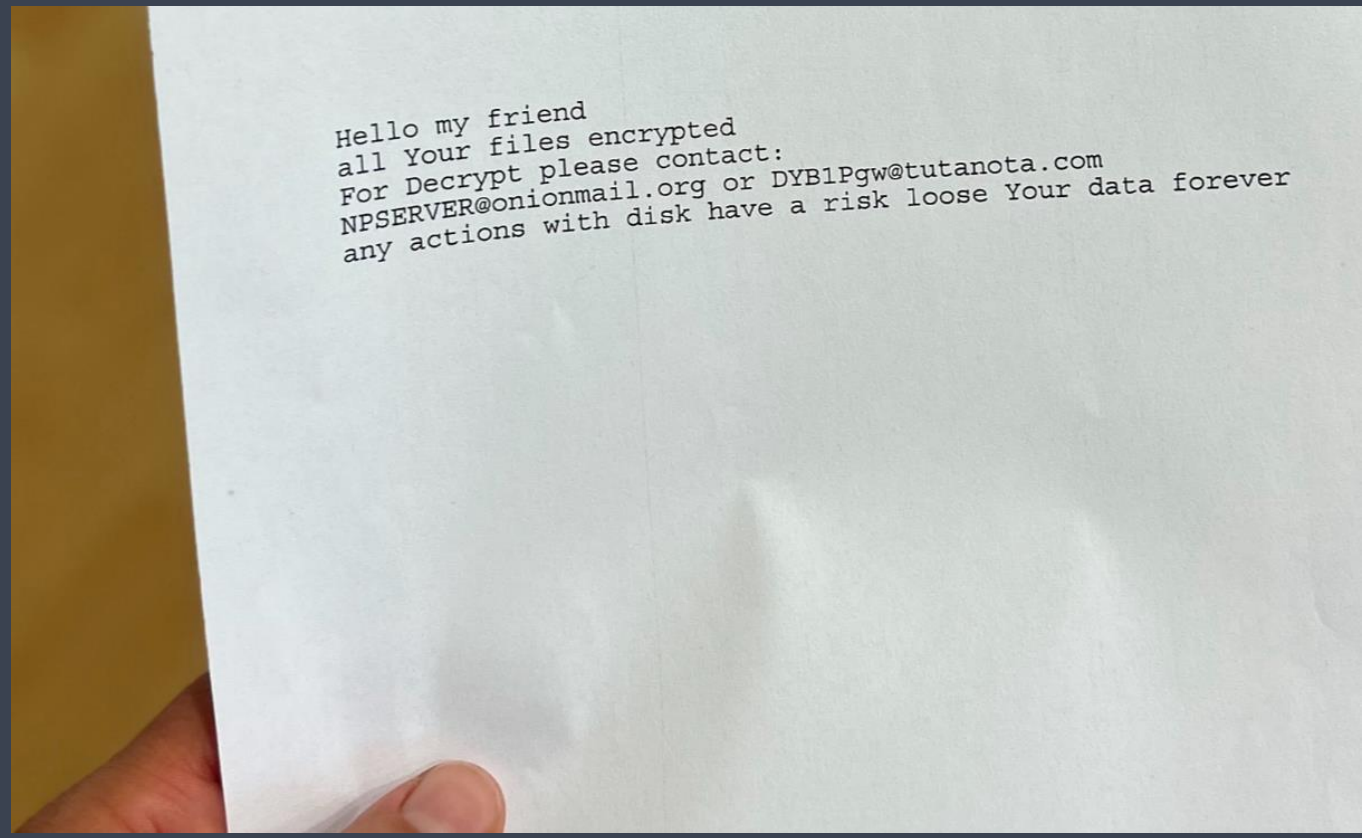


HOTLINE: +36 (1) 48 19 911

CTRL CYBER THREAT RESILIENCE TEAM BY T

Tipikus ransomware támadás

- Éjszakai ügyeletes bejelentése bizonyos szolgáltatások elérhetetlenné válásáról
- Másnap reggel ransom note-ok a nyomtatókban és a munkaállomásokon
- Minden titkosítva
- A mentés elérhetetlen
- Zsarolás + DDoS
- Adatok publikálása



A támadás mögött

Szinte minden esetben e-mail + PDF vagy link

Automatizált kódok

Sérülékenységek kihasználása

Magasabb jogosultságok szerzése

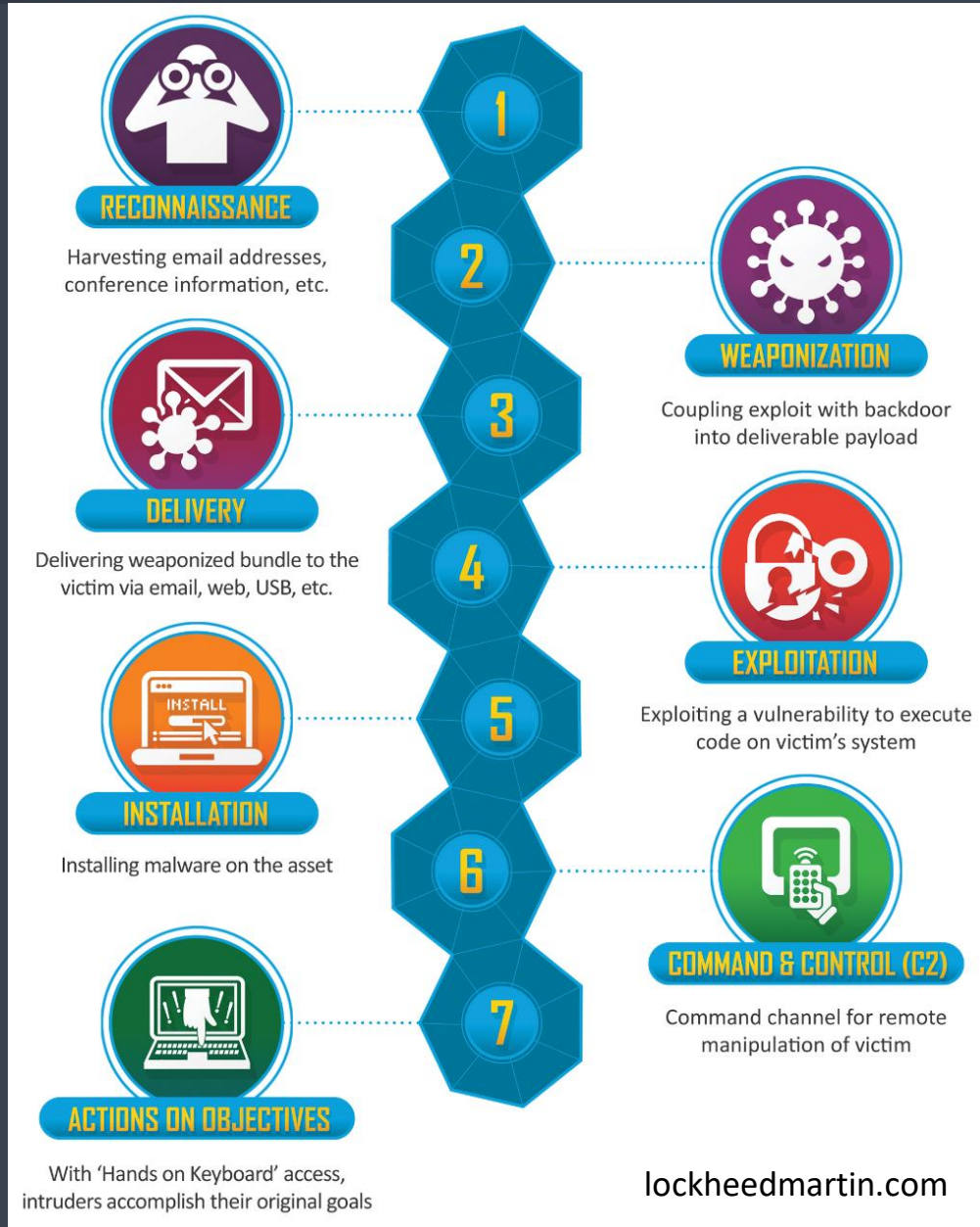
Lokális terjeszkedés

- Mentés
- Virtualizáció
- AD
- Backdoor-ok

Adatszivárogtatás

Titkosítás

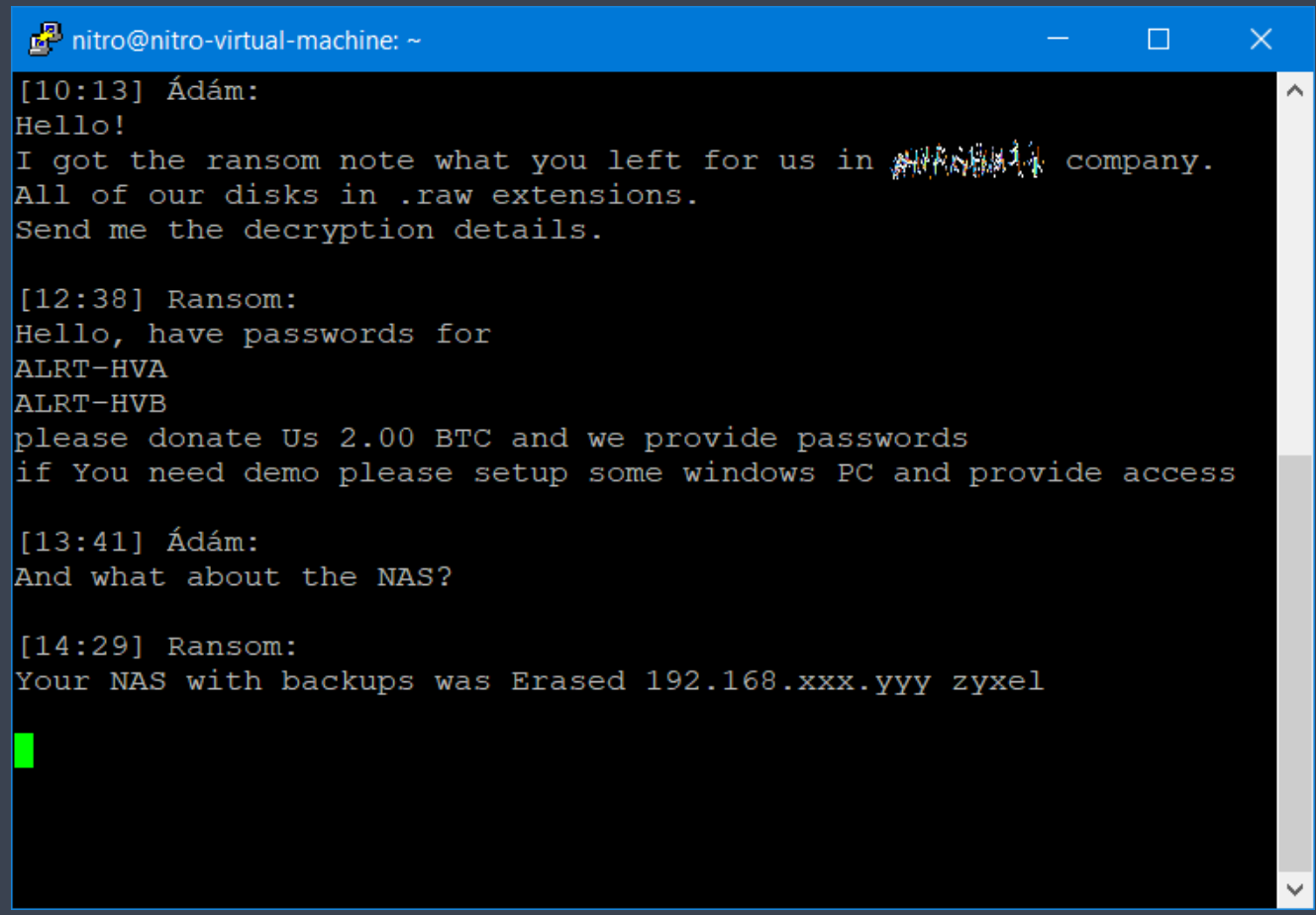
CTRL CYBER THREAT RESILIENCE TEAM BY T



lockheedmartin.com

Tipikus hiányosságok

- Biztonságtudatossági hiányosságok
- Szegmentációs hiányosságok
- Sérülékenységek
- Védelmi rétegek hiánya
- Hardening hiánya
- MFA hiánya
- Jogosultságok kezelése
- Ransomware-proof mentés hiánya
- DR folyamat hiánya
- Nincs biztonsági monitoring



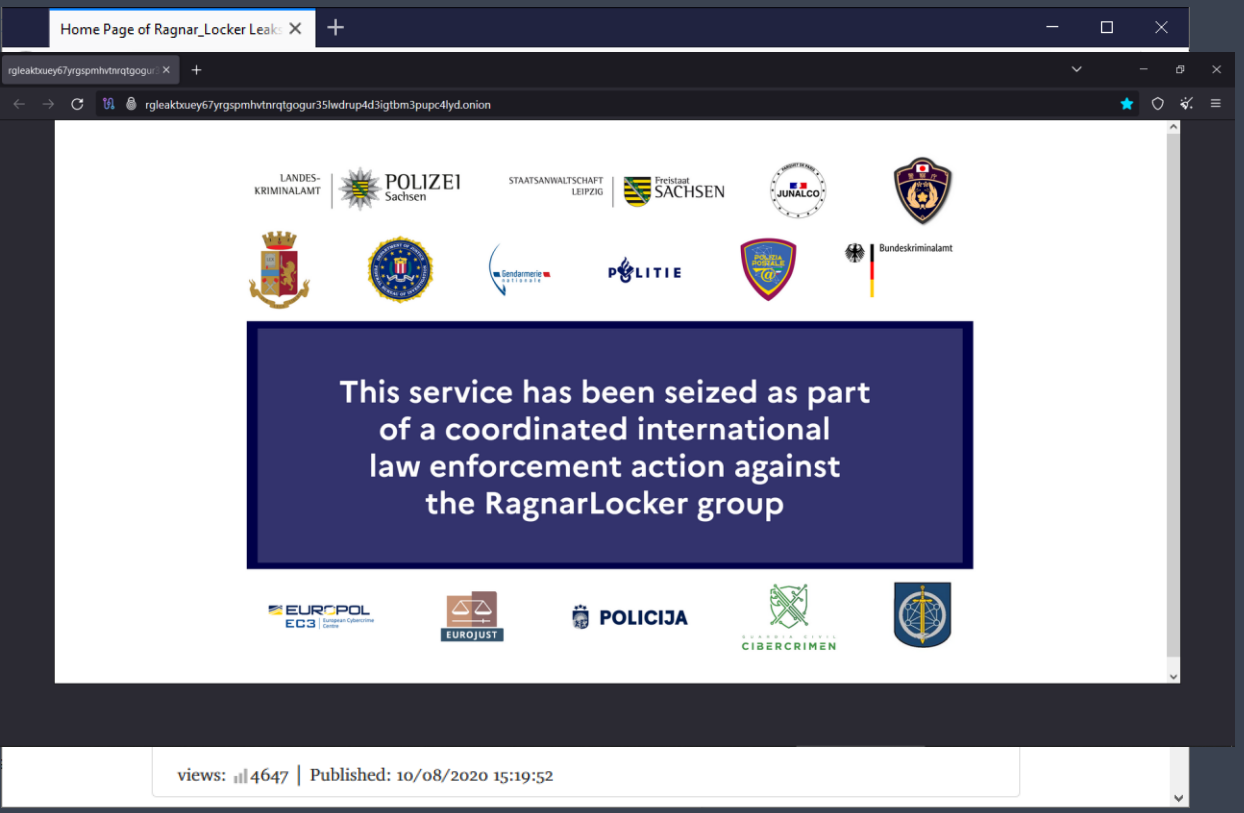
CTRL CYBER THREAT RESILIENCE TEAM BY T

Általános szolgáltatástartalom ransomware esetében

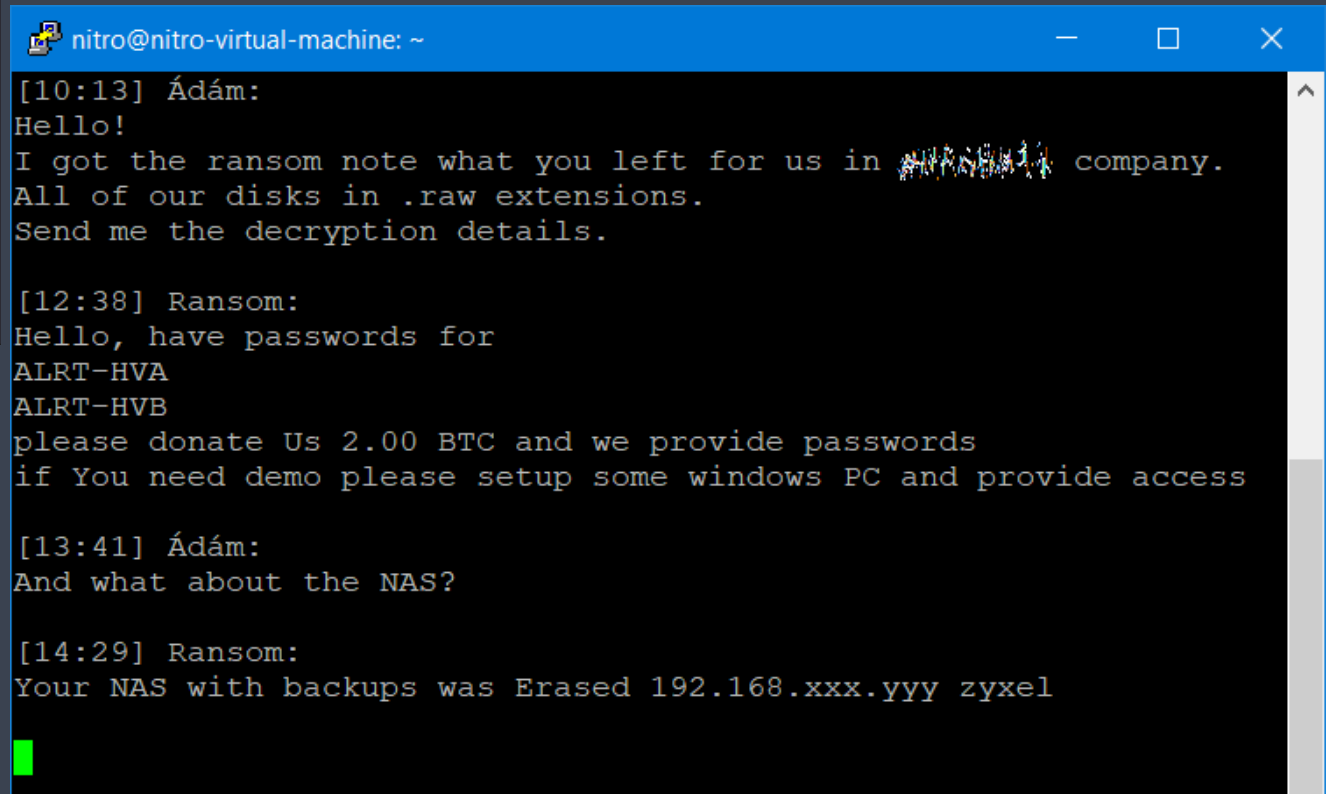
- Felmérés
  - Okozott károk
  - Környezet
  - Üzleti igények
- Forensics
  - Támadás módja
  - Ransom beazonosítása
  - Idővonal
- Visszaállítás támogatása
  - Tervezés támogatása
  - Biztonsági ellenőrzés
  - Technológiai eszközök
- GAP-ek és sérülékenységek felmérése
- Post-mortem riport és fejlesztési javaslatok

CTRL CYBER THREAT RESILIENCE TEAM BY T

A sikerek – néhány példa sikeres visszaállásra



- NAS-on lévő mentés visszaállítása
- Részleges migráció
- Fejlesztői / UAT környezet
- Decrypter

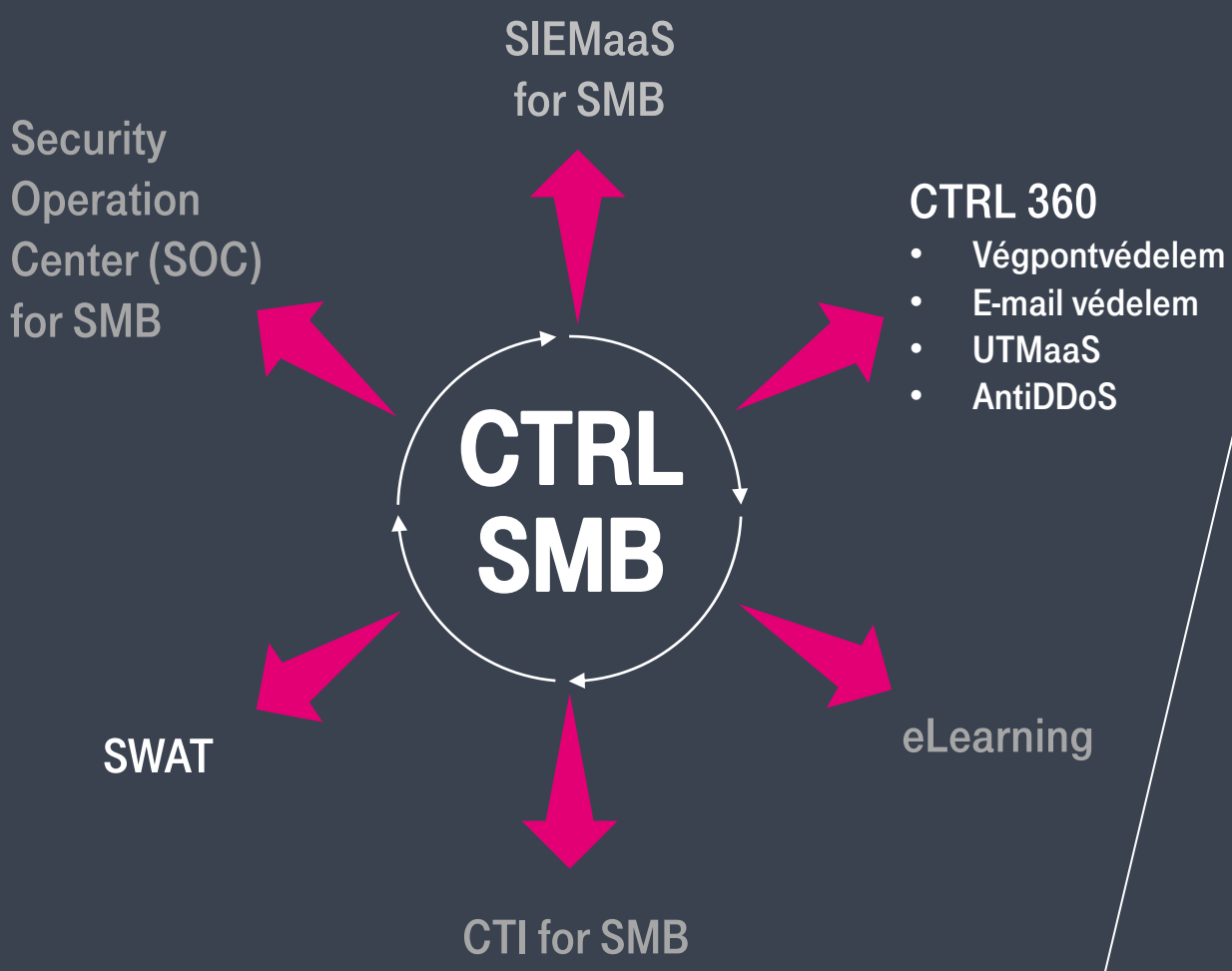


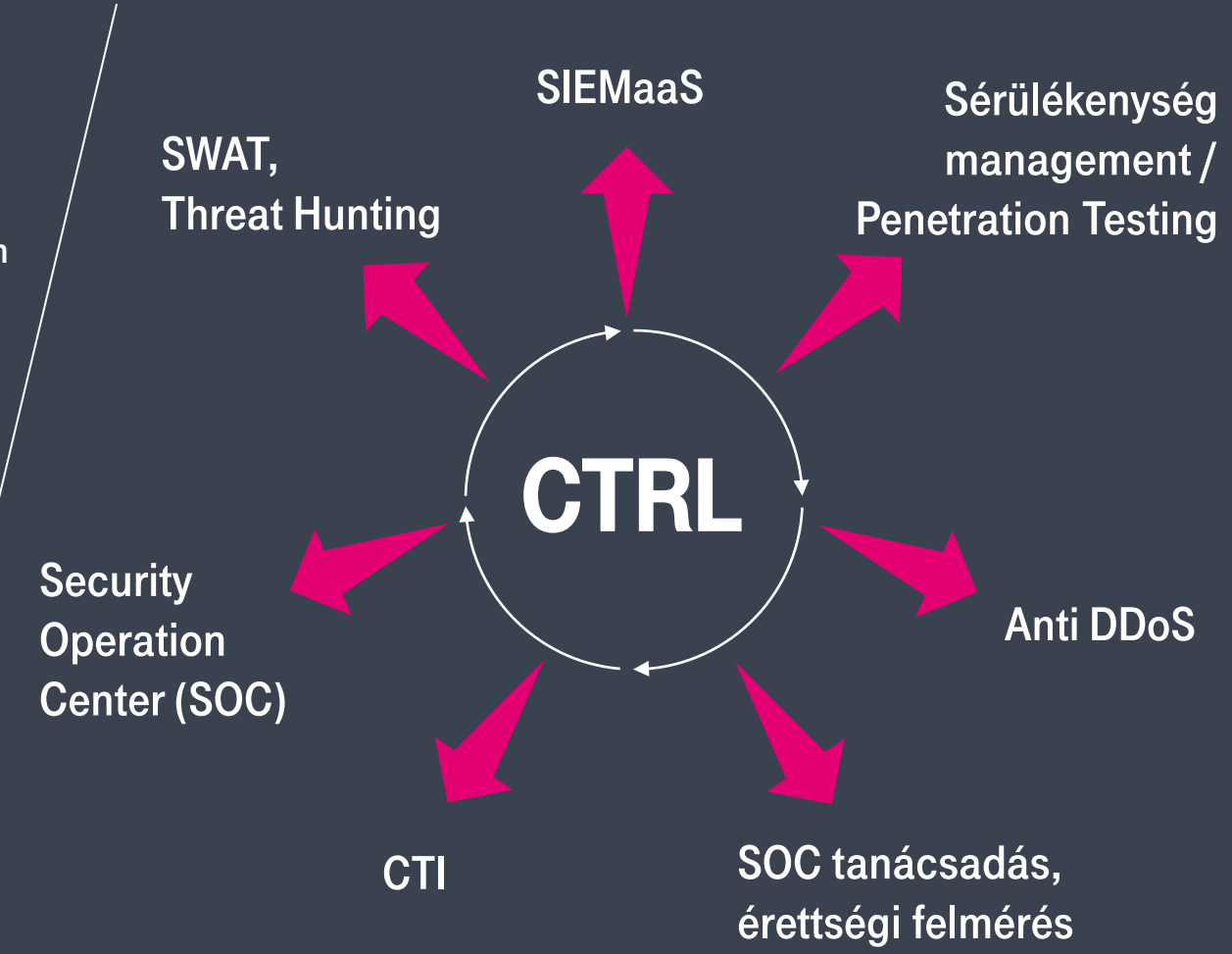
CTRL CYBER THREAT RESILIENCE TEAM BY T

Köszönöm a figyelmet

hlavaty.gyozo@telekom.hu

Cybersecurity services





CTRL CYBER THREAT RESILIENCE TEAM BY T