

HTE
KIBERSZABÁLYOZÁSI
MINIKONFERENCIA
2024. március 19. | Budapest

HTE75
ÉV
1949-2024



Incidenskezelési esettanulmányok a SWAT életéből

... azaz miért van szükség biztonsági minimumokra

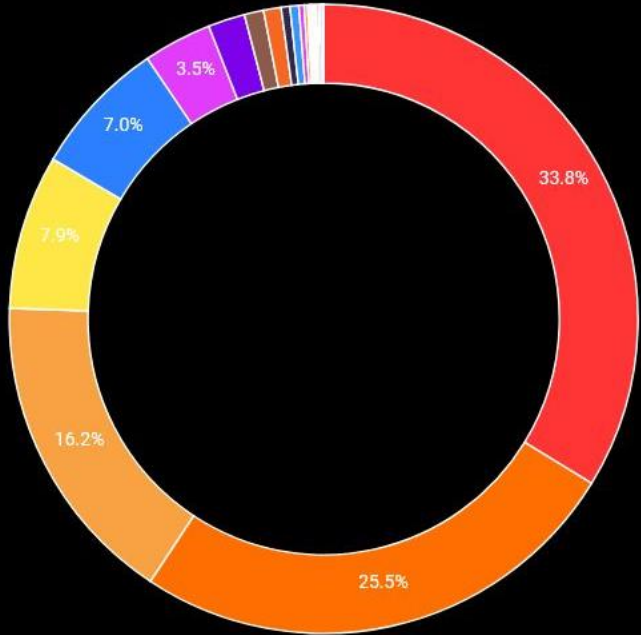


1,108

EVENTS

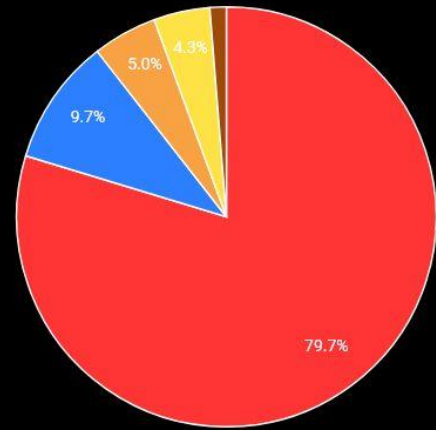
12.18

EVENTS/DAY



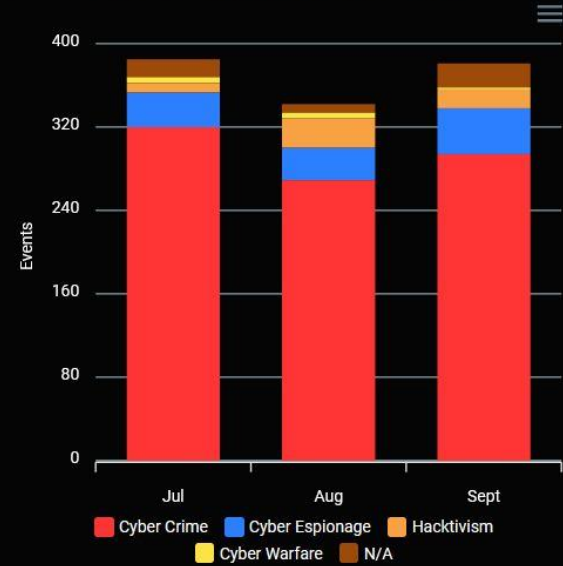
- Malware
- Vulnerability
- Unknown
- Account Takeover
- Targeted Attack
- DDoS
- Scam
- Misconfiguration
- Coordinated Inauthentic Behavior
- SQLi
- Malicious Script Injection
- Defacement
- AI Chatbot
- Prompt Injection
- Password Spray
- Malicious Docker Images
- Malicious Browser Extension
- Deepfake
- Credential stuffing
- Brute-force
- Brute force
- Ad Fraud

Motivations - Q3 2023

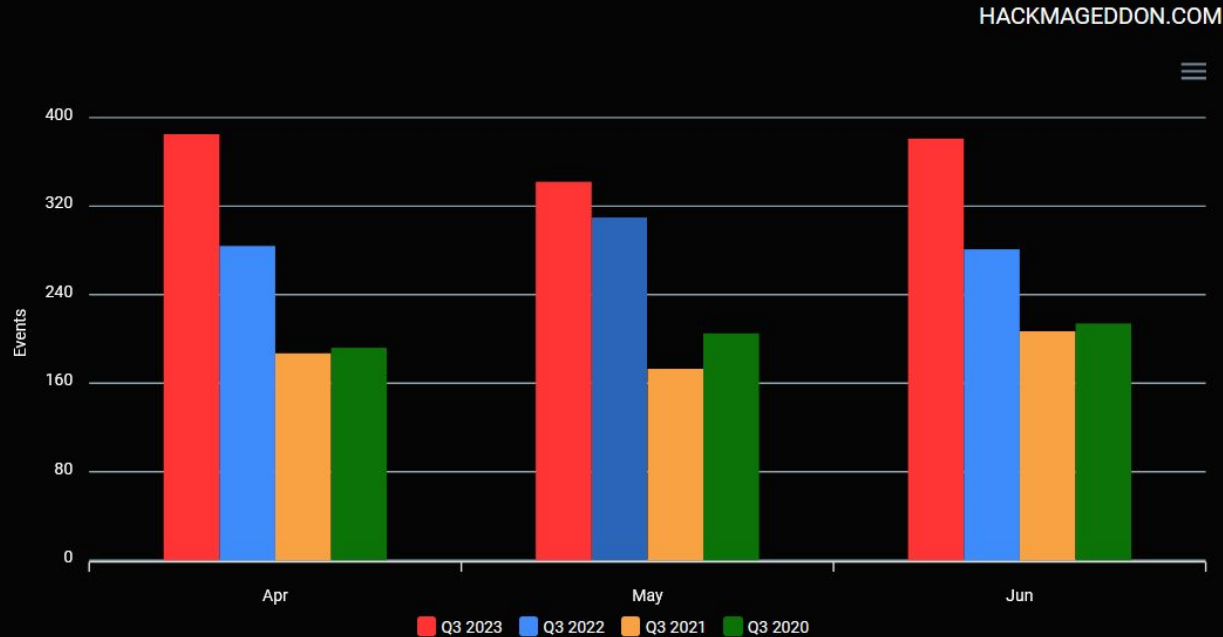


- Cyber Crime
- Cyber Espionage
- Hacktivism
- N/A
- Cyber Warfare

Motivations (Monthly Breakdown) - Q3 2023



Total Events - Q3 (2023 vs 2022 vs 2021 vs 2020)



CYBER THREAT RESILIENCE TEAM BY

Legfőbb fenyegetettségek

Zsarolóvírusok

- Lopás, titkosítás, DDoS és nyomásgyakorlás
- RaaS

Account takeover

Business e-mail compromise

DDoS

Támadás felhőben lévő végpontok ellen

Tox



Tox

toxicola7qww37qj.onion

FOR SALE

Ransomware as
a Service. The
menace!

Contact tox@sigaint.org and make an offer:

BeforeCrypt.com

- Platform + virus;
- Platform + virus + database + toxicola7qww37qj.onion private key.

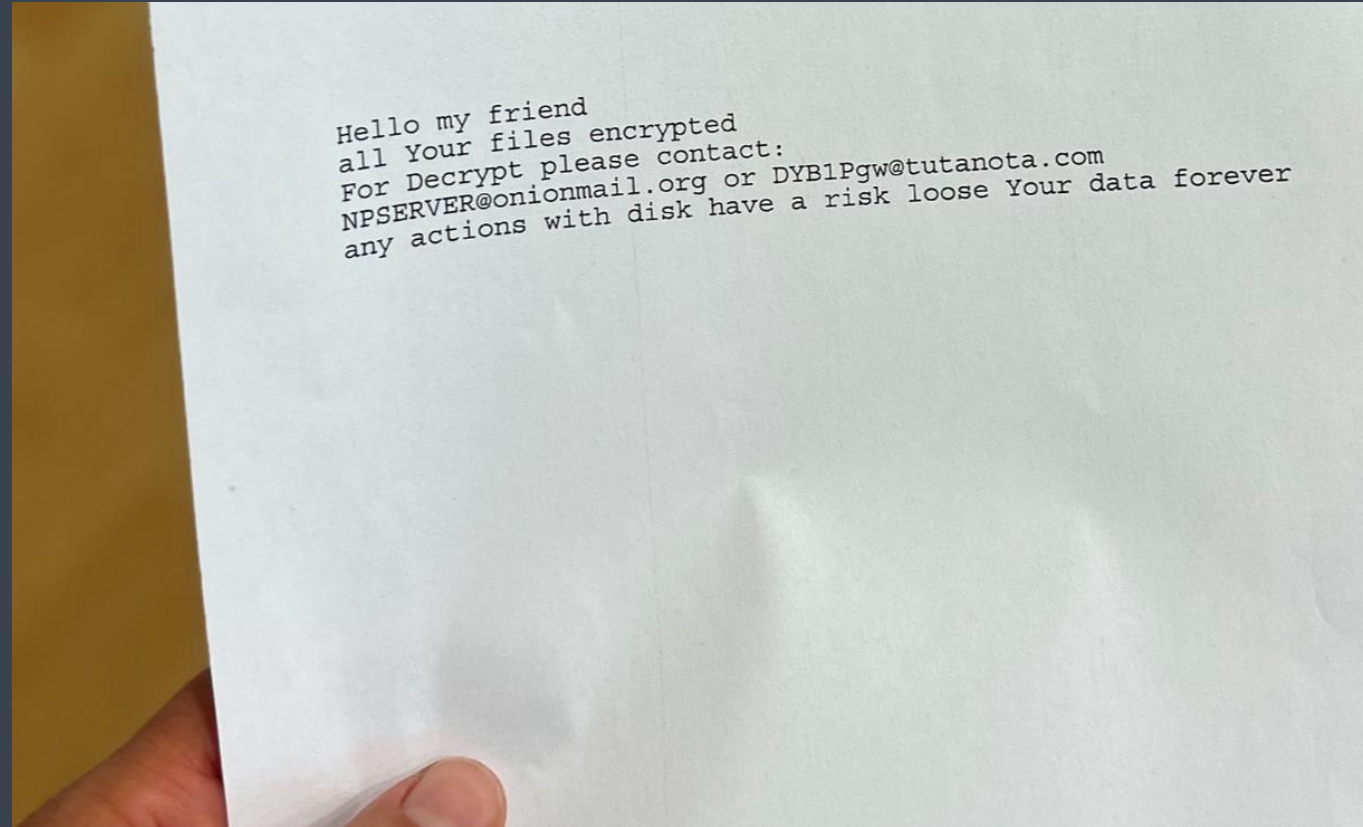
I'm talking about source code and documentation, you'll have to set up your own server.

CTRL

CYBER THREAT RESILIENCE TEAM BY 

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

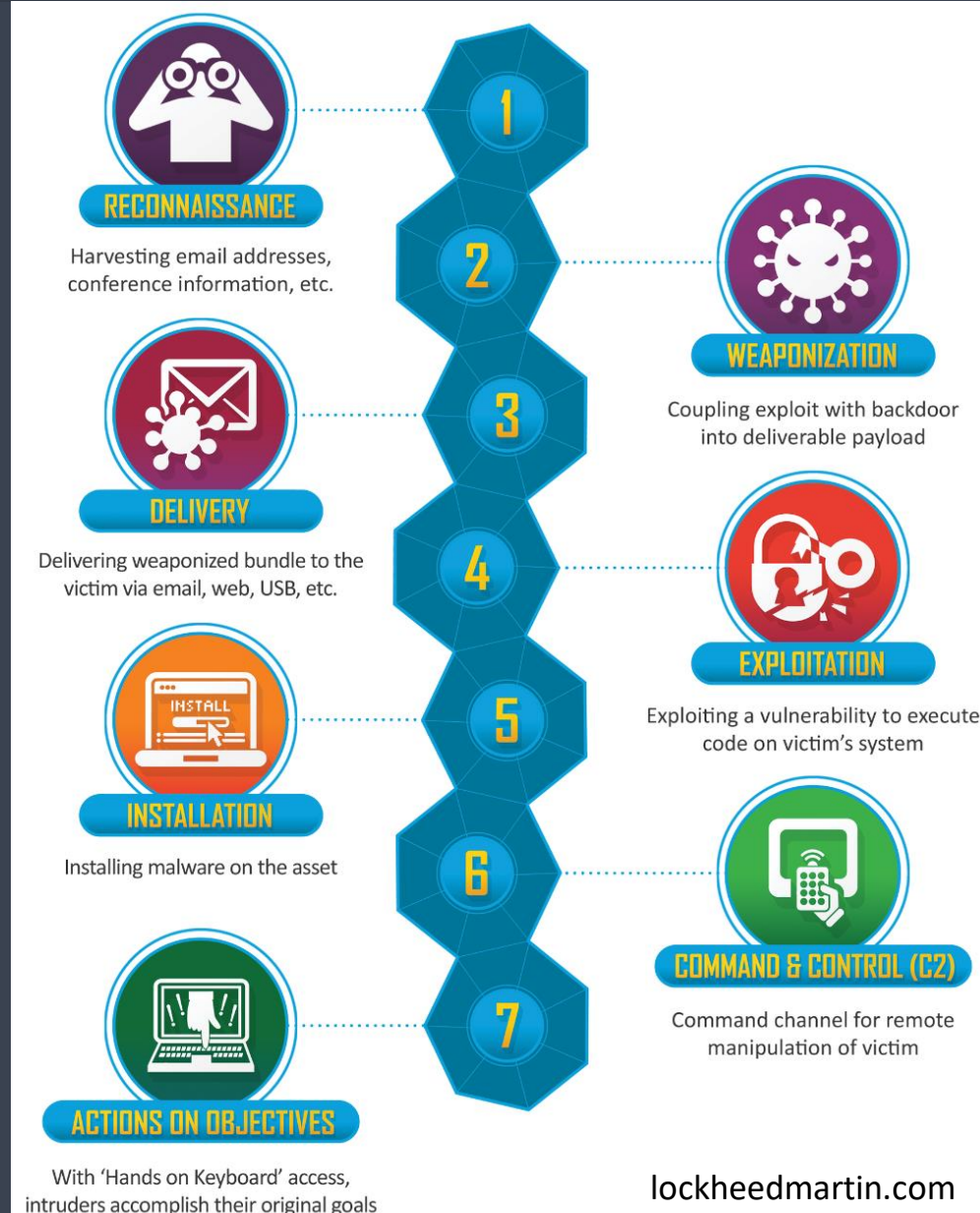
- Mentés
- Virtualizáció
- AD
- Backdoor-ok

Adatszivárogtatás

Titkosítás

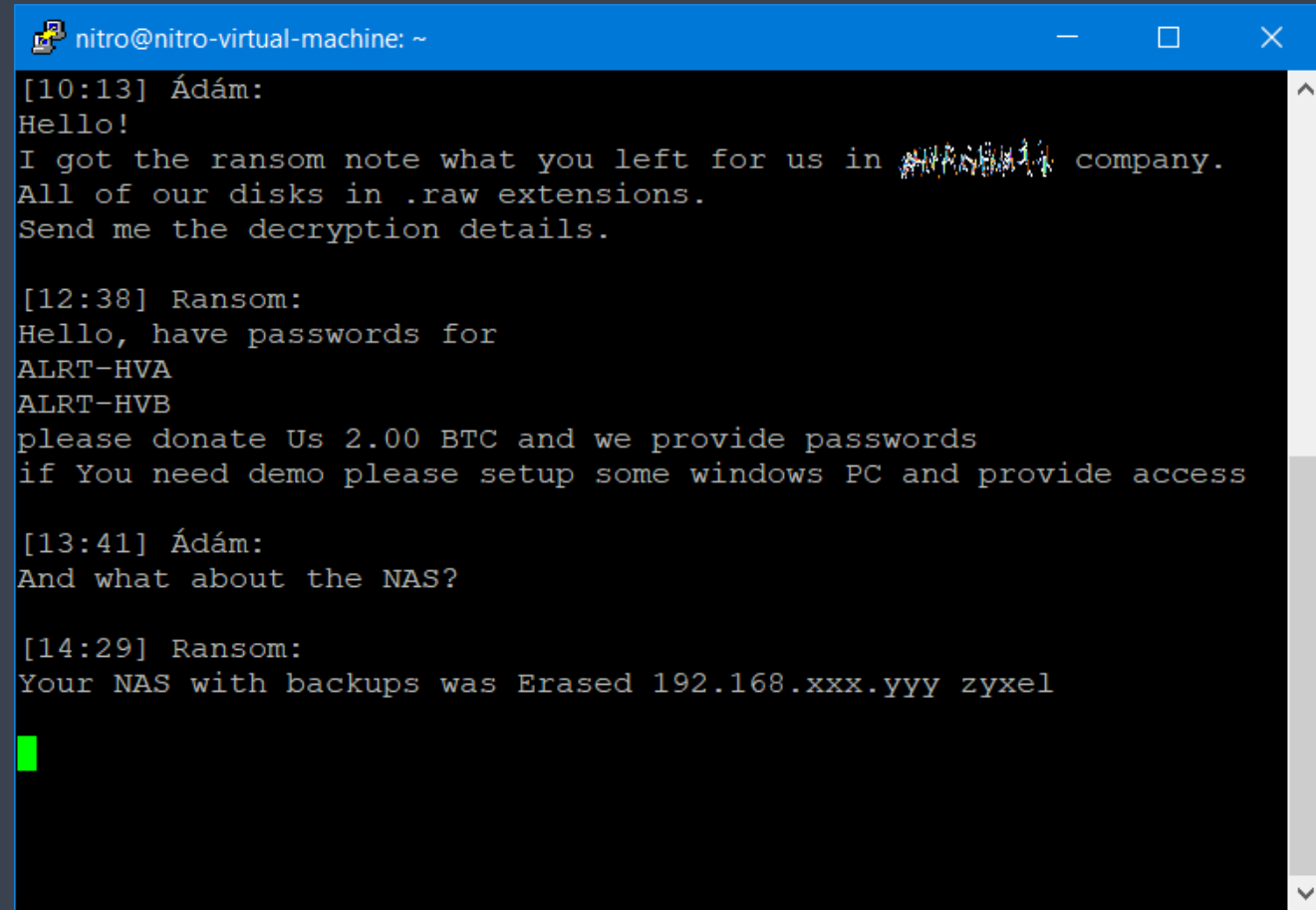
CTRL

CYBER THREAT RESILIENCE TEAM BY 



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



The screenshot shows a terminal window titled "nitro@nitro-virtual-machine: ~". The conversation is as follows:

```
[10:13] Ádám:  
Hello!  
I got the ransom note what you left for us in ALRT-HVA company.  
All of our disks in .raw extensions.  
Send me the decryption details.  
  
[12:38] Ransom:  
Hello, have passwords for  
ALRT-HVA  
ALRT-HVB  
please donate Us 2.00 BTC and we provide passwords  
if You need demo please setup some windows PC and provide access  
  
[13:41] Ádám:  
And what about the NAS?  
  
[14:29] Ransom:  
Your NAS with backups was Erased 192.168.xxx.yyy zyxel
```

Általános szolgáltatástartalom ransomware esetében

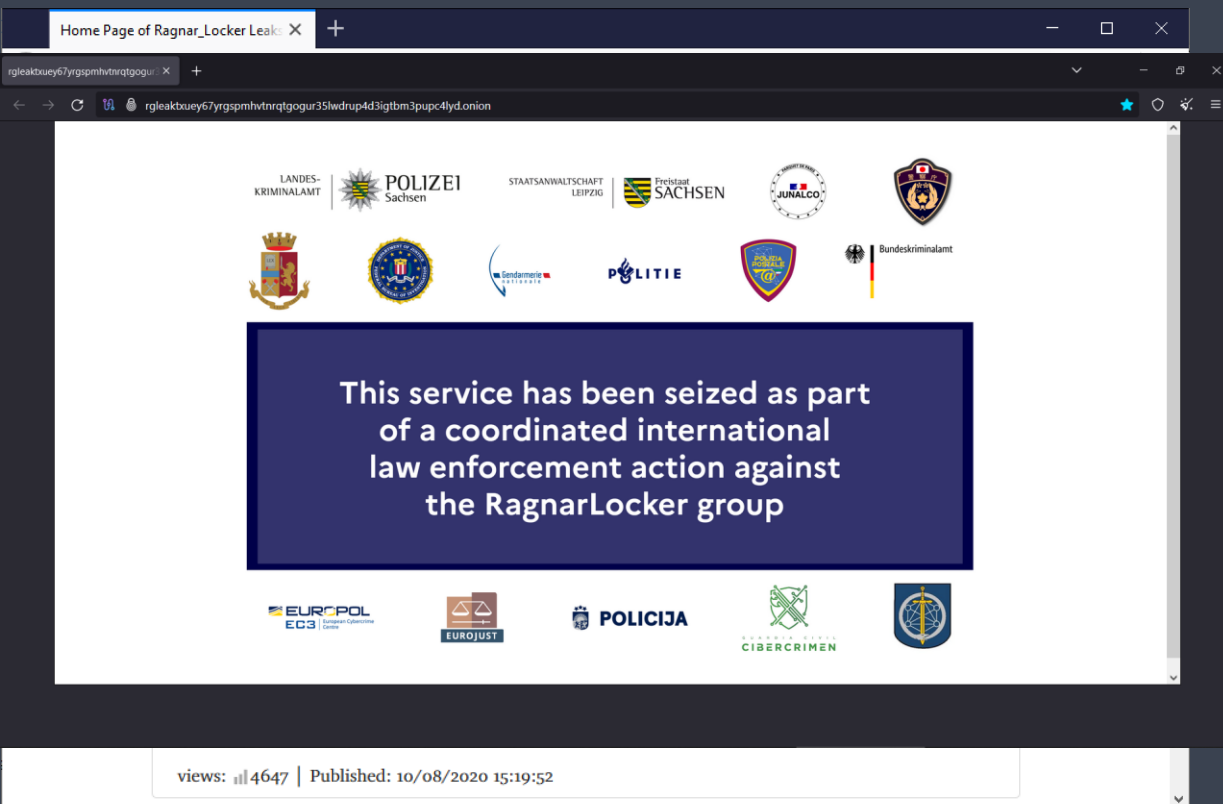
- **Felmérés**
 - Okozott károk
 - Környezet
 - Üzleti igények
- **Forensics**
 - Támadás módja
 - Ransom beazonosítása
 - Idővonal
- **Visszaállítás támogatása**
 - Tervezés támogatása
 - Biztonsági ellenőrzés
 - Technológiai eszközök
- **GAP-ek és sérülékenységek felmérése**
- **Post-mortem riport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



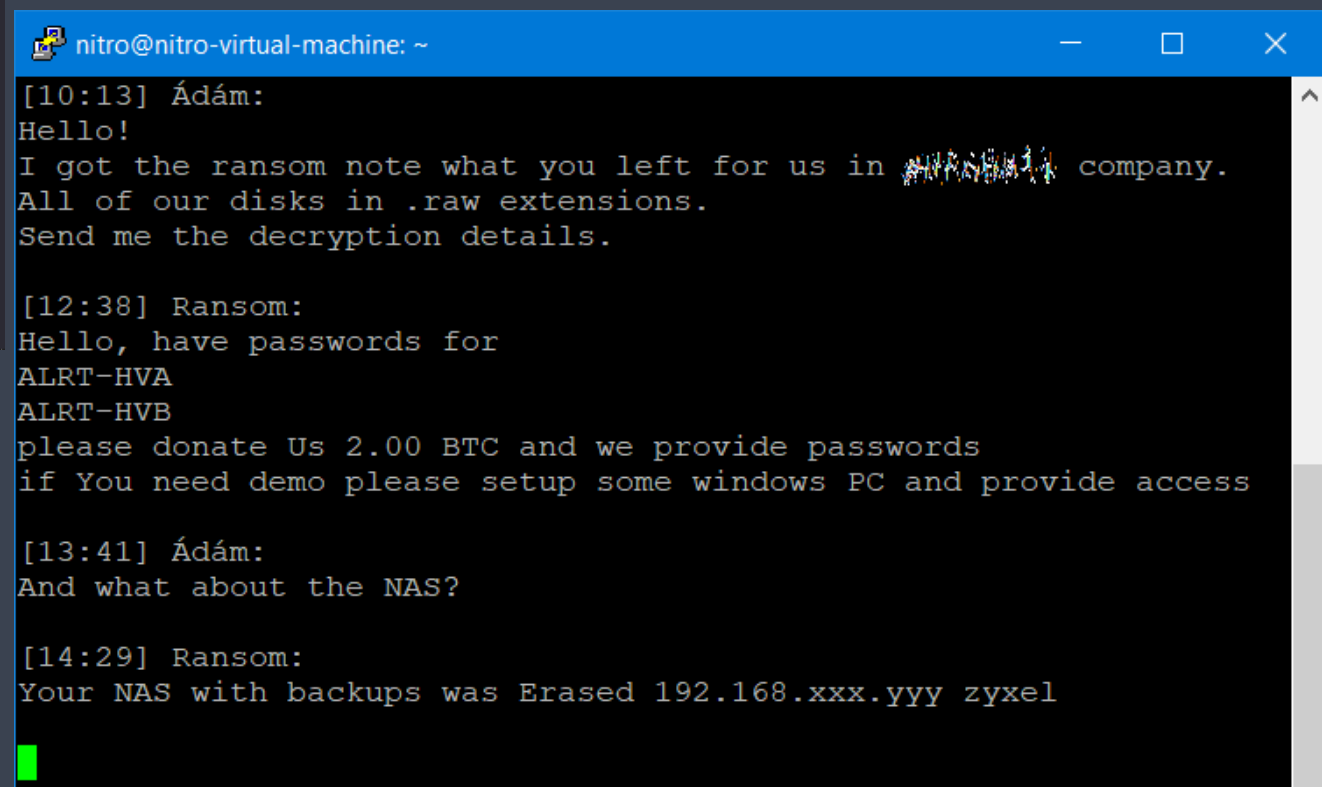
CTRL

CYBER THREAT RESILIENCE TEAM BY T

A sikerek – néhány példa sikeres visszaállásra



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



HTE
KIBERSZABÁLYOZÁSI
MINIKONFERENCIA
2024. március 19. | Budapest

HTE 75
ÉV
1949-2024



Köszönöm a figyelmet

hlavaty.gyozo@telekom.hu



Cybersecurity services

