InfoGuard
SWISS CYBER SECURITY

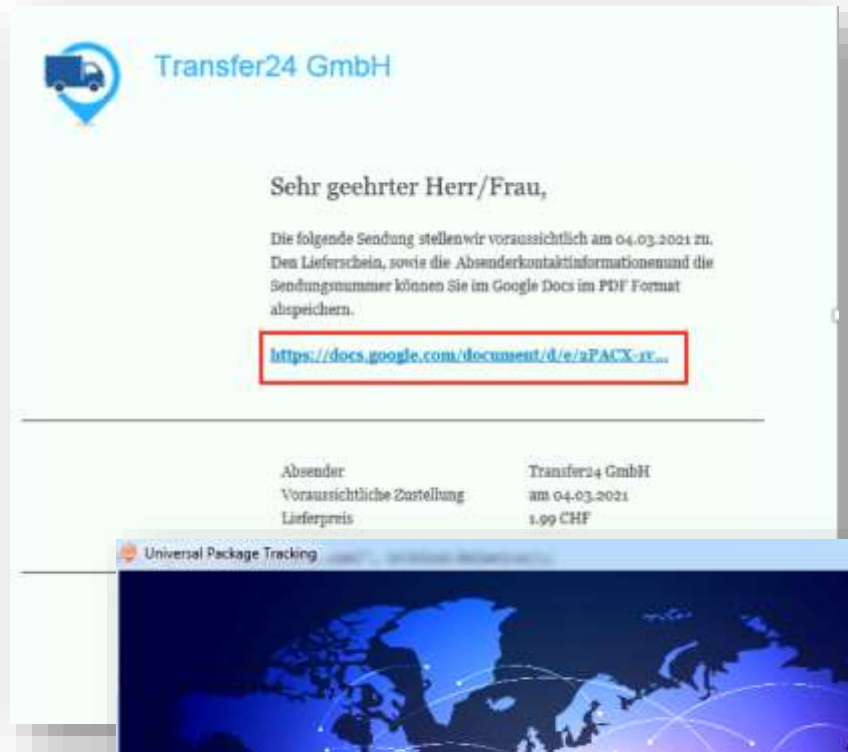
RANSOMWARE IN SWITZERLAND AND AROUND THE WORLD

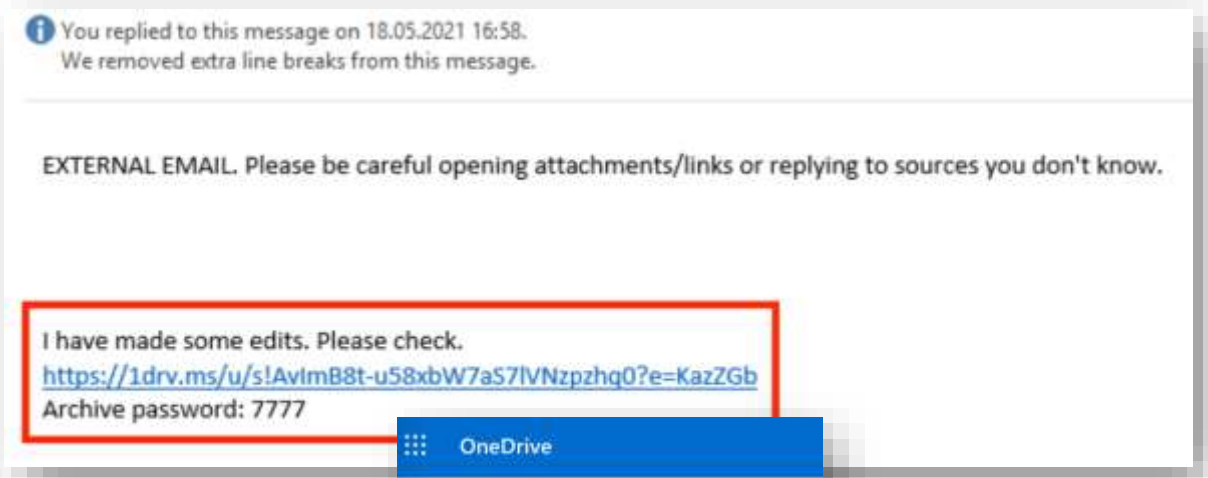
Insights, Facts and Findings

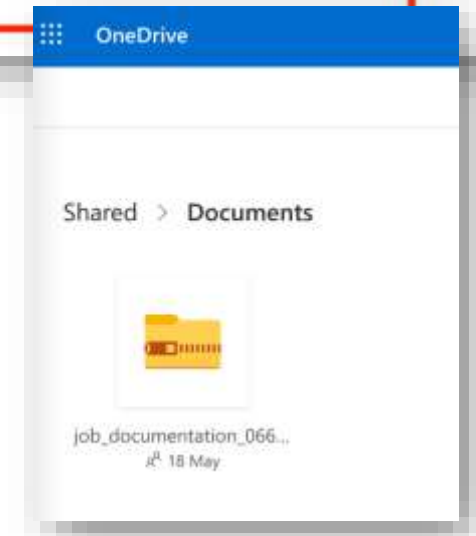
Initial Entry

Source: https://en.wikipedia.org/wiki/Fort_Bourtange

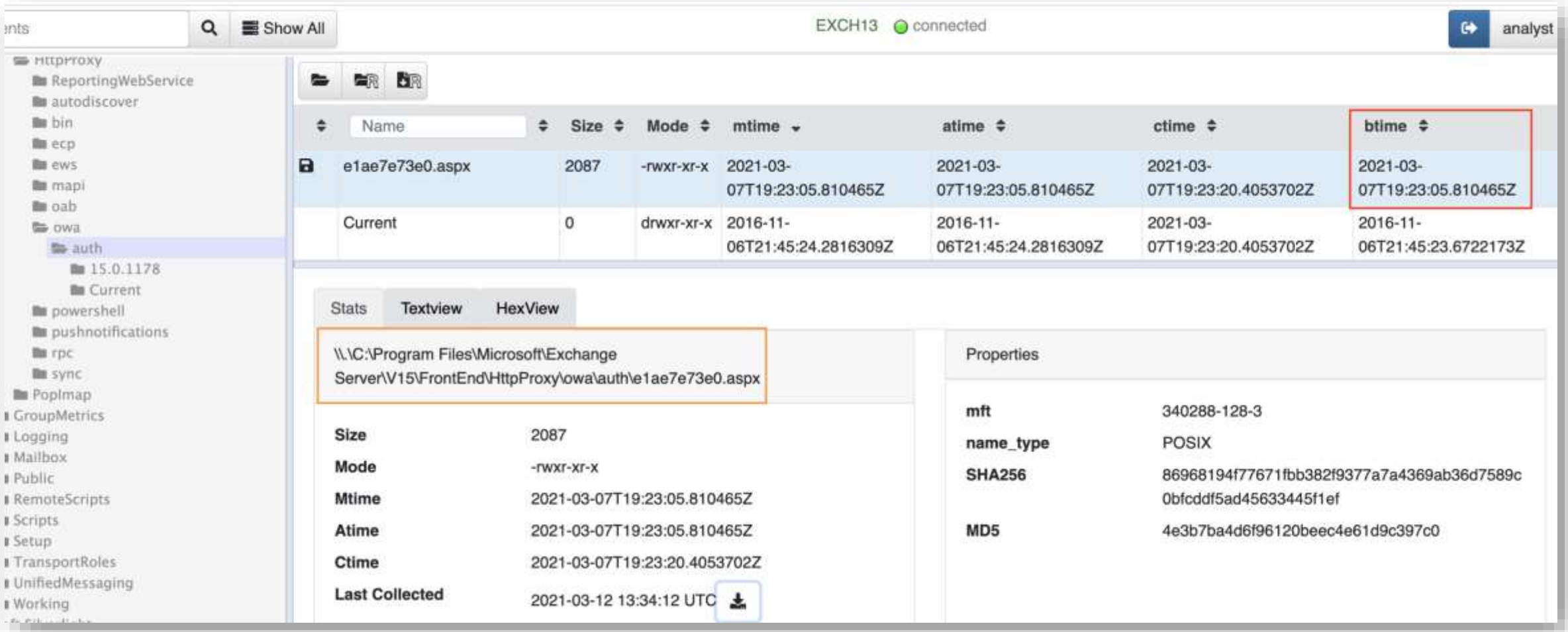
Phishing / Malicious documents



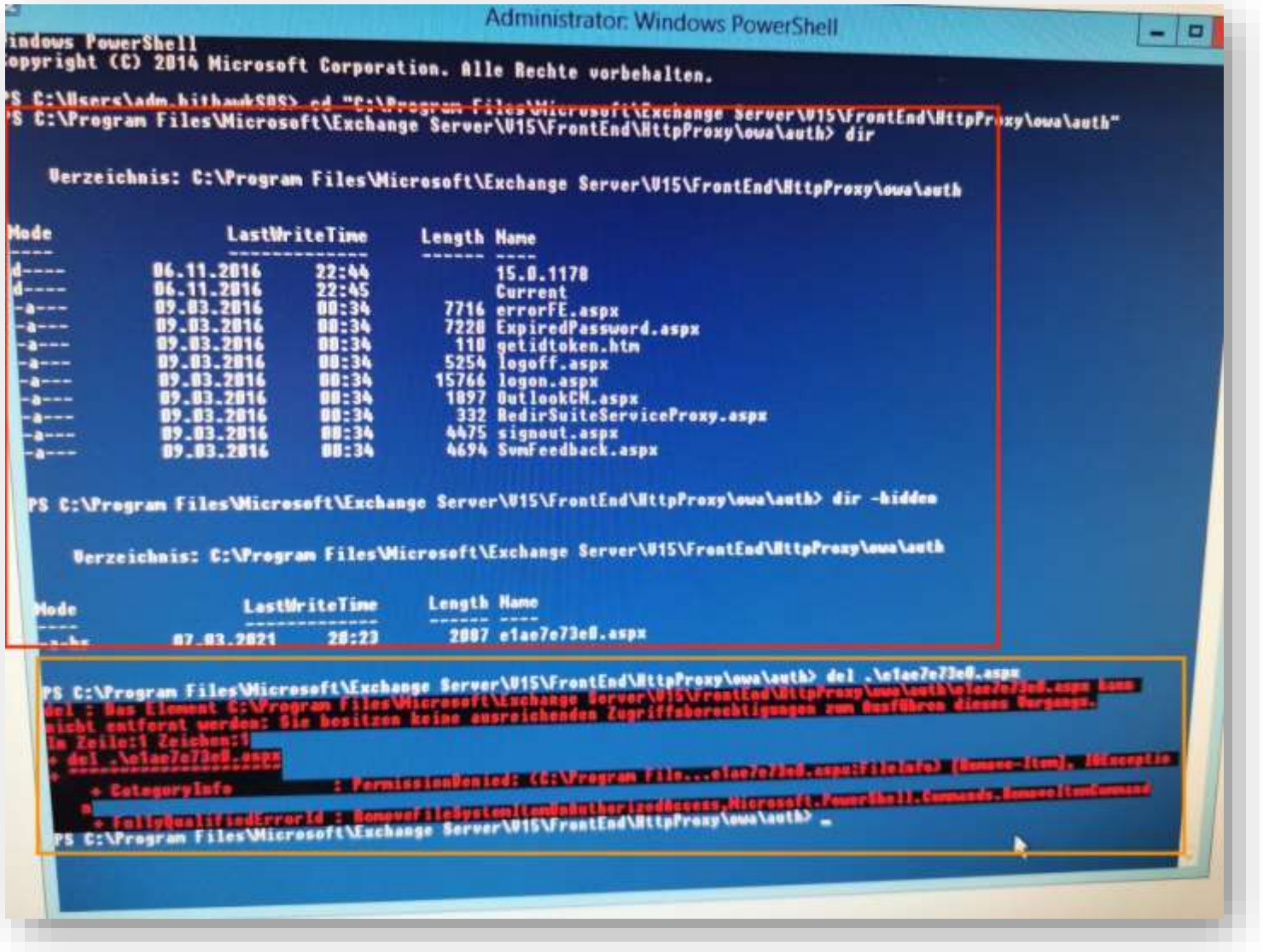




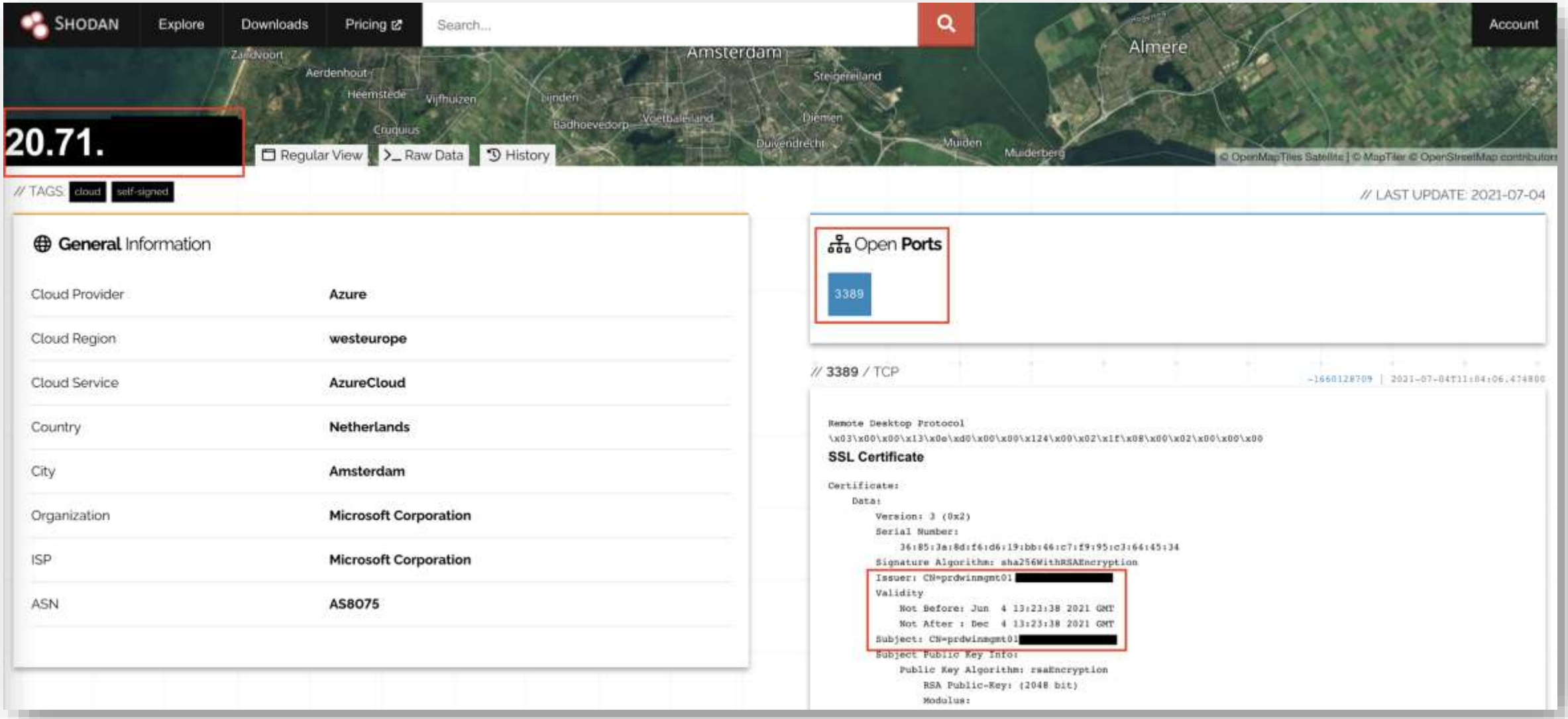
Vulnerabilities



Vulnerabilities



Extended Perimeter



Key Points

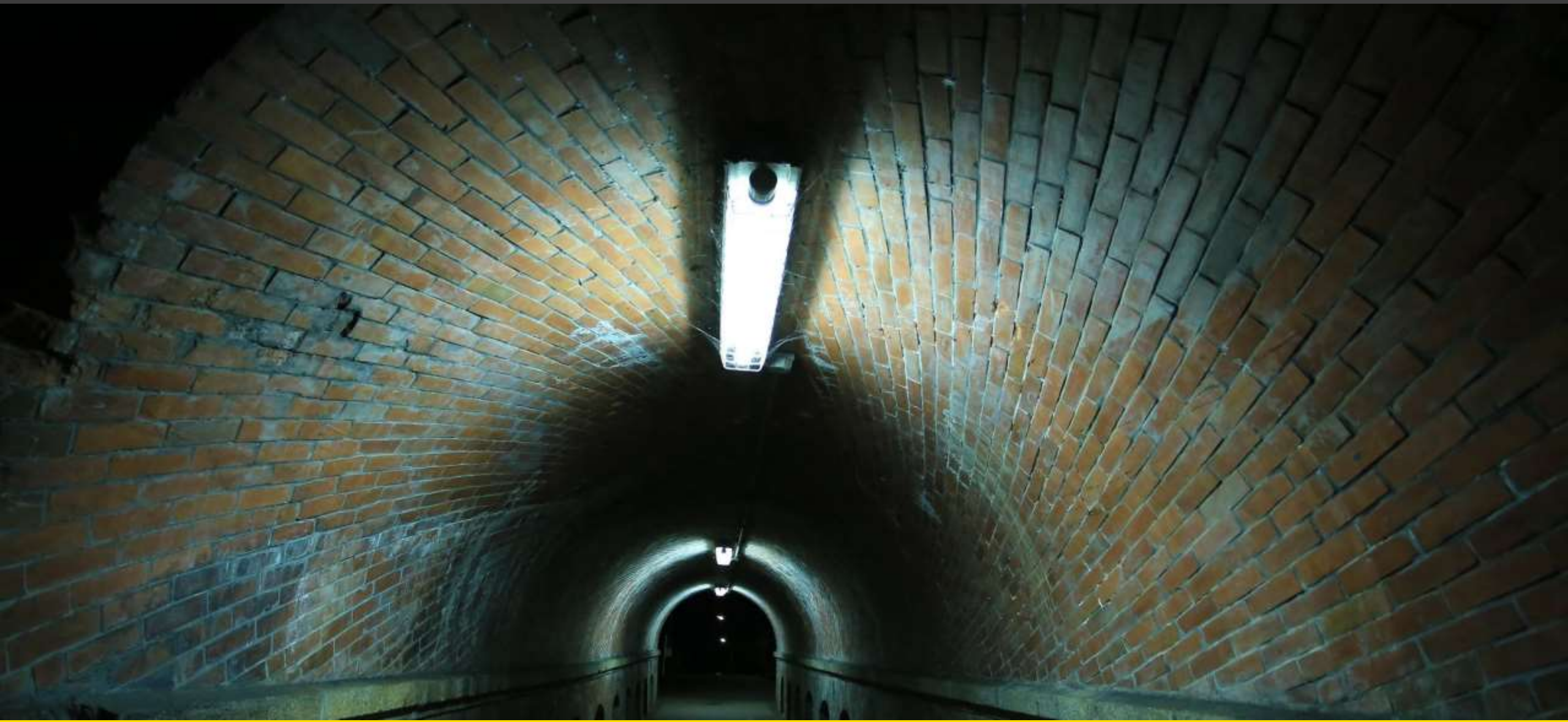
- MFA all the things

- Assume breach – even after applying patches
  - And change **all** passwords
    - And **check** that you changed all passwords

- Extend asset management to the Cloud (automate what you can)

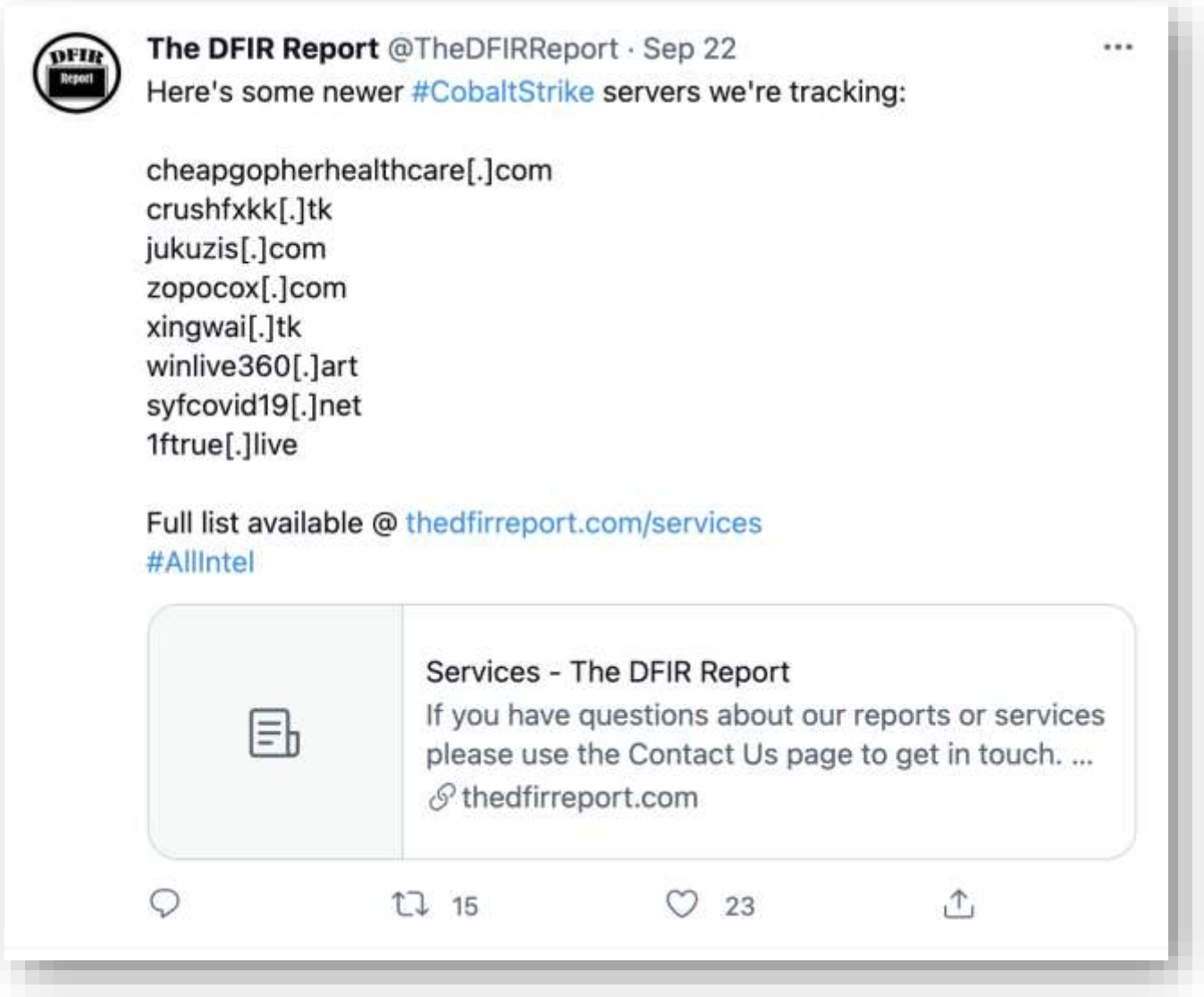
Persistent Access and Backdoors

InfoGuard
SWISS CYBER SECURITY



Remote Desktop Solutions

Cobalt Strike



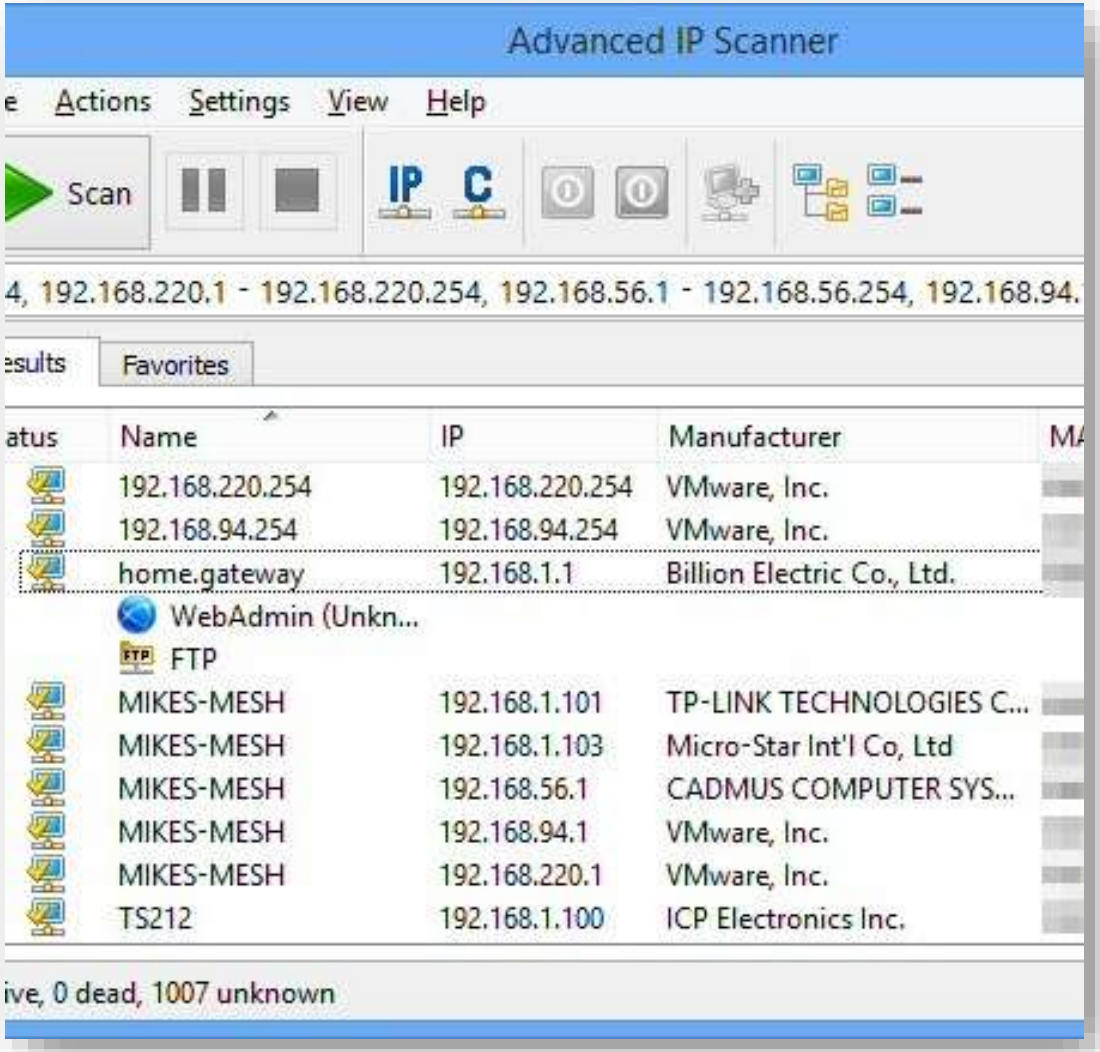
Key Points

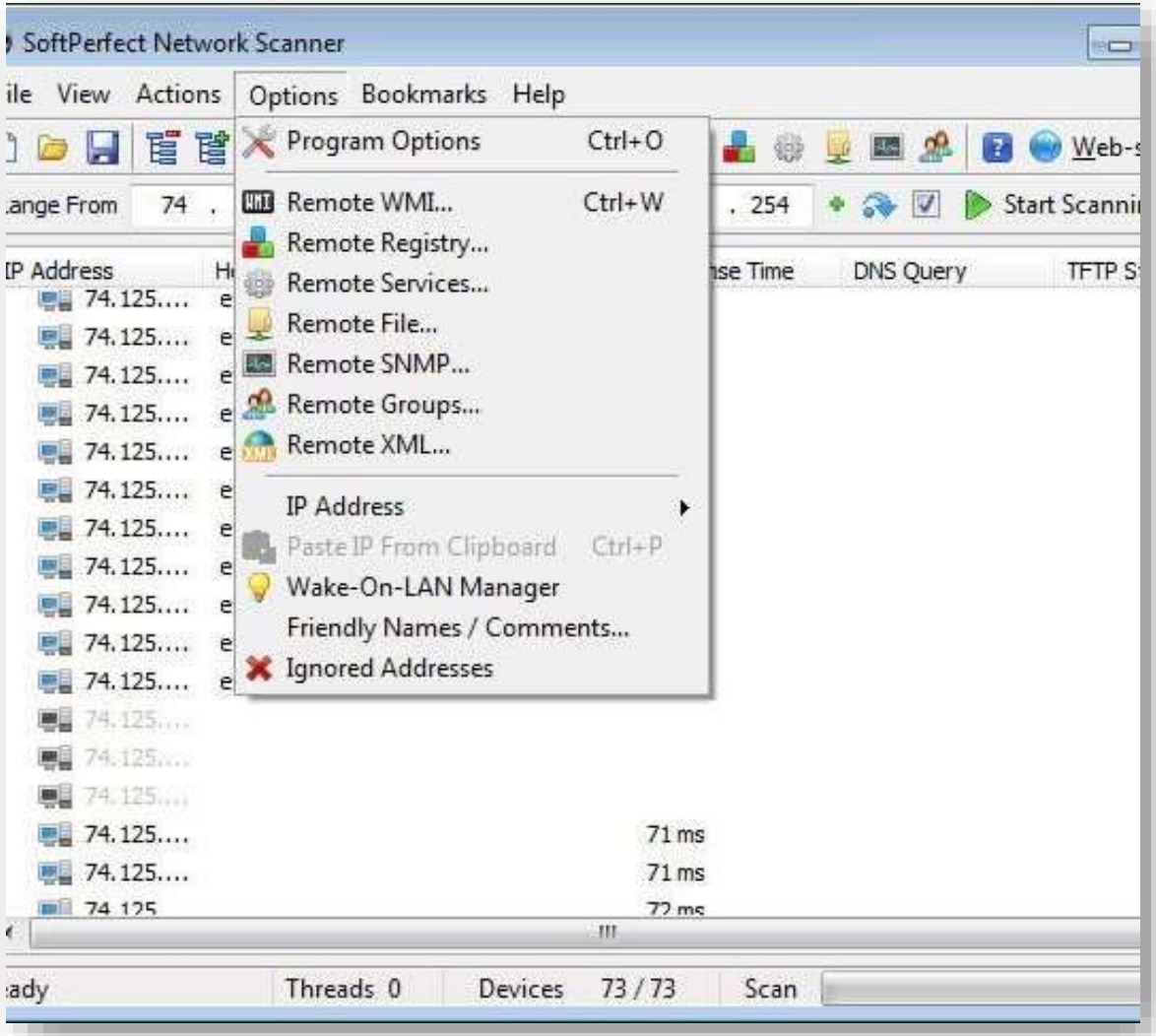
- Monitor connections to known remote desktop providers
  - Proxy-Logs
  - Firewall

- Use freely available data – as an example, the Cobalt-Strike IP list
  - Firewall

- Remote desktop software may write connection data
  - For example, the AnyDesk Traces file
  - May be useful in the event of an incident

Reconnaissance inside the network



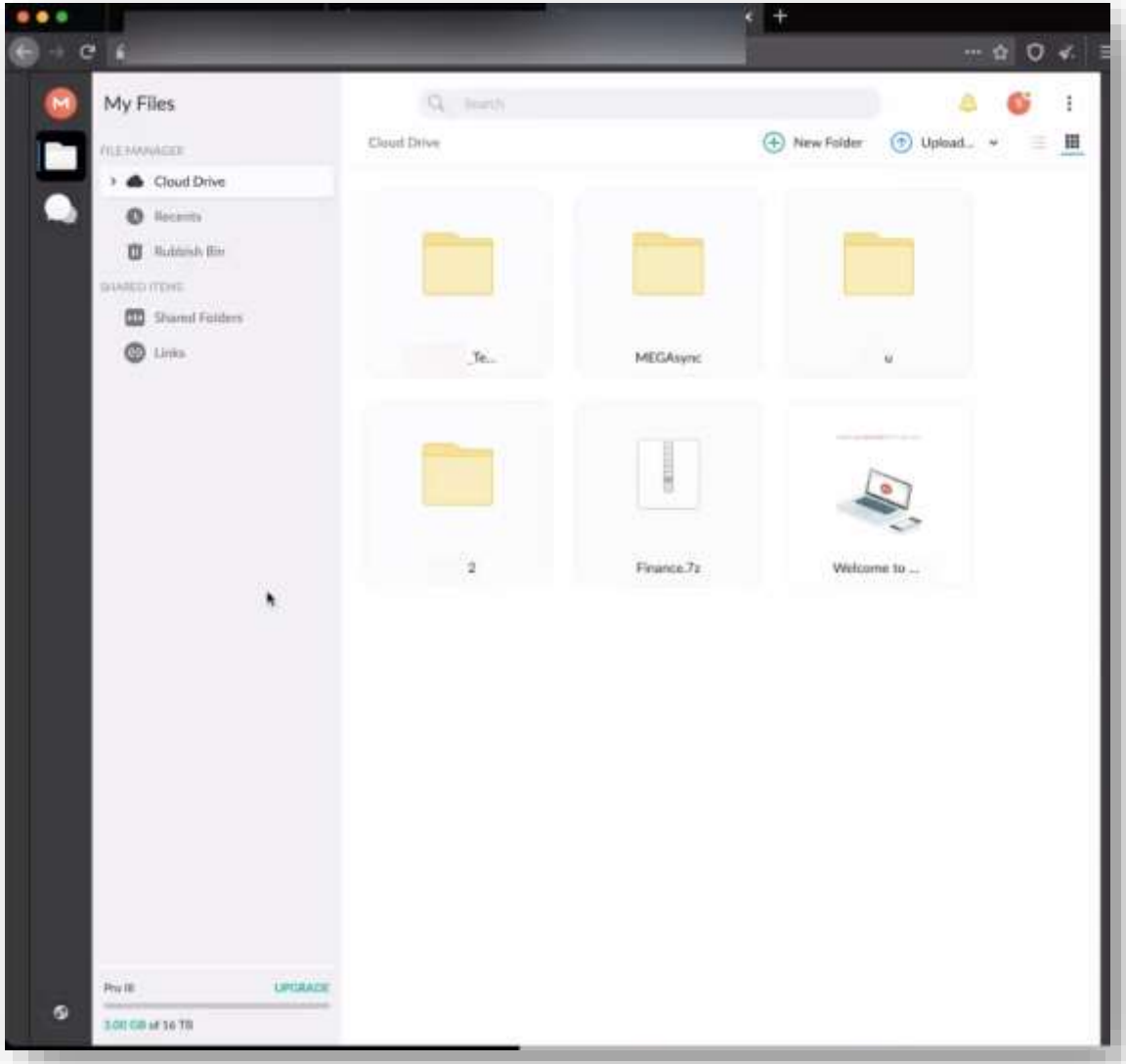


Key Points

- High CPU load
  - Check the processes on the host
- Softperfect license file
  - Tracking adversaries trough various breaches
- Advanced IP scanner
  - Stores the last scanned IP-Ranges within the registry (Useful for Incident Responder)

Exfiltration

Exfiltration – The other side around



Key Points

- Blocking (if possible) of known Upload-Providers
  - Mega.NZ
  - Yandex

- The configuration file for the cloud exporter might still be on disk
  - Or it could be carved out of the file system
  - May give you an advantage during negotiations

AV-Logs

Antivirus Event Analysis Cheat Sheet

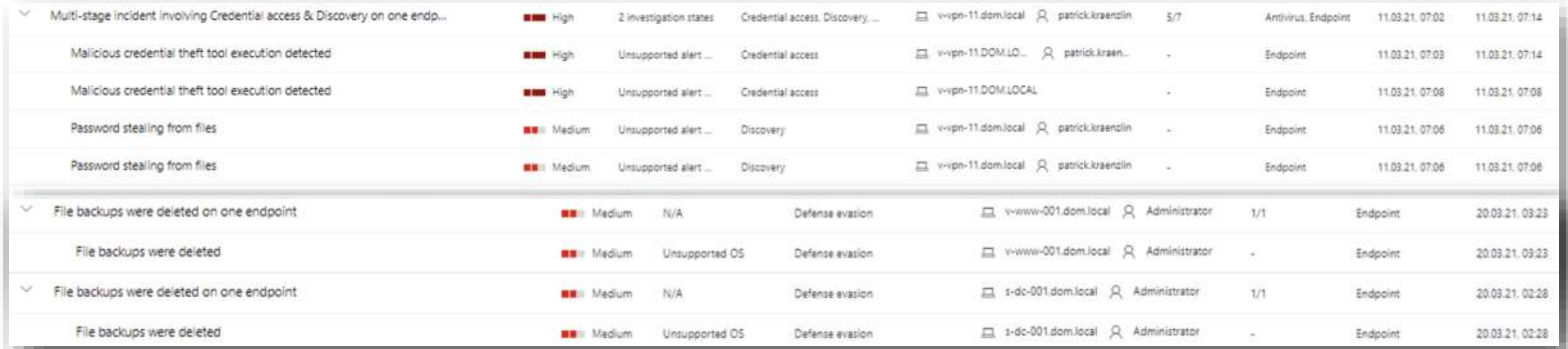
Version 1.7.2

Florian Roth @cyb3rops

Attribute	Less Relevant	Relevant		Highly Relevant	
Virus Type	HTML Iframe Keygen Joke Adware Clickjacking Crypto FakeAV	Trojan Backdoor Agent Malware JS Creds PS PowerShell Exploit Ransom	PassView Tool-Netcat Tool-Nmap RemAdm NetTool Crypto Scan	HackTool HTool HKTL PWCrack SecurityTool Clearlogs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP	CobaltStrike Keylogger MeteTool Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump Swrort Rozena

Source: https://www.nextron-systems.com

AV-Logs



Multi-stage incident involving Credential access & Discovery on one endp...	High	2 investigation states	Credential access, Discovery, ...	v-vpn-11.dom.local	patrick.kraenzlin	5/7	Antivirus, Endpoint	11.03.21, 07:02	11.03.21, 07:14
Malicious credential theft tool execution detected	High	Unsupported alert ...	Credential access	v-vpn-11.DOM.LO...	patrick.kraen...	-	Endpoint	11.03.21, 07:03	11.03.21, 07:14
Malicious credential theft tool execution detected	High	Unsupported alert ...	Credential access	v-vpn-11.DOM.LOCAL		-	Endpoint	11.03.21, 07:08	11.03.21, 07:08
Password stealing from files	Medium	Unsupported alert ...	Discovery	v-vpn-11.dom.local	patrick.kraenzlin	-	Endpoint	11.03.21, 07:06	11.03.21, 07:06
Password stealing from files	Medium	Unsupported alert ...	Discovery	v-vpn-11.dom.local	patrick.kraenzlin	-	Endpoint	11.03.21, 07:06	11.03.21, 07:06
File backups were deleted on one endpoint	Medium	N/A	Defense evasion	v-www-001.dom.local	Administrator	1/1	Endpoint	20.03.21, 03:23	
File backups were deleted	Medium	Unsupported OS	Defense evasion	v-www-001.dom.local	Administrator	-	Endpoint	20.03.21, 03:23	
File backups were deleted on one endpoint	Medium	N/A	Defense evasion	s-dc-001.dom.local	Administrator	1/1	Endpoint	20.03.21, 02:28	
File backups were deleted	Medium	Unsupported OS	Defense evasion	s-dc-001.dom.local	Administrator	-	Endpoint	20.03.21, 02:28	

Key Points

- AV usually detects one or more steps of the attackers

- The alarms are either
  a. not heeded
  b. not understood
  c. or not connected to a monitoring system at all

- Good (and underestimated) alert system

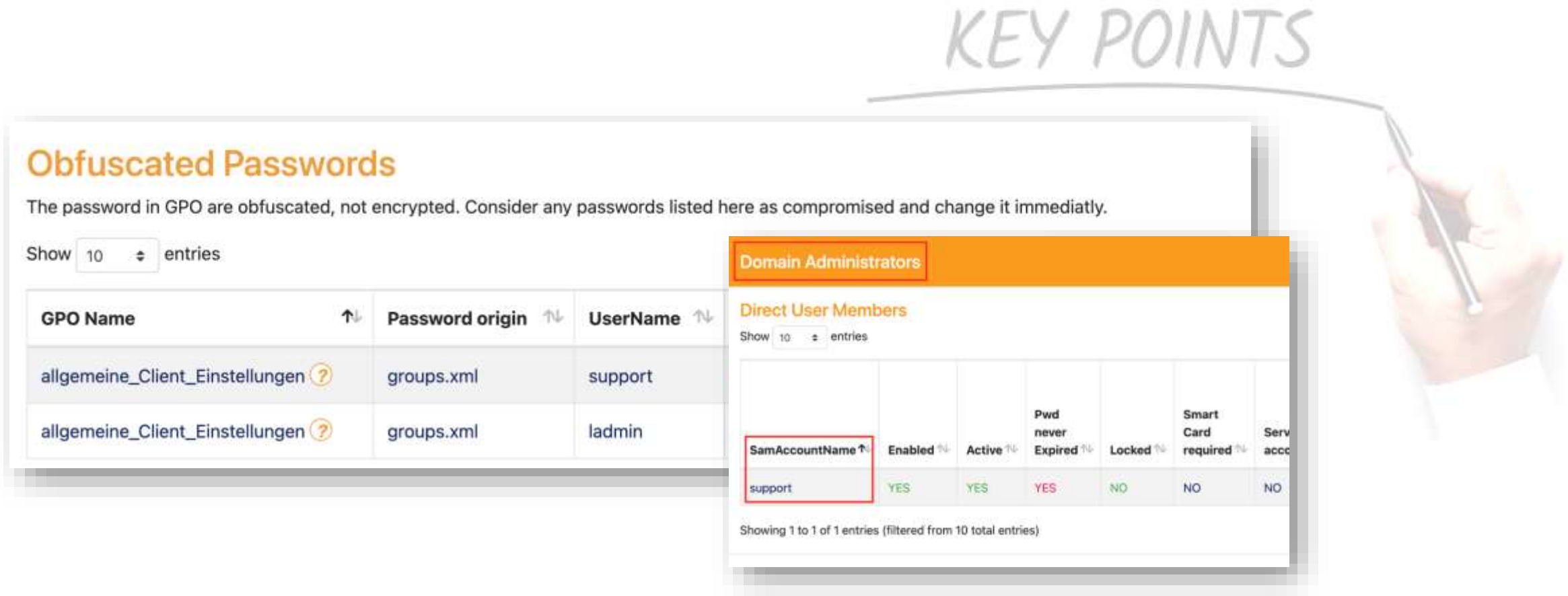
InfoGuard
SWISS CYBER SECURITY

Get Active Directory Security at 80% in 20% of the time

Active directory is quickly becoming a critical failure point in any big sized company, as it is both complex and costly to secure..

KeyPoints

- Check for stored passwords – from Zero to ~~Hero~~ Domain Administrator



INFOGUARD
Cyber Defence Center

InfoGuard
SWISS CYBER SECURITY

InfoGuard CYBER DEFENCE CENTER

- Swiss CDC
- 7x24
- 250m²
- 45 employees

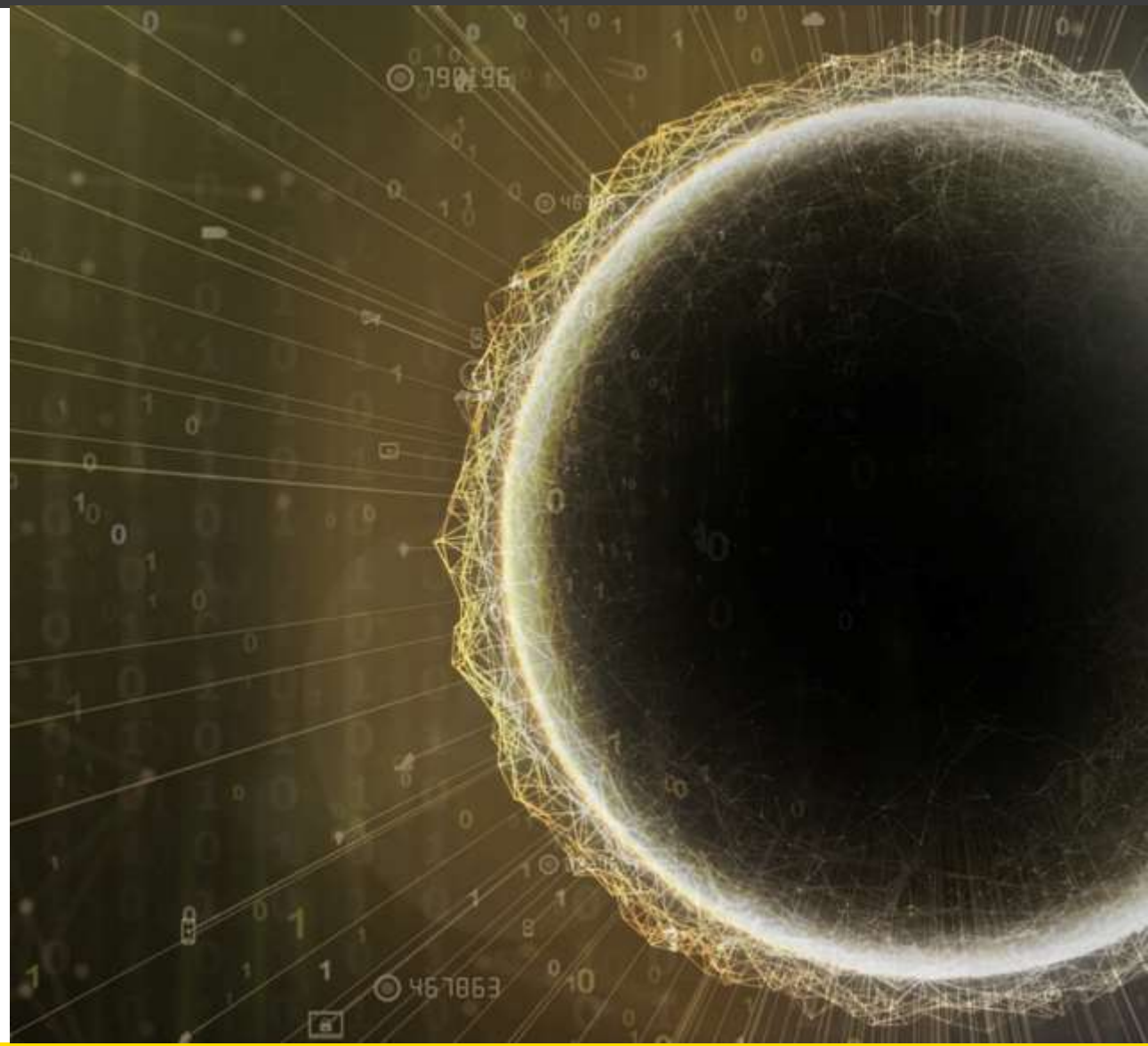
ISO 27001
ISAE 3000 TYPE 2

Questions?

InfoGuard
SWISS CYBER SECURITY

INFOGUARD –
the Swiss cyber security expert

Stephan Berger
Senior Cyber Security Analyst



InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz

Telefon +41 41 749 19 00