



Die Anatomie eines Ransomware Angriffs

Robert Wortmann & Oliver Locher





Robert Wortmann

Principal Security Strategist DACH, UK & Ireland



Oliver Locher

Sales Engineer DACH

Cybercrime big picture

Financially motivated attacks dominate

Cybercrime (for profit) remains the **largest portion of incidents**. In many incident response engagements, well over 75 % are driven by e-crime motives (ransom, fraud, theft)

Credentials and brute force

Attacks via weak or reused passwords are common – **credential stuffing** and **RDP brute-force** remain effective against organizations without multifactor authentication. Stolen credentials from data breaches or info-stealer malware fuel many intrusions

Cybercrime big picture

Criminal innovation

Attackers rapidly adopt new tech and strategies from using AI chatbots to craft phishing lures to exploiting emerging platforms (e.g. attacks via collaboration tools, deepfake scams in video calls)

Fragmentation of groups

Law enforcement takedowns (of infrastructure or arrests) lead to **splinter groups and rebrands** rather than eliminating threats. The cybercrime ecosystem adapts, ensuring a continuous barrage of new malware strains and threat actor aliases

AI Malware?

NYU team behind AI-powered malware dubbed 'PromptLock'

Researchers at NYU's Tandon School of Engineering confirmed they created the code as part of a project to illustrate potential harms of AI-powered malware.

BY [DEREK B. JOHNSON](#) • SEPTEMBER 5, 2025

🔊 Listen to this article 7:23 Learn more.



Tools like “PromptLock” (NYU proof-of-concept) show that LLMs can generate **basic malware building blocks** — but not full attack chains

Current AI models do **not autonomously create functional malware**: no payload delivery, persistence, lateral movement, or command logic

There is no sign of "autonomous malware development" — LLMs lack intent, context awareness, and execution logic

Risk comes from **lowering the entry barrier** — less-skilled actors can build scripts faster, but not smarter

Step 1: the right victim

Size doesn't matter

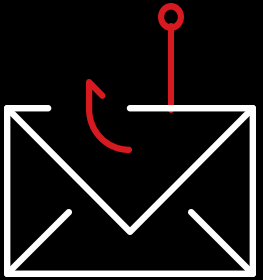
800 employees

24x7 production

Cloud usage

No SOC

Most-seen initial access techniques



Phishing

Targeting
credentials



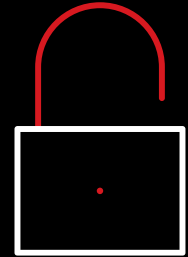
Social Engineering

Targeting data,
credential resets,
support scam



Internet-facing vulnerabilities

Notably VPN
gateways



Internet-facing misconfigs

Open RDP,
lack of MFA

Chronology



11/2023 Spear Phishing of a marketing employee

Chronology

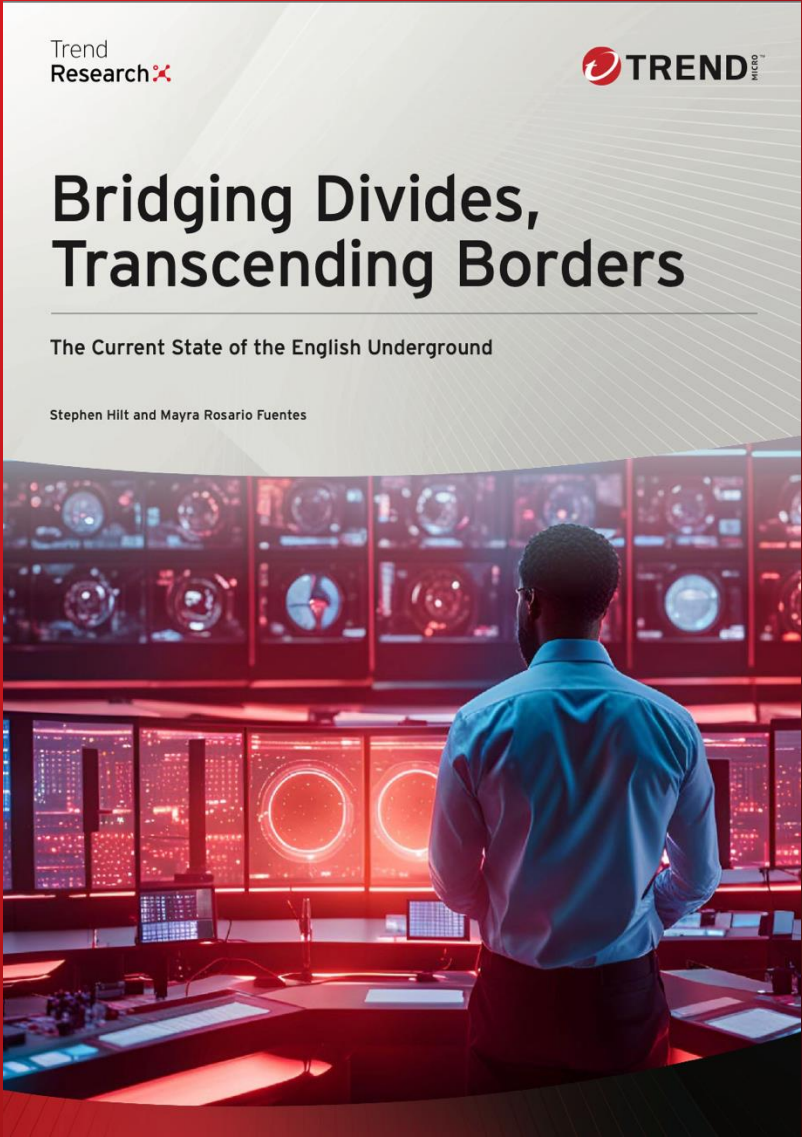
● **11/2023** Spear Phishing of a marketing employee

● **01/2024** Offering access via marketplace

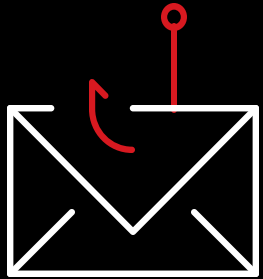
Initial access often outsourced to access brokers

Sample Offering	One-time cost US\$
Chemical manufacturer in Israel	\$2,000
Billion-dollar company in Australia	\$20,000
Government agency in South Korea	\$500
Electricity, oil & gas production co.	\$20,000
Healthcare company in Maryland	\$600

Source: Bridging Divides, Transcending Borders: The Current State of the English Underground.
Trend Micro, January 2025



Important counter measures



Phishing

Proper Email
Security (BEC)



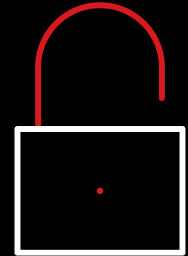
Social Engineering

Awareness Trainings
incl. Social
Pentesting



Internet-facing vulnerabilities

Active Vulnerability
Management



Internet-facing misconfigs

Active Posture
Management

Important counter measures (cont.)



Bad Websites

Proper Web
Controls (e.g. block
of uncat. sites)

Step 2: the implementation

Chronology

- **11/2023** Spear Phishing of a marketing employee
- **01/2024** Offering access via marketplace
- **03/2024** Access via Citrix VDI Farm, disabling protection

Impair defenses

Trend Vision One™ | Workbench > WB-12179

Summary

Case: [Open new case](#)

Owners: None

[Heuristic Attribute] Possible Abuse Elevation Control Mechanism

Detects possible abuse elevation control mechanism technique.

Score: 63

Impact scope: 1 16 1

Created: 2024-08-18 03:17:05

Automated responses: None | [Execute playbook](#)

Highlights

UAC Bypass via ICMLuaUtil Interface

Technique: [T1548.002 - Bypass User Account Control](#)

Data source / processor: Endpoint Sensor

2024-08-18 03:12:50 | [View event](#)

[redacted]

(objectFileHashSha1) 5f2c7da181a0ef32df5b9c...

(parentCmd) C:\WINDOWS\system32\svchost.e...

(processCmd) C:\WINDOWS\system32\DllHost...

(objectCmd) [redacted] \Downloa...

Trend Vision One™ | Workbench > WB-12179-20240817-00010

Summary

Case: [Open new case](#)

Owners: None

[Heuristic Attribute] Impair Defenses

Detects Impair Defenses Technique

Score: 51

Impact scope: 1

Created: 2024-08-17 23:09:25

Automated responses: None | [Execute playbook](#)

Highlights

Behavior Monitoring Detection - TDSSKiller disabling TM Product

Technique: [T1489 - Service Stop](#)
[T1562 - Impair Defenses](#)
[T1562.001 - Disable or Modify Tools](#)

Rule name: Malware Behavior Blocking

Data source / processor: Trend Micro Apex One as a Service

2024-08-17 23:01:34 | [View event](#)

[redacted]

(objectCmd) -dcsvc "TMBMServer" -accepteula

(processFileHashSha1) 8c5437cd76a89ec983e3b364e219944da3dab464

(processCmd) /C [redacted] \Desktop\tdsskiller.bat"

(processFilePath) C:\Windows\System32\cmd.exe

(engineOperation) Create Process

(act) Terminate

(objectFileHashSha1) 8c96200c80fc632d0645bf7493cd55e5cdf11cda

(objectFilePath) C:\Windows\tdsskiller.exe

Lateral Movement

netscan.exe

Profile

Events

Observed Attack Techniques:

Network Scanning Using SoftPerfect Network Scanner

Object type:

Process

Created:

2024-08-08 01:47:41

Process name:

netscan.exe

File path:

\\localhost\c\$\Downloads\softportable_netscan\netscan.exe

CLI command:

"\\localhost\c\$\Downloads\softportable_netscan\netscan.exe"

File SHA-1:

e38082ae727aaef4f241a1920150fdf6f149106

File SHA-256:

d1347f4dccebf2fcd672dcef9c66c91b9d3f12b9881e3e390626927718fda6...

File MD5:

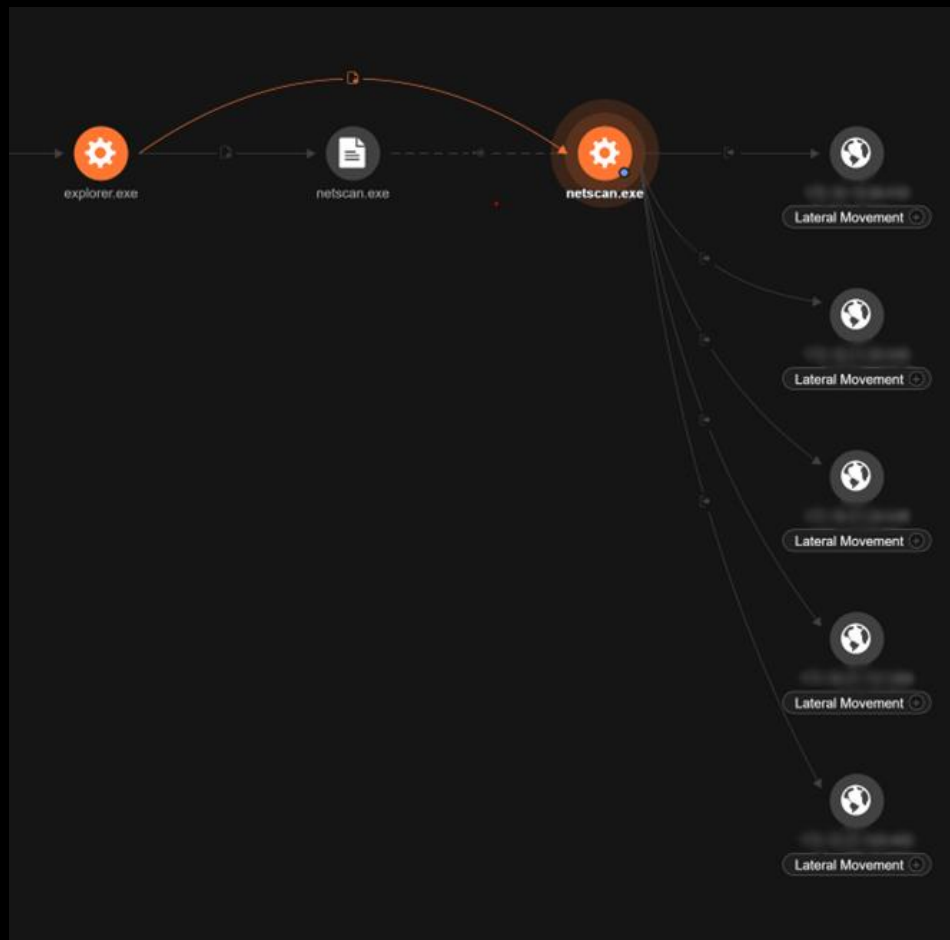
719ba3d7051173982919d1e4e9e9a0ec

Process ID:

9804

Signer:

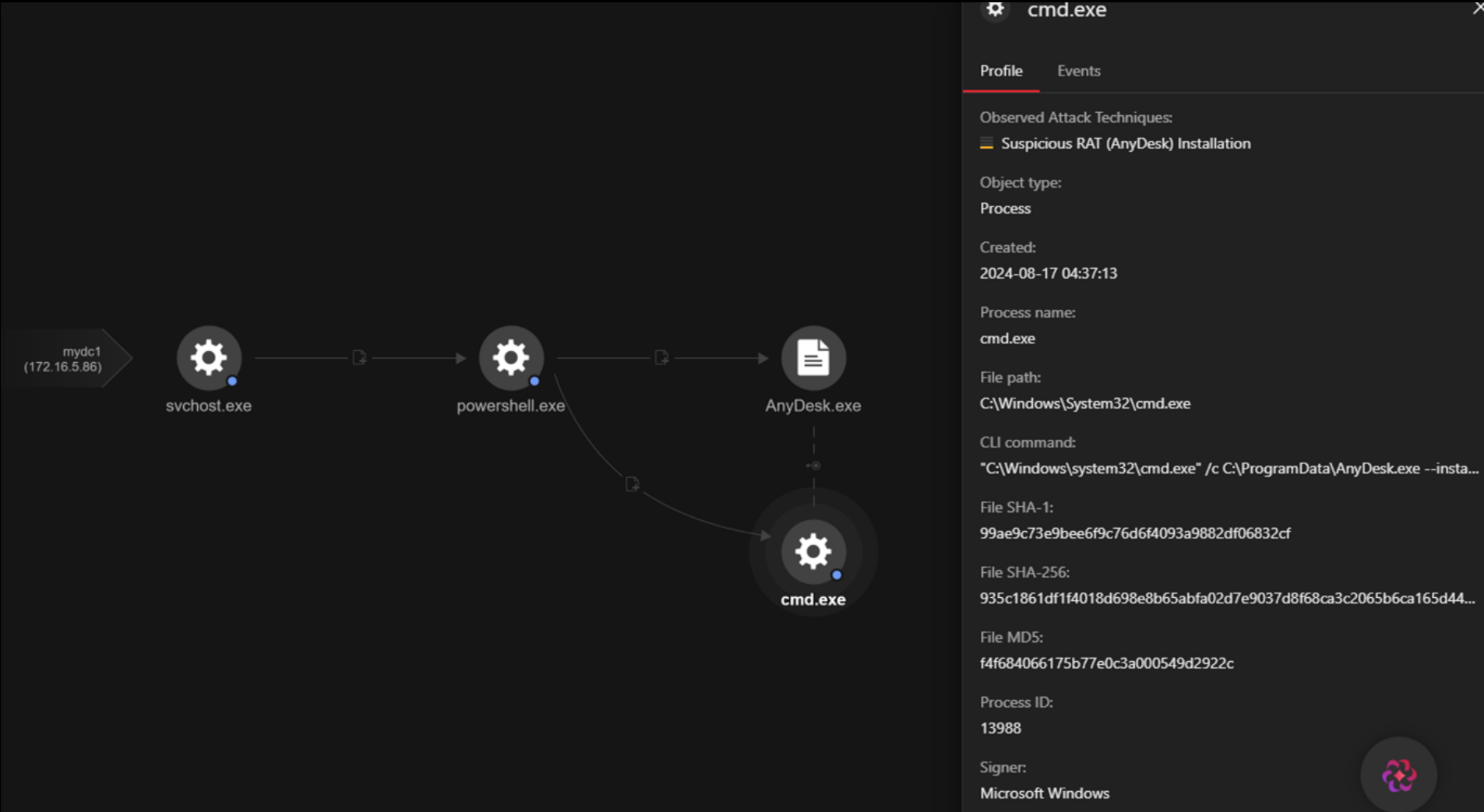
SoftPerfect Pty. Ltd., SoftPerfect Pty. Ltd.



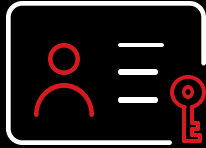
Chronology

- **01/2024** Spear Phishing of a marketing employee
- **03/2024** Offering access via marketplace
- **03/2024** Access via Citrix VDI Farm, disabling protection
- **03/2024** Creation of further persistences on unprotected clients, credential dump and data exfiltration

Remote Access

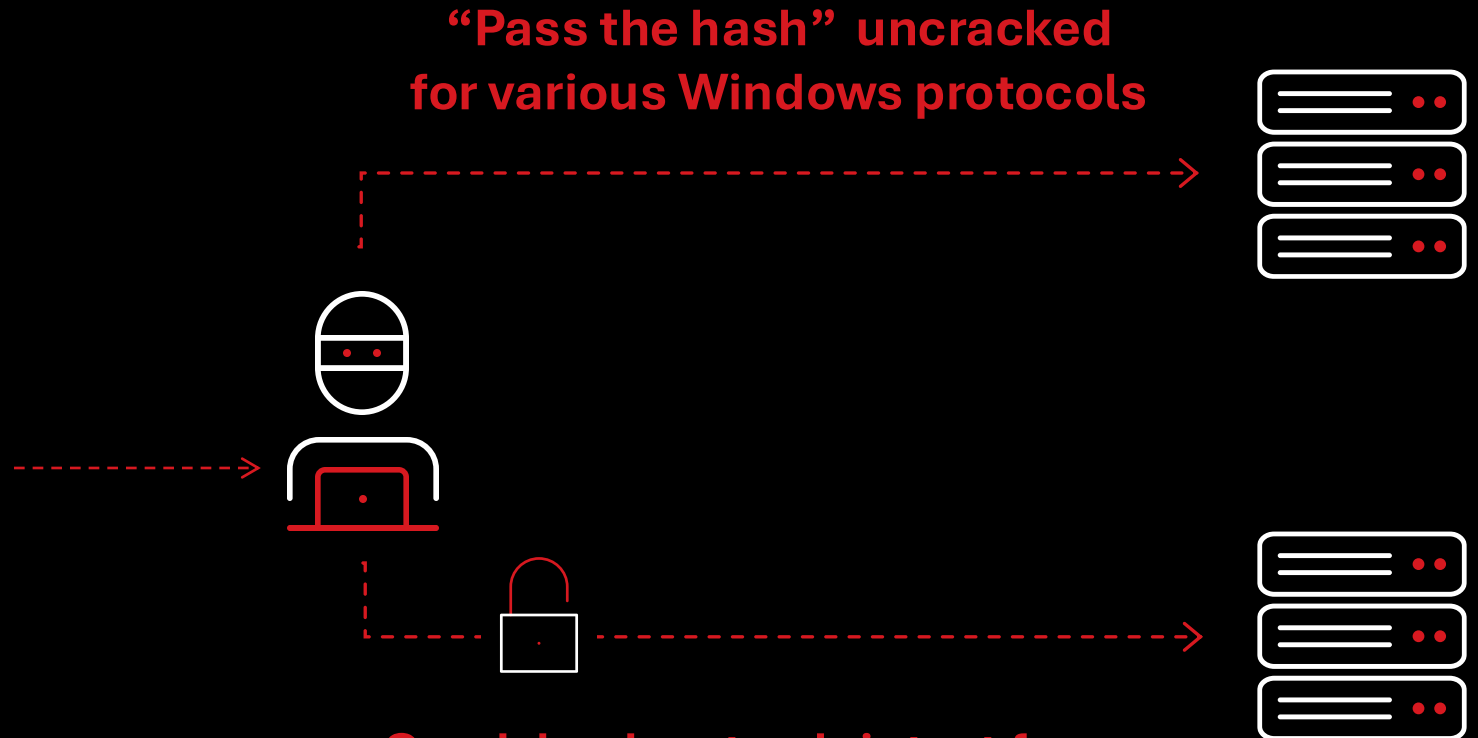


Password hash cracking is now faster/cheaper



Windows Password Hashes obtained by an attacker

8846F7EAAE8FB117AD06BDD830B7586C
E10ADC3949BA59ABBE56E057F20F883E
B7E0F58E067DC79A3EED1C68476C681C
682C99035B38A3B9A9F40D369D42F482
B0D32D0DA05AEBE8706F7DF6B1D58E4F
3328f34bd5d9e61fcbc97a8809492848
2a86a9e0313b84a8ccd94a36ee99f7fa
25fd70cd5ae456a1c76cf0db0f1529d4
1559133a36298127a58cd505965b0f64
0aa4a26fd4db4bea7628f49bf93189bd
231fa9239f4c574f1647c81b97e01ad4
2939ac78ab4c90bf99a3891ce09395fd



**“Pass the hash” uncracked
for various Windows protocols**

**Crack hashes to plaintext for use
in web apps, VPN logins, etc.**

**Hash cracking used to take time...
and expensive GPUs...**

A \$30K Hash
Cracking Rig...

Or do it for
\$0.29 using

aws +



NPK

Chronology

- **01/2024** Spear Phishing of a marketing employee
- **03/2024** Offering access via marketplace
- **03/2024** Access via Citrix VDI Farm, disabling protection
- **03/2024** Creation of further persistences on unprotected clients, credential dump and data exfiltration
- **01.04.2024** Various notifications by Trend Micro, as well as outgoing phishing and BEC

Chronology

- **01/2024** Spear Phishing of a marketing employee
- **03/2024** Offering access via marketplace
- **03/2024** Access via Citrix VDI Farm, disabling protection
- **03/2024** Creation of further persistences on unprotected clients, credential dump and data exfiltration
- **01.04.2024** Various notifications by Trend Micro, as well as outgoing phishing and BEC
- **02.04.2024** Encryption of data

Encryption

processFilePath	C:\Users\user\Downloads\amd64.exe
processCmd	C:\Users\user\Downloads\amd64.exe" -pass 5e9f842d111b08ea0d5a4700fda541105dfffc7d6b1e43305fa5ee3eab4dcd509
eventSubId	2 - TELEMETRY_PROCESS_CREATE
objectFilePath	C:\Windows\System32\cmd.exe
objectCmd	cmd.exe /c ""vssadmin.exe Delete Shadows /all /quiet\""

Encryption

>> What happens?

Your data is stolen and encrypted. If you don't pay the ransom, the data will be published on our blog (<http://knight3xppu263m7g4ag3xlit2qxpryjwueobh7vjdc3zrscqlfu3pqd.onion>). Keep in mind that once your data appears on our blog, it could be bought by your competitors at any second, so don't hesitate for a long time.

>> How to contact with us?

1. Download and install TOR Browser (<https://www.torproject.org/>). [If you don't know that, Google search!]

2. Open

<http://f3r6nz2bopxnotodfcp4qztpr3mmapnkioa3ho7j2cuovb32nlf3zcyd.onion/621d81ec62c879476a39fb0bde5735ce7c95e59d562bdcf2e48b9dd90a4a3d1fa6dae6e1d655248cd12d6ba66f5b5a15/>

>>> Warning! Recovery recommendations.

Do not MODIFY or REPAIR your files, Or they will be lost forever.

Do not hire a recovery company. Can't solve anything without us, They always think they're expert negotiators, but the truth is they don't care about you and business

Do not report to the Police, FBI, They don't care about your business and it's going to get worse. (You could be hit with a hefty fine.)

Chronology

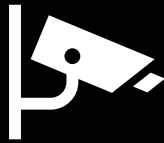
- **01/2024** Spear Phishing of a marketing employee
- **03/2024** Offering access via marketplace
- **03/2024** Access via Citrix VDI Farm, disabling protection
- **03/2024** Creation of further persistences on unprotected clients, credential dump and data exfiltration
- **01.04.2024** Various notifications by Trend Micro, as well as outgoing phishing and BEC
- **02.04.2024** Encryption of data
- **02.04.2024** Incident Response

Important counter measures



Tamper Prot.

Endpoint Security
Agent Protection



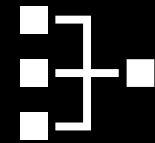
24x7 SecMon

Threat Detection
Monitoring &
Alerting



EDR

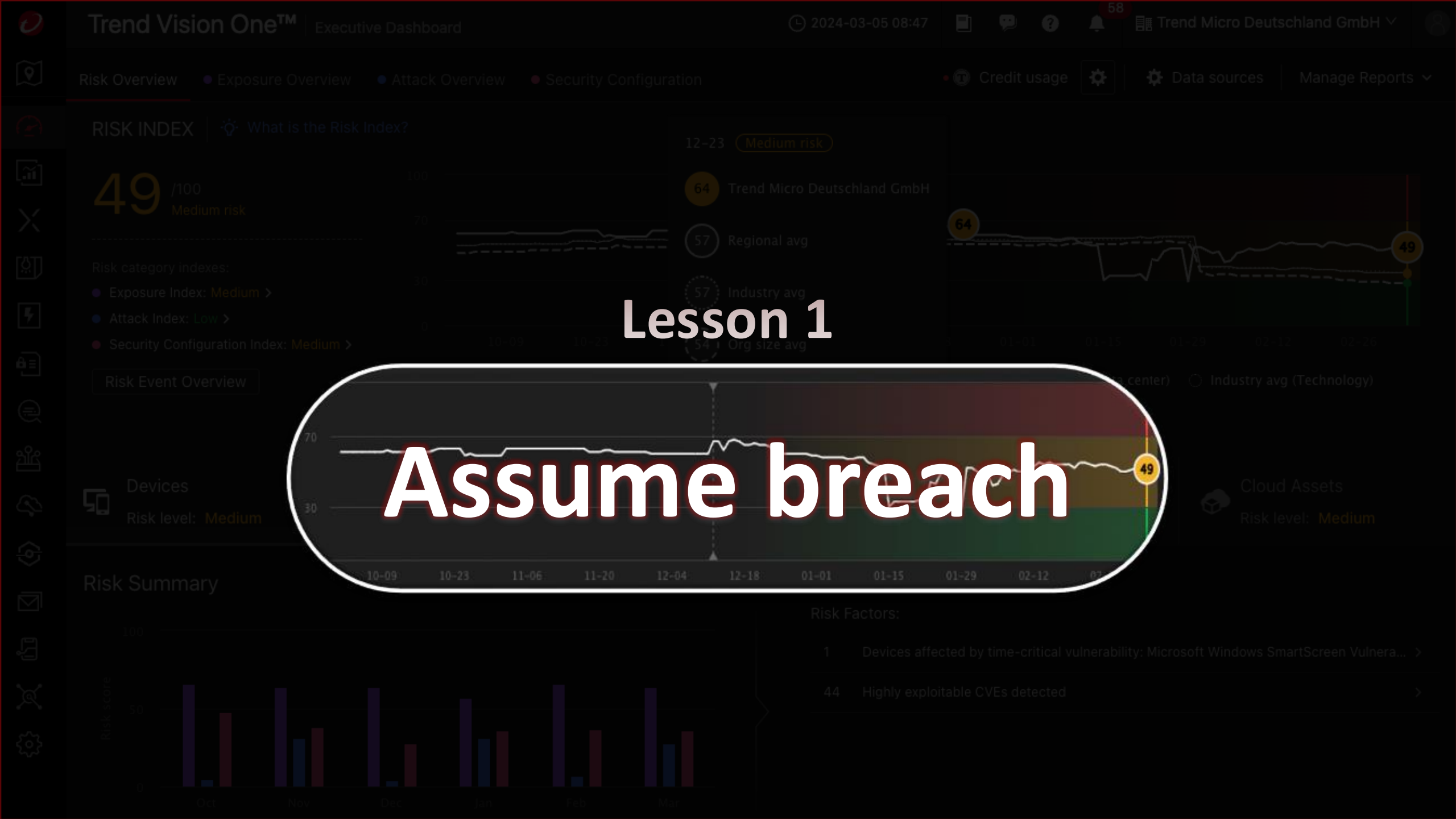
Endpoint Detection
& Response
(ID,RA,CD,PtH,ENC)



NDR

Network Detection
& Response
(PS,LA,DL)

Step 3: lessons learned



Assume Breach

Foster transparency: Collect and analyze telemetry & logs centrally with 24x7 alerting

Define, test and optimize incident plans: Keep your incident processes up to date and be aware of the steps required

Backup, Backup, Backup: Be prepared for full restoration; keep in mind to do offline backups and test the restore frequently

Important: This is a "Pre-release" feature and is not considered an official release. Please review the [Pre-release Disclaimer](#) before using the feature.

New Threat 2023-12-12

Type: Cybercrime AKA: Lockbit

Water Selkie

The **LockBit** intrusion set, tracked by Trend Micro as **Water Selkie**, has one of the most active ransomware operations today.

Campaign Overview:...

[Learn more](#)

Last seen: Any time ▾

Matched result: All ▾

Type: All ▾

Targeted country: All ▾

Targeted industry: All ▾

🔍 Search

Lesson 2

Top targeted country

United States of ...
India
United Kingdom o...
Thailand
Japan



Top targeted industries



Top matched alerts

No Workbench
matched to Ca
Intelligence tra
threats

Threat

Threat status

AKA

Type

Impact scope

Last seen

Water Selkie

Active

Lockbit

Cybercrime

📄 0 🖨 0 📊 0

Decemb

TargetCompany Ransomware

Active

Fargo, Mallox, TargetComp, Xollam

Cybercrime

📄 0 🖨 0 📊 0

Decemb

Pawn Storm

Active

APT28, Fancy Bear, Group 74, IRON TWILIGHT, ...

APT

📄 0 🖨 0 📊 0

Decemb

Total: 83

10 per page ^

< 1

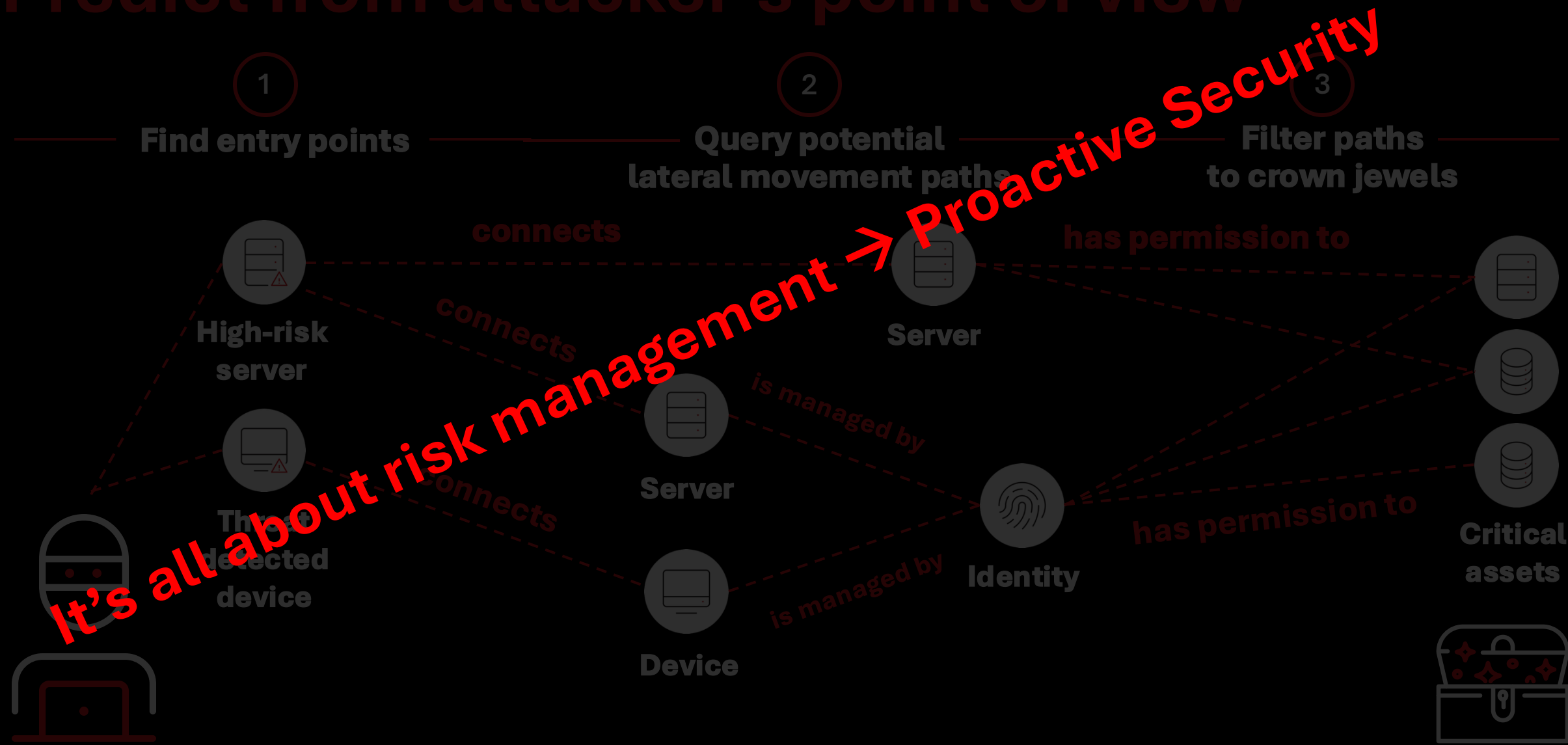
2

3

4

5

Predict from attacker's point of view



Important: This is a "Pre-release" feature and is not considered an official release. Please review the [Pre-release Disclaimer](#) before using the feature.

New Threat 2023-12-12

Type: Cybercrime AKA: Lockbit

Water Selkie

The LockBit intrusion set, tracked by Trend Micro as **Water Selkie**, has one of the most active ransomware operations today.

Campaign Overview:...

[Learn more](#)

Last seen: Any time

Matched result: All

Type: All

Targeted country: All

Targeted industry: All

🔍 Search

Lesson 3

Top targeted country



Top targeted industries



Top matched alerts

No Workbench matched to Campaign Intelligence threats

Threat

Threat status

AKA

Type

Impact scope

Last seen

Water Selkie

Active

Lockbit

Cybercrime

0 0 0 0

Decemb

TargetCompany Ransomware

Active

Fargo, Mallox, TargetComp, Xollam

Cybercrime

0 0 0 0

Decemb

Pawn Storm

Active

APT28, Fancy Bear, Group 74, IRON TWILIGHT, ...

APT

0 0 0 0

Decemb

Total: 83

10 per page

1

2

3

4

5

Processes

Know your processes: Who, how and when will be alerted by the SecOps team? Take in consideration to do a „kill switch“ of a production chain/facility

Test your processes: Conduct frequent critical incidents by red teaming activities incl. test restoration e.g. of a whole AD forest

Update your processes: Embrace continuous learning of test results and implement the improvements