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

https://cyberscoop.com/ai-ransomware-promptlock-nyu-behind-code-discovered-by-security-researchers/

Step 1: the right victim

Size doesn’t matter

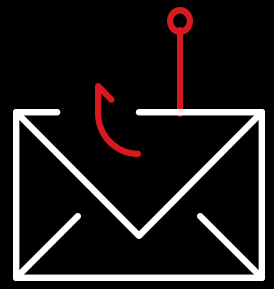
800 employees

24x7 production

Cloud usage

No SOC

Most-seen initial access techniques



Phishing

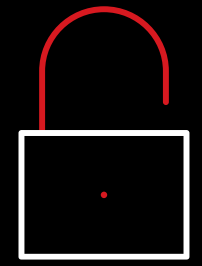
Targeting credentials

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

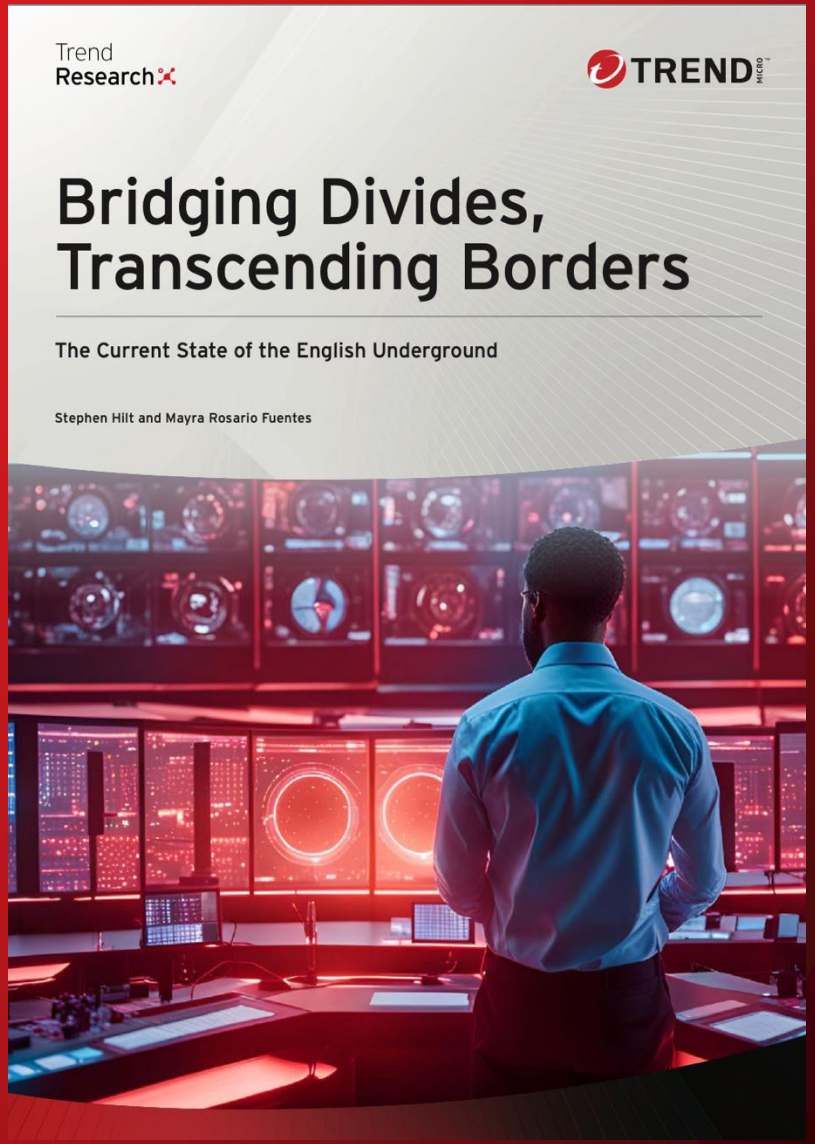
11/2023 Spear Phishing of a marketing employee

01/2024 Offering access via marketplace

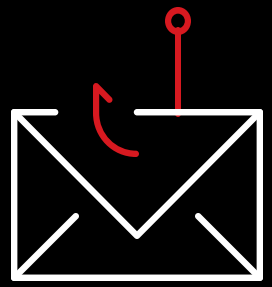
Initial access often outsourced to access brokers

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

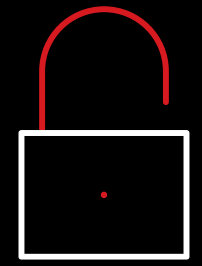
Proper Email Security (BEC)

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

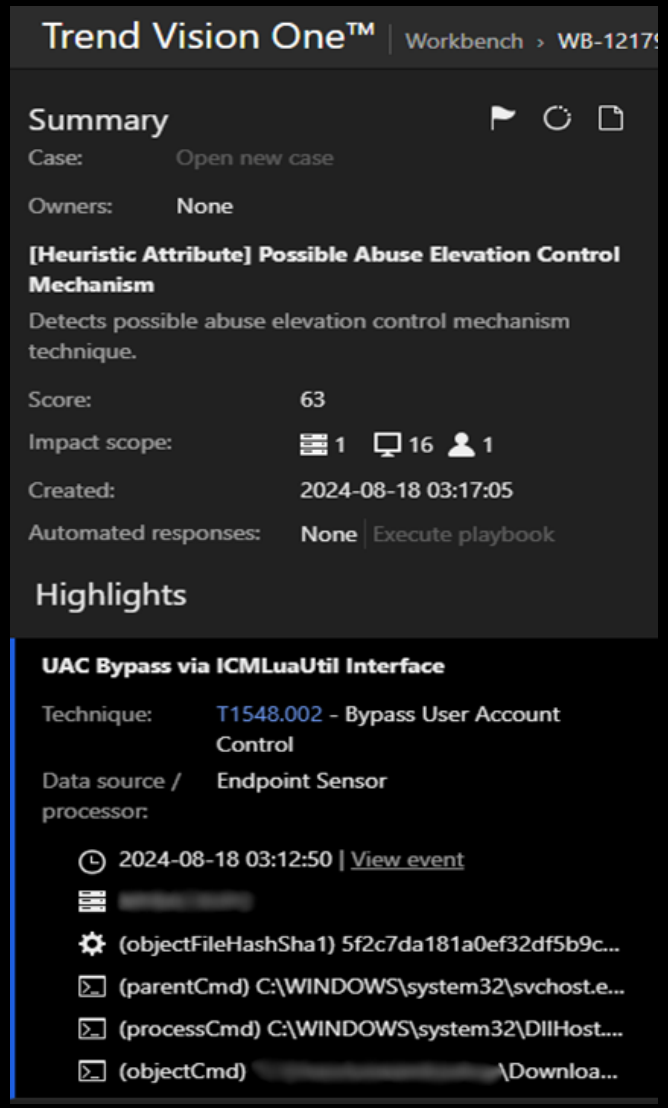
Proper Web Controls (e.g. block of uncat. sites)

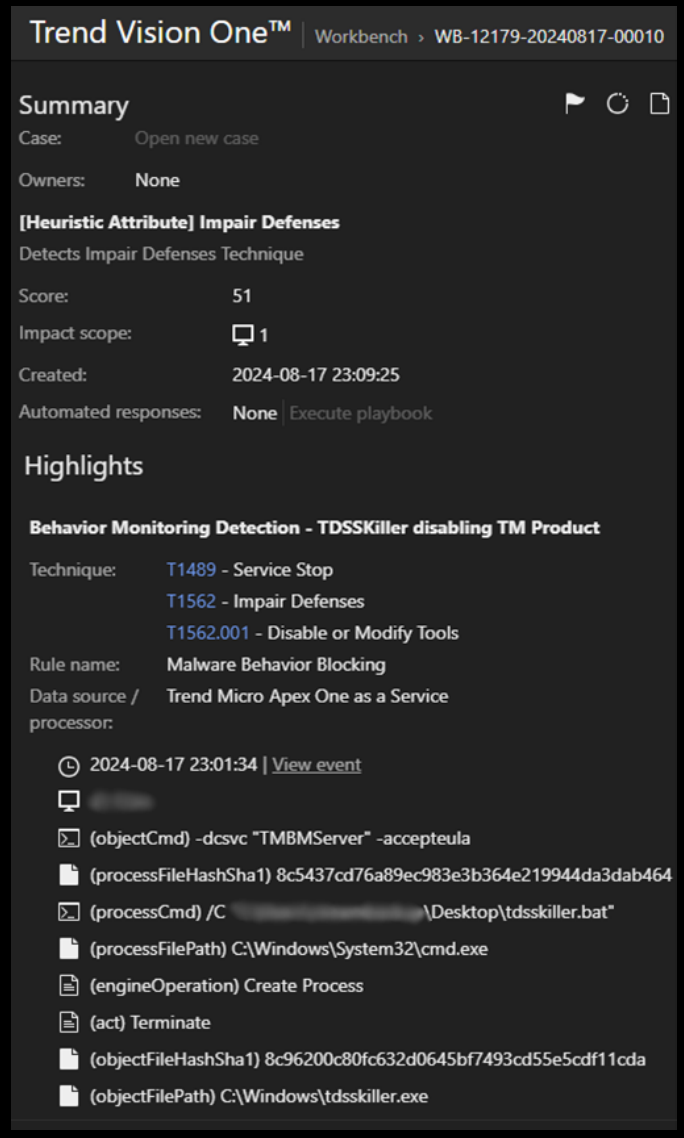
Step 2: the implementation

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





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:

[redacted]\Downloads\softportable_netscan\netscan.exe

CLI command:

[redacted]\Downloads\softportable_netscan\netscan.exe"

File SHA-1:

e38082ae727aeaef4f241a1920150fdf6f149106

File SHA-256:

d1347f4dccebf2fcd672dcef9c66c91b9d3f12b9881e3e390626927718fda6...

File MD5:

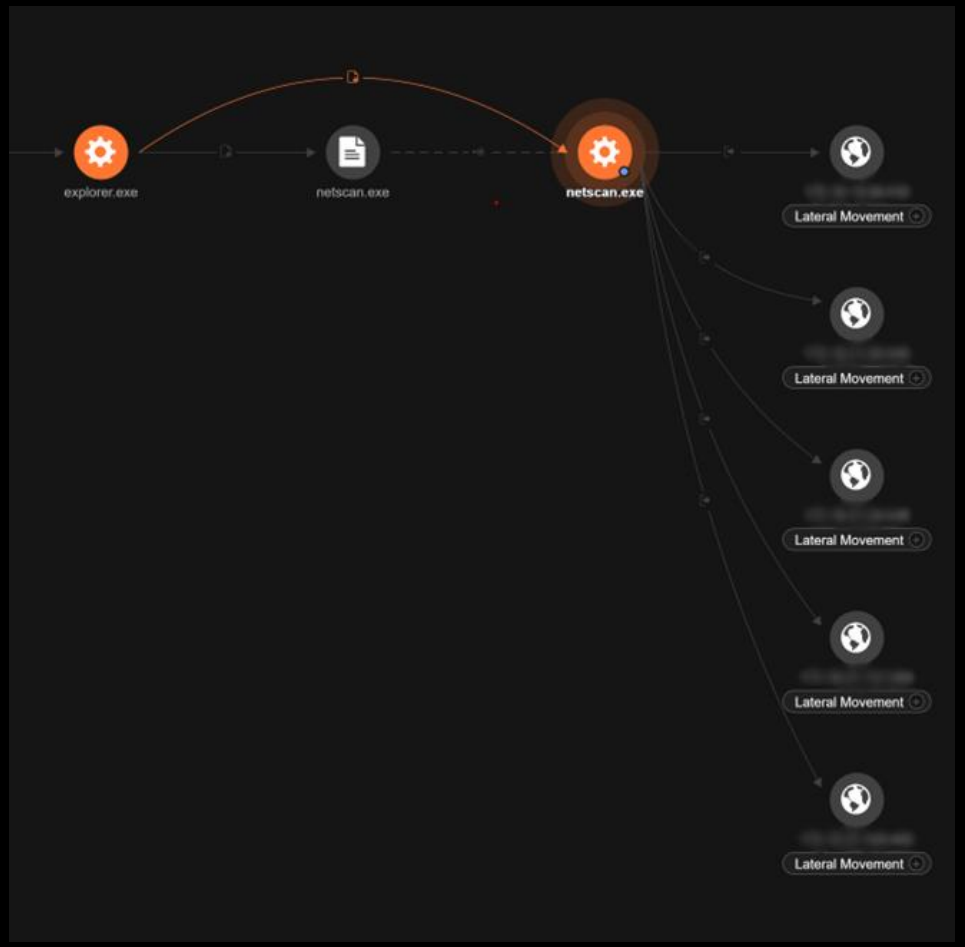
719ba3d7051173982919d1e4e9e9a0ec

Process ID:

9804

Signer:

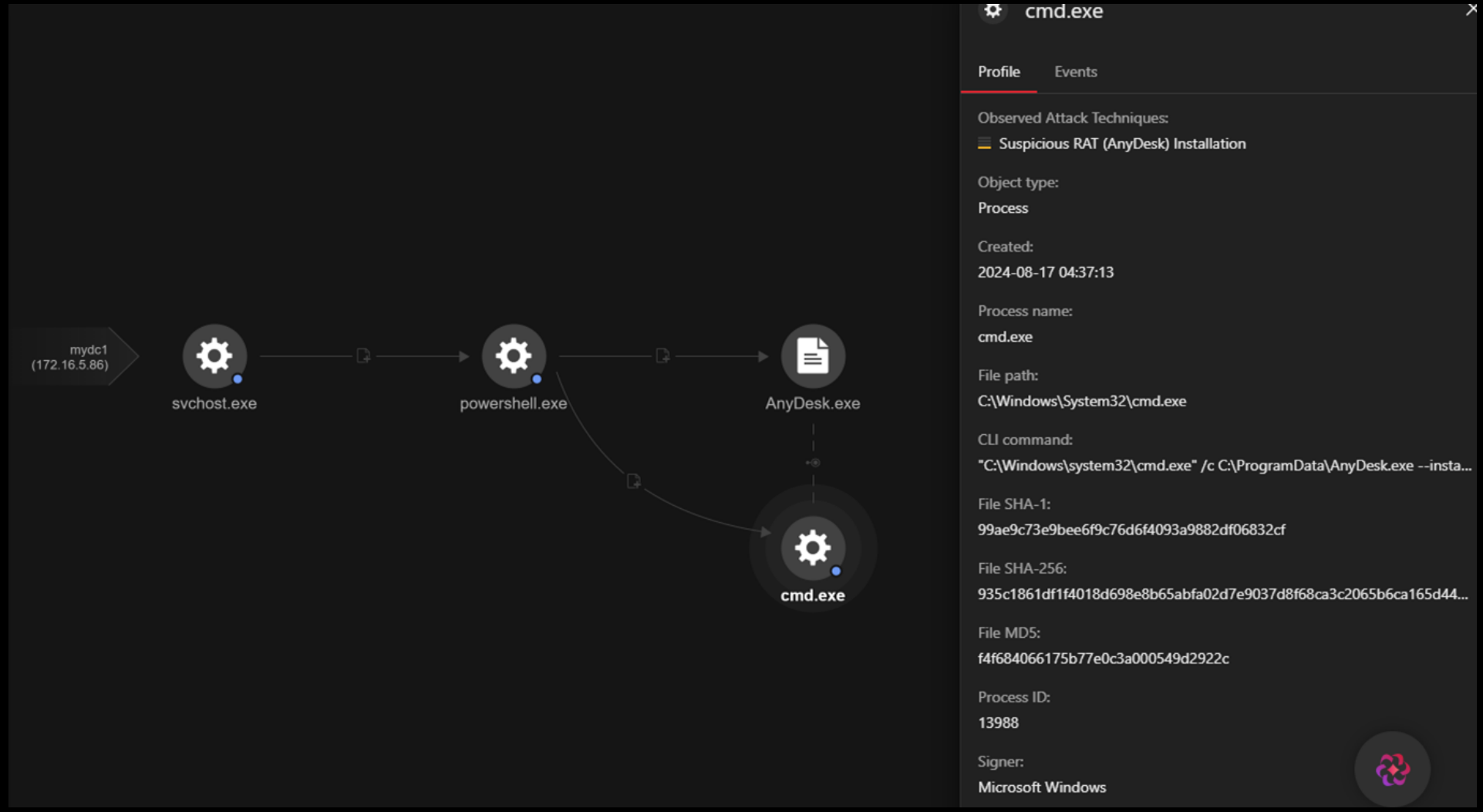
SoftPerfect Pty. Ltd., SoftPerfect Pty. Ltd.



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

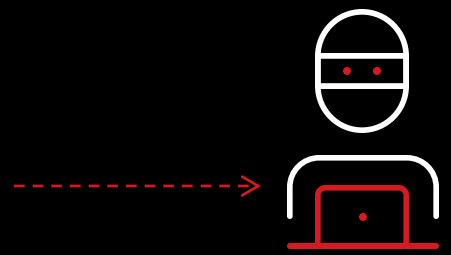
Remote Access



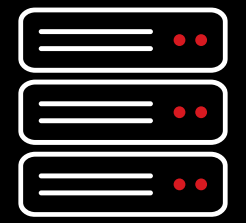
Password hash cracking is now faster/cheaper

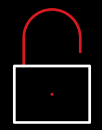
Windows Password Hashes obtained by an attacker

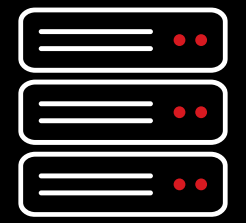
```
8846F7EAEE8FB117AD06BDD830B7586C
E10ADC3949BA59ABBE56E057F20F883E
B7E0F58E067DC79A3EED1C68476C681C
682C99035B38A3B9A9F40D369D42F482
B0D32D0DA05AEBE8706F7DF6B1D58E4F
3328f34bd5d9e61fcbc97a8809492848
2a86a9e0313b84a8ccd94a36ee99f7fa
25fd70cd5ae456a1c76cf0db0f1529d4
1559133a36298127a58cd505965b0f64
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...

TREND MICRO

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	[redacted]\Downloads\amd64.exe
processCmd	[redacted]\Downloads\amd64.exe" -pass 5e9f842d111b08ea0d5a4700fda541105dffc7d6b1e43305fa5ee3eab4dcd509
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/621d81ec62c879476a39fb0bde573
5ce7c95e59d562bdcf2e48b9dd90a4a3d1fa6dae6e1d655248cd12d6ba66f5b5a15/
>>> 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.

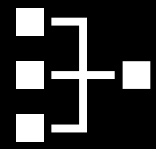
Endpoint Security Agent Protection

24x7 SecMon

Threat Detection Monitoring & Alerting

EDR

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



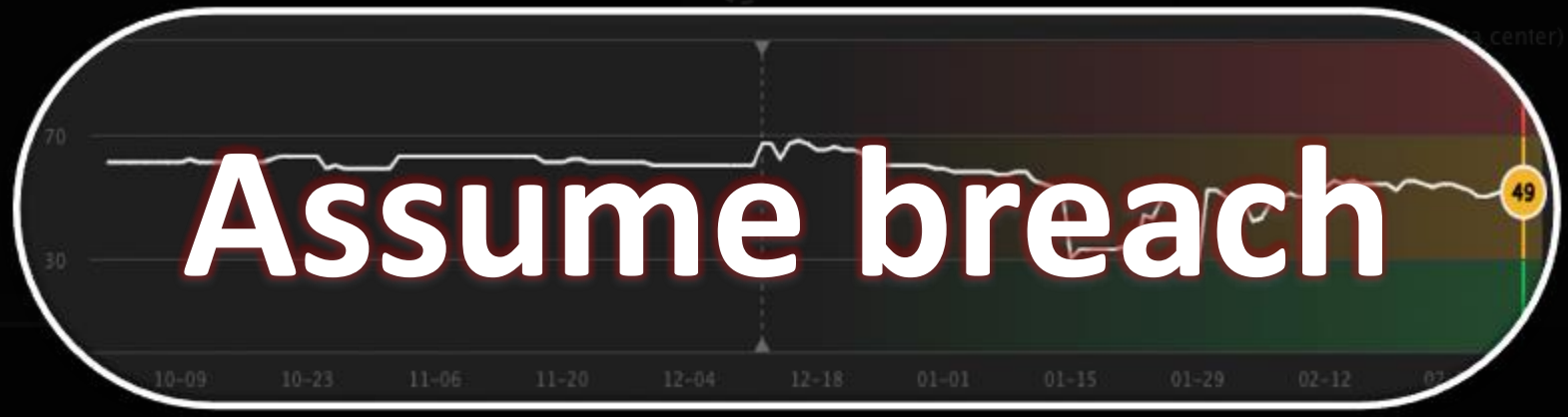
NDR

Network Detection & Response (PS,LA,DL)

Step 3: lessons learned

Lesson 1

Assume breach



Assume Breach

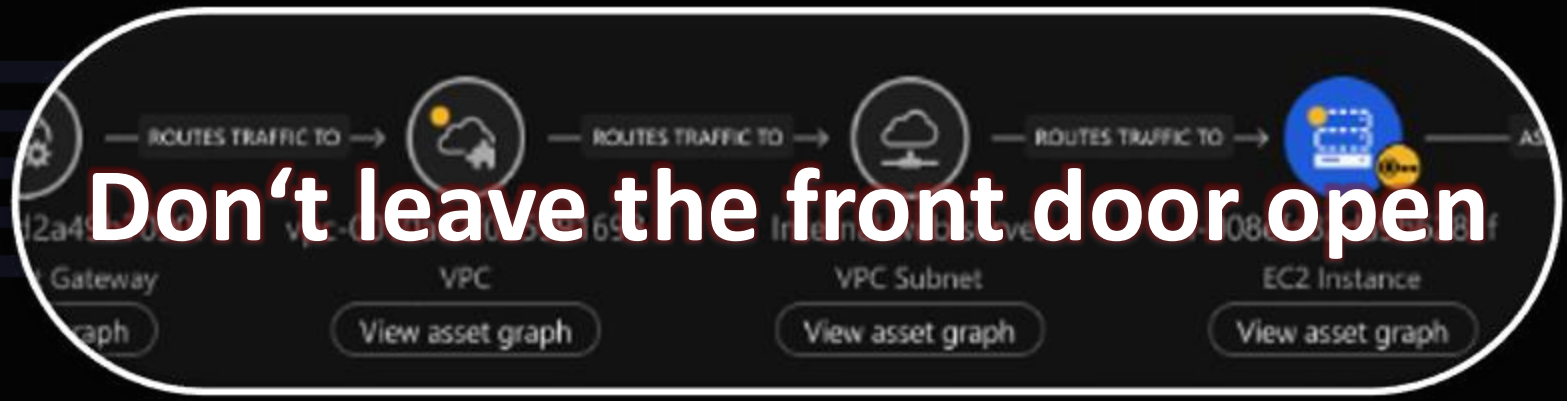
Foster transparency: Collect and analyze telemetry & logs centrally with 24x7 alerting

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

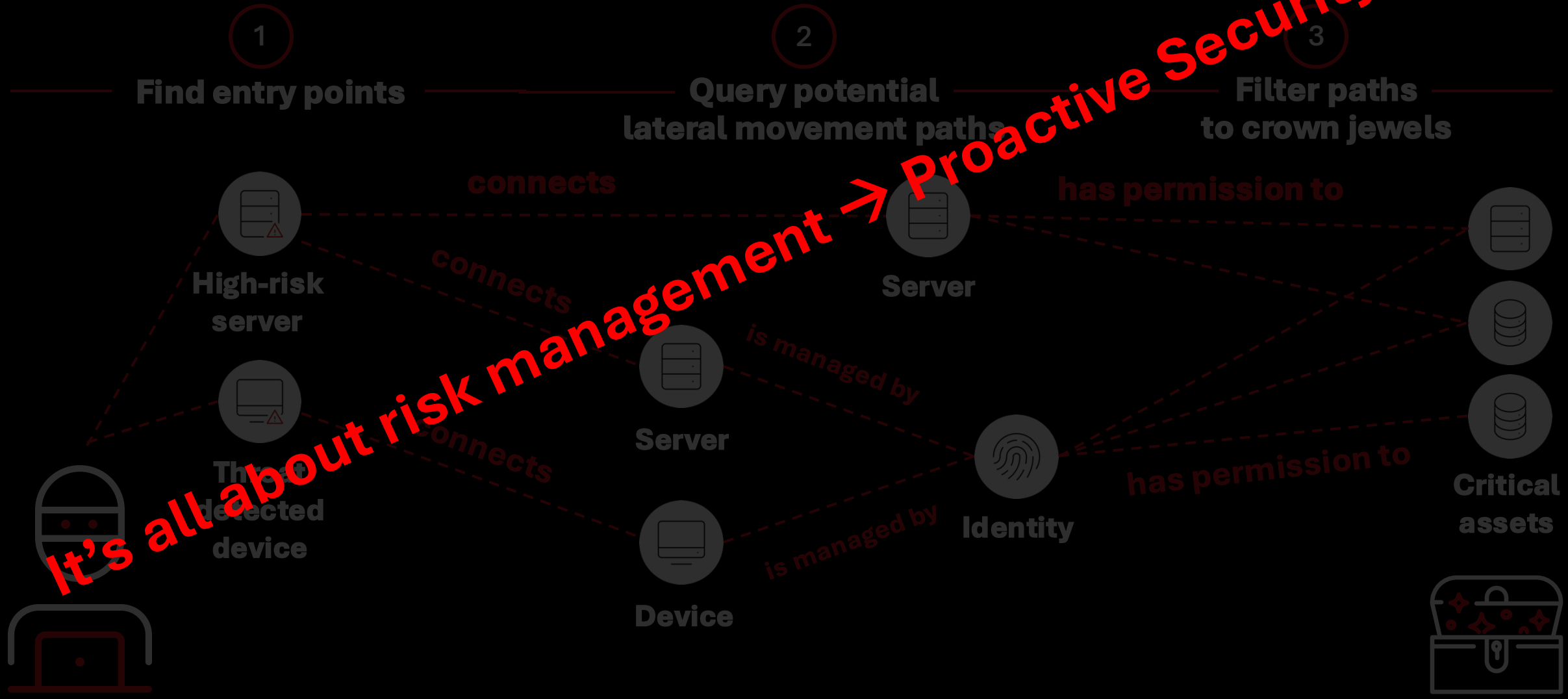
Backup, Backup, Backup: Be prepared for full restoration; keep in mind to do offline backups and test the restore frequently

Lesson 2

Don‘t leave the front door open



Predict from attacker's point of view



It's all about risk management → Proactive Security

Lesson 3

Processes

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