Anti-Forensics

You are doing it wrong (Believe me, I'm an IR consultant)

2025/010/21

/Stephan Berger – whoami

- Head of Investigations at InfoGuard
- @malmoeb on all platforms
- I blog, too (dfir.ch)

- Original Anti-Forensics talk is 200+ slides - short excerpt today 😬


Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
Mandatory Introduction

The Hackers Choice, published in 1995

InfoGuard
SWISS CYBER SECURITY

```
##############################################
#                                            #
#          HOW TO COVER YOUR TRACKS          #
#                                            #
##############################################
```

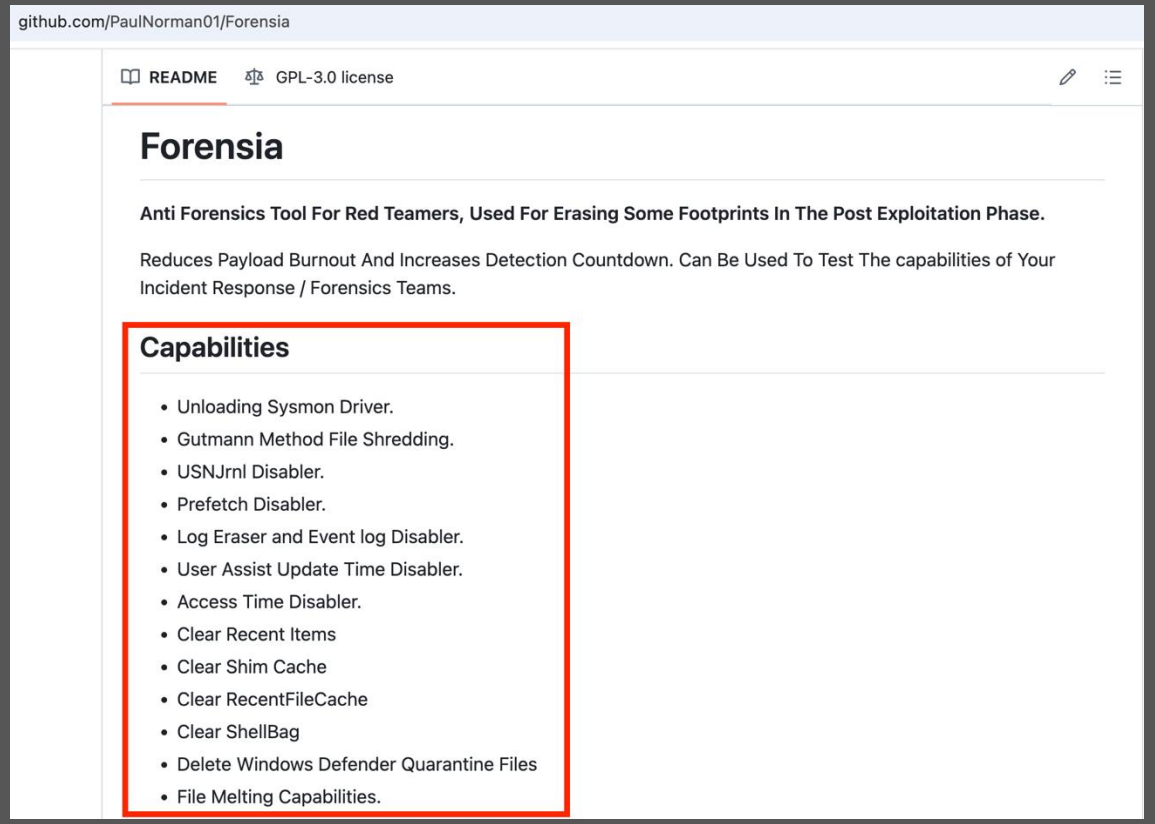
PART ONE : THEORY & BACKGROUND

I. INTRODUCTION
II. MENTAL
III. BASICS
IV. ADVANCED
V. UNDER SUSPECT
VI. CAUGHT
VII. PROGRAMS
VIII. LAST WORDS

Forensia

“Can Be Used To Test The capabilities of Your Incident Response / Forensics Teams.”

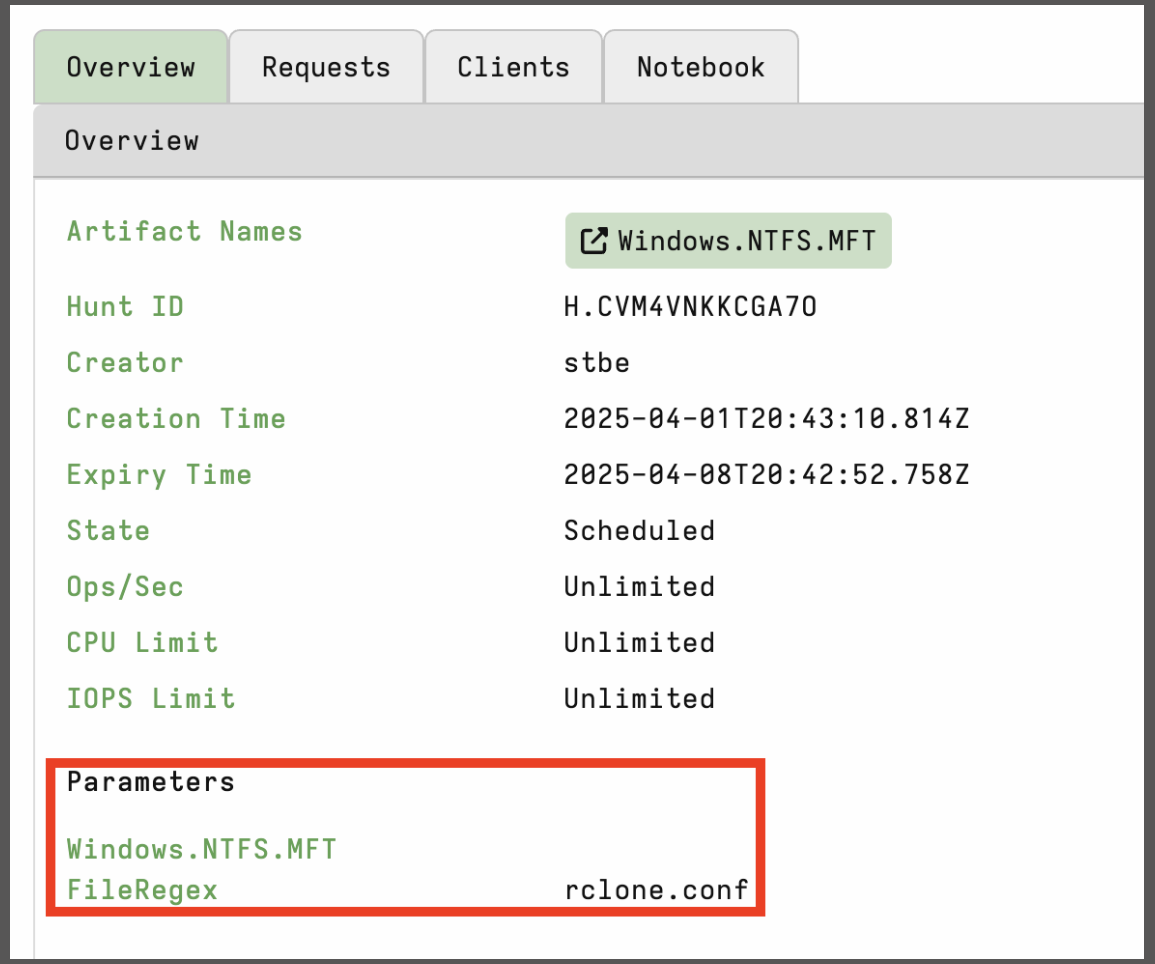
Challenge accepted ;)




Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
Cover your tracks

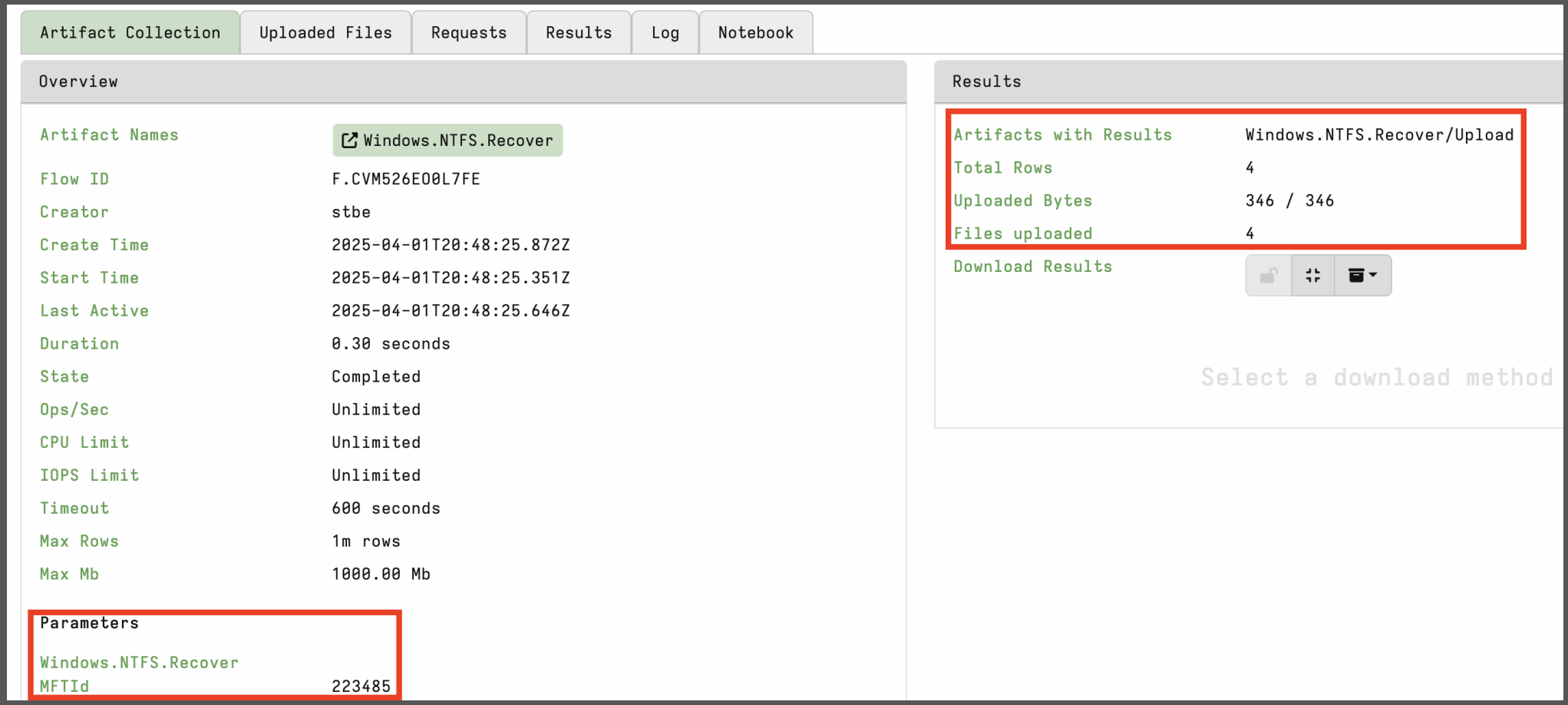
Plain and simple – Delete the file

- When you delete a file on **NTFS**, the data isn't immediately erased.
- Instead, the **MFT entry** (which contains metadata like filename, timestamps, and pointers to data) is marked as available.
- The actual data blocks on disk and the MFT record may remain intact until overwritten by new data.
- **rclone**: Loved by ransomware groups to exfiltrate data.



NFTS Recover

- The search returned some hits, and provided us with the **MFTId**, the ID of the file on the Master File Table.



Recovered rclone.conf

- We recovered the configuration file for rclone! - **Cleartext credentials to the attacker's server!**

Artifact Collection | Uploaded Files | Requests | Results | Log | Notebook

0-4/4 | 10

Timestamp	started	vfs_path	Type	file_size	uploaded_size	Preview
1743540507	2025-04-01 20:48:27.005576375 +0000 UTC	\\.\C:\<Err>\<Parent 220671-12 need 11>\rclone.conf\223485-14-8		72	72	®> ¡Û ¯ JT ¡Û òûBù...
1743540507	2025-04-01 20:48:27.005779039 +0000 UTC	\\.\C:\<Err>\<Parent 220671-12 need 11>\rclone.conf\223485-48-4		88	88	ÿ] ¯ JT-¡Û ¯ JT...
1743540507	2025-04-01 20:48:27.005958863 +0000 UTC	\\.\C:\<Err>\<Parent 220671-12 need 11>\rclone.conf\223485-48-5		90	90	ÿ] ¯ JT-¡Û ¯ JT...
1743540507	2025-04-01 20:48:27.006113189 +0000 UTC	\\.\C:\<Err>\<Parent 220671-12 need 11>\rclone.conf\223485-128-1		96	96	[mega1] type = mega...

Download file.

More deleted files fun

USN Journal

InfoGuard
SWISS CYBER SECURITY

- The USN Journal, short for **Update Sequence Number Journal,** is a feature of the NTFS file system that logs changes to files and directories on a volume.

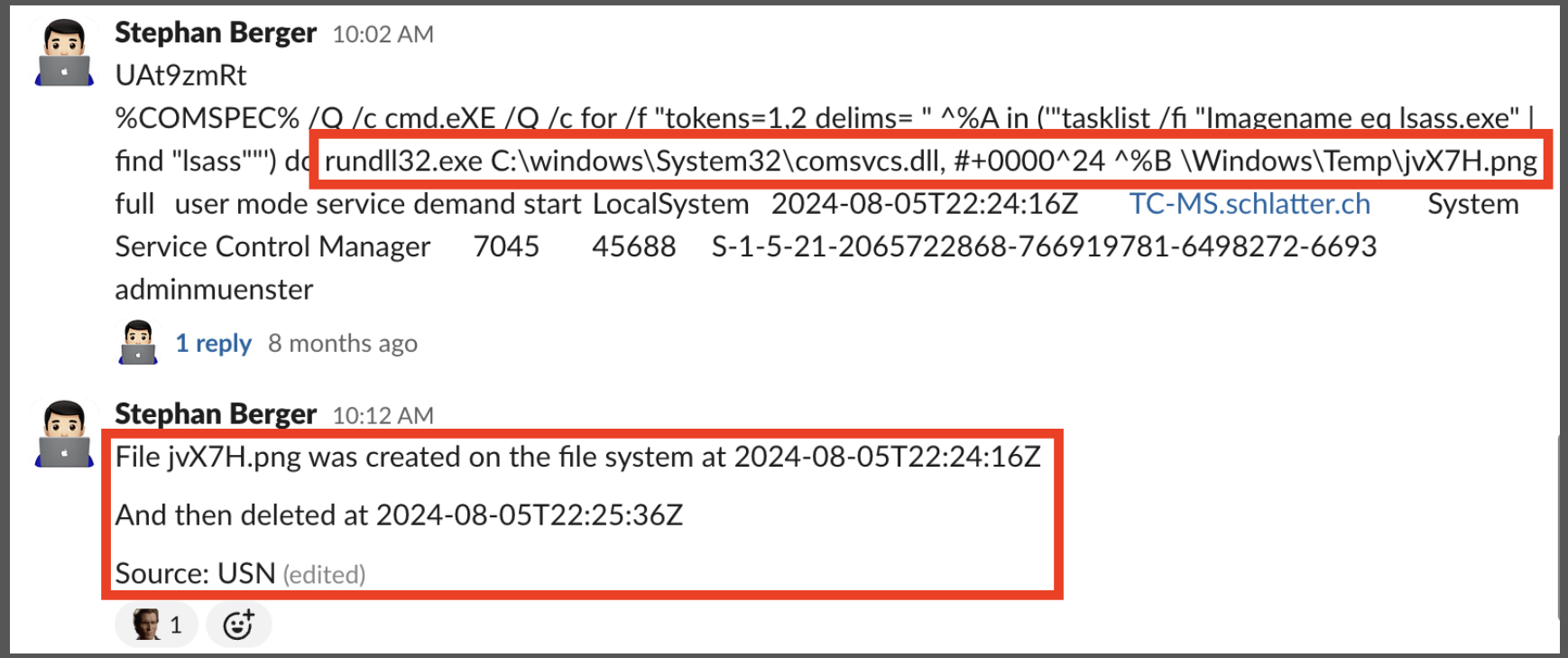
- **Creation, Deletion, Modification, Renaming**.

- The journal is circular and has a size limit, so old entries eventually get overwritten.

- **But depending on how active the system is and how big the journal is configured to be, it can retain weeks or even months of change history.**

USN Journal

- From a forensics perspective, the USN Journal is incredibly valuable.
- It can contain records of files that were deleted or renamed, even if those files are no longer present on the drive. Example here, **jvX7H.png is an LSASS dump** (and deleted..).



Disable / Delete the USN Journal

InfoGuard
SWISS CYBER SECURITY

```
fsutil usn deletejournal /d C:
```

Before:

Results

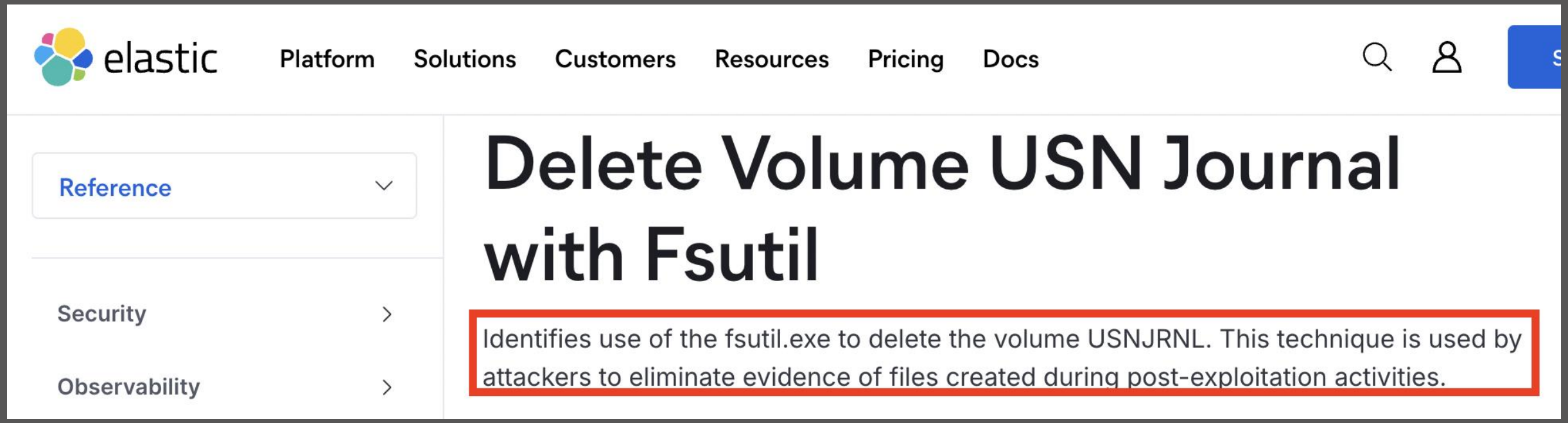
Artifacts with Results	Windows.Forensics.Usn
Total Rows	24
Uploaded Bytes	0 / 0
Files uploaded	0

After:

Results

Artifacts with Results	
Total Rows	0
Uploaded Bytes	0 / 0
Files uploaded	0

Detection


elastic
Platform
Solutions
Customers
Resources
Pricing
Docs
Reference
Security
Observability
Delete Volume USN Journal with Fsutil
Identifies use of the fsutil.exe to delete the volume USNJRNL. This technique is used by attackers to eliminate evidence of files created during post-exploitation activities.


Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
SRUM

Detection

InfoGuard
SWISS CYBER SECURITY

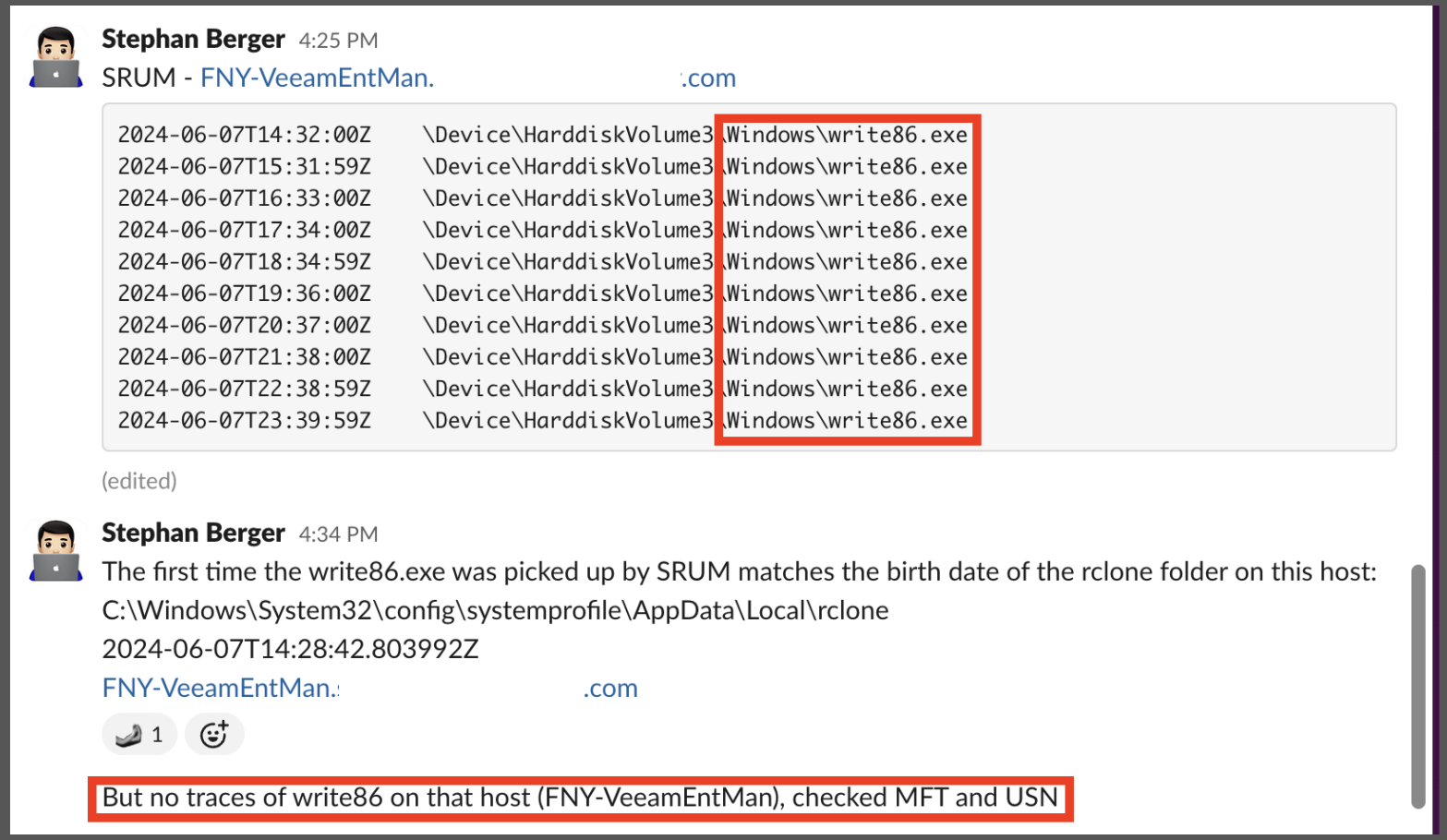
- Remember the screenshot before from Forensia? Purge as much traces as possible?

- SRUM (**System Resource Usage Monitor**) is a built-in Windows feature that tracks detailed **system and application resource usage**, storing this data in a database.

- The database not only logs process execution but also provides insights into CPU, memory, and network activity, **creating a distinct timeline of events that can confirm what was run.**

Detection

- **write86.exe** is rclone (again). MFT and USN shows no sign of this binary. Extremely useful in investigations (evidence of execution).

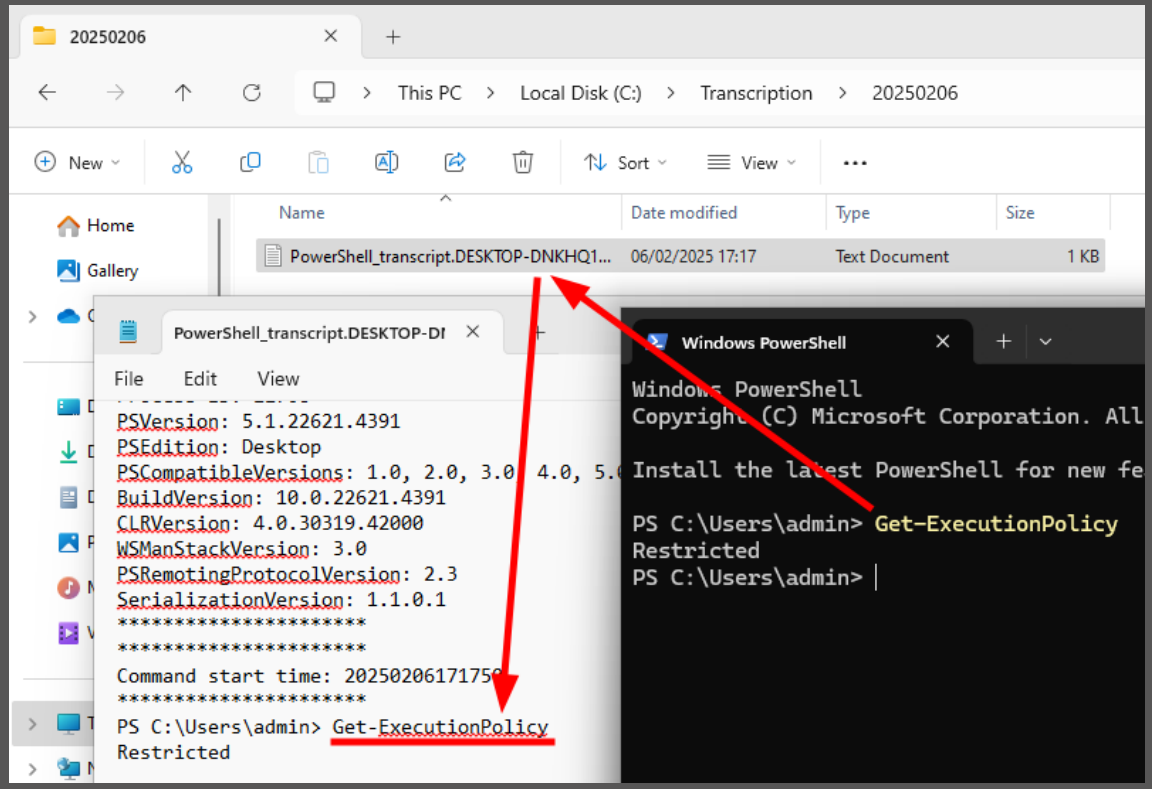



Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
PowerShell

PowerShell Transcript

- **PowerShell Transcript** is a feature that records the entire input and output of a PowerShell session, which is especially useful for auditing, troubleshooting, and security monitoring.

- Yes, might leak secrets, too.



Console_History

InfoGuard
SWISS CYBER SECURITY

- The **PSReadLine** module tracks commands used in all PowerShell sessions and writes them to a file.
- Data exfil preparation from a recent case:

```
3: $filesDir1 = 'D:\Group_FR'
4: $rarDir = "D:\O365\SACT"
5: $archiveName = Join-Path $rarDir (Get-Random -max 9999999999 -min 999999999)
6: & "C:\Program Files\WinRar\Rar.exe" a -r -ep1 -v1g -n*pdf -n*doc -n*docx -n*xls -n*xlsx
-n*txt -ta20240101000000 -tb20260101000000 -sl200000000 -ed "$archiveName" "$filesDir1\*"

7: $filesDir1 = 'D:\Group_FR\01_BE'
8: $rarDir = "D:\O365\SACT"
9: $archiveName = Join-Path $rarDir (Get-Random -max 9999999999 -min 999999999)
10: & "C:\Program Files\WinRar\Rar.exe" a -r -ep1 -v1g -n*pdf -n*doc -n*docx -n*xls -
n*xlsx -n*txt -ta20240101000000 -tb20260101000000 -sl200000000 -ed "$archiveName"
"$filesDir1\*"

11: $filesDir1 = 'D:\Group_FR\04_COMMERCIAL'
12: $rarDir = "D:\O365\SACT"
13: $archiveName = Join-Path $rarDir (Get-Random -max 9999999999 -min 999999999)
14: & "C:\Program Files\WinRar\Rar.exe" a -r -ep1 -v1g -n*pdf -n*doc -n*docx -n*xls -
n*xlsx -n*txt -ta20240101000000 -tb20260101000000 -sl200000000 -ed "$archiveName"
"$filesDir1\*"
```

Tampering with the History file

InfoGuard
SWISS CYBER SECURITY

- Change where these logs are saved using `Set-PSReadLineOption -HistorySavePath {File Path}`.
  This will cause **ConsoleHost_history.txt** to stop receiving logs.

- Additionally, it is possible to turn off logging to this file:
  `Set-PSReadlineOption -HistorySaveStyle SaveNothing`

- `Remove-Item -Path $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt`

From Elastic's GitHub Protection Artifacts Repository

InfoGuard
SWISS CYBER SECURITY

protections-artifacts / behavior / rules / windows / **defense_evasion_suspicious_powershell_console_history_deletion.toml**

Code | Blame | 58 lines (50 loc) · 1.76 KB

```
16      (
17       process.name : ("powershell.exe", "rundll32.exe", "regsvr32.exe", "cmd.exe", "wscript.exe", "cscript.exe", "mshta.exe",
18                       "winword.exe", "excel.exe") or
19       process.executable : ("?:\\Users\\*", "?:\\Windows\\Temp\\*", "?:\\ProgramData\\*", "?:\\Windows\\Microsoft.NEt\\*") or
20       (process.code_signature.trusted == false or process.code_signature.exists == false)
21      ) and
22      not user.id : ("S-1-5-18", "S-1-5-19")
23      ]
24      [file where event.action == "deletion" and file.name : "ConsoleHost_history.txt"]
25      '''
26
```


Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
BMC

From a recent case

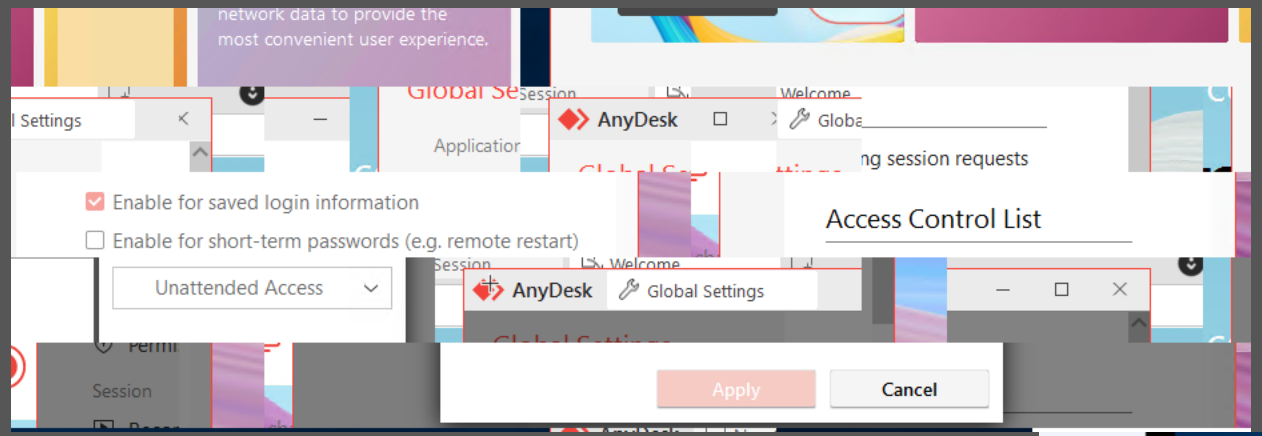
- Deleting registry keys and files related to RDP
- Removing AutomaticDestinations

```
@echo off
reg.exe delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg.exe delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg.exe add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
attrib -s -h %userprofile%\documents\Default.rdp
del %userprofile%\documents\Default.rdp
del /f /s /q /a %AppData%\Microsoft\Windows\Recent\AutomaticDestinations
```

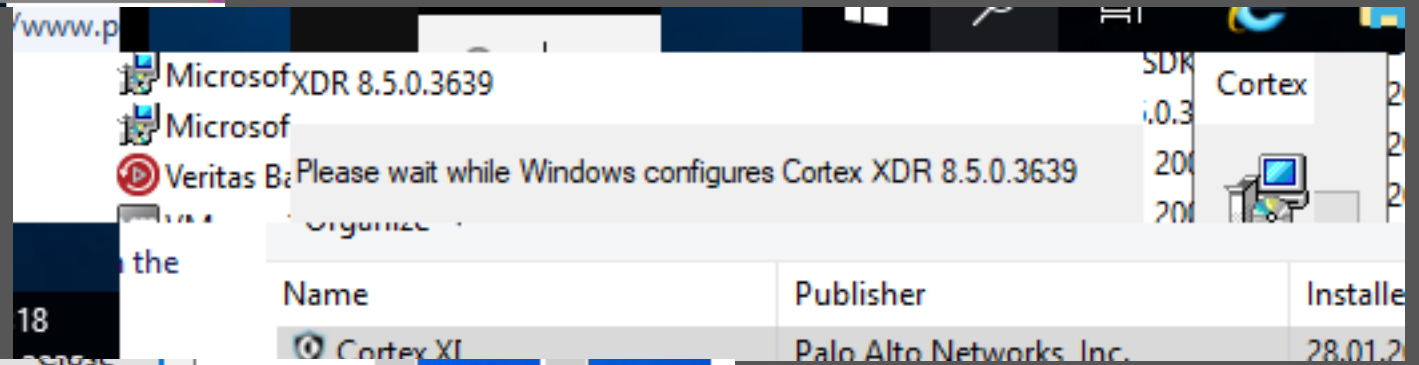
They forgot about the Bitmap Cache

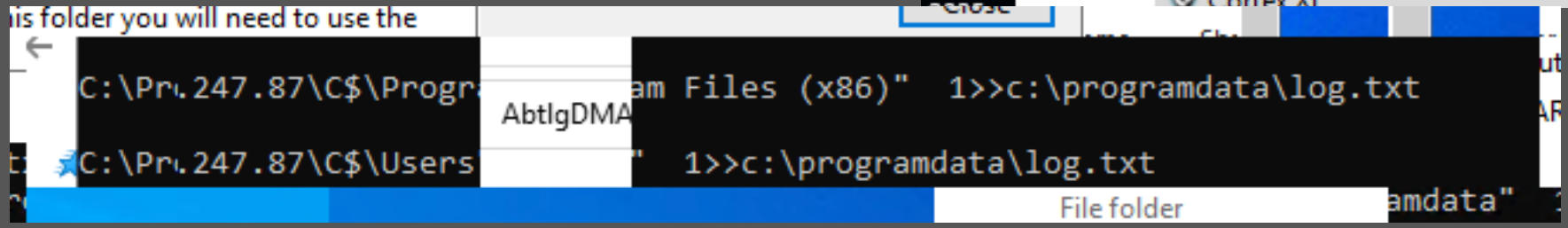
- Bitmap caches are used by the client and server to store graphic bitmaps. Each bitmap cache holds bitmaps of a specified size in pixels (known as the “tile size”).
- Puzzle time! ☺

Zooming in



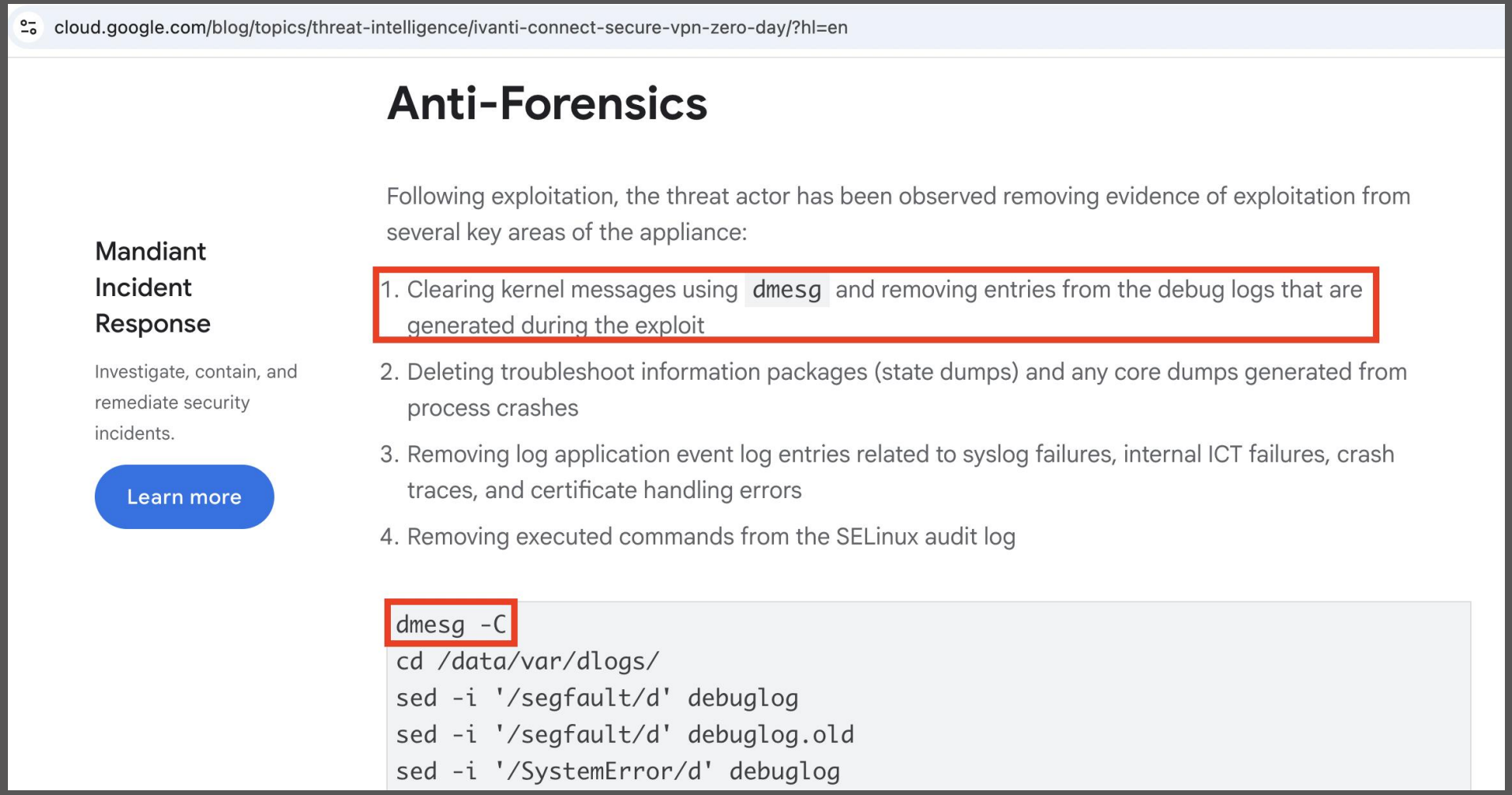
- Evidence of (deleted) files might be visible as well.
- So useful to find staging folders.





Clearing dmesg

Anti-Forensics, Mandiant, January 2025



Anti-Forensics, in action

InfoGuard
SWISS CYBER SECURITY

- First command: I see the loading of a kernel module
- Second command: Traces are gone. But are they?

```
root@anti:~# dmesg
[3448421.426674] dfir: loading out-of-tree module taints kernel.
[3448421.426687] dfir: module verification failed: signature and/or required key missing -
tainting kernel
[3448421.428389] Hello, DFIR!

root@anti:~# dmesg -C && dmesg
root@anti:~#
```

/var/log/kern.log

InfoGuard
SWISS CYBER SECURITY

- Even if one clears logs, there are other places we might find traces of attackers. For example, **/var/log/kern.log** holds also the Kernel messages.

```
root@anti:~# cat /var/log/kern.log

2025-04-23T19:50:49.753460+00:00 anti kernel: dfir: loading out-of-tree module taints kernel.
2025-04-23T19:50:49.753497+00:00 anti kernel: dfir: module verification failed: signature
and/or required key missing - tainting kernel
2025-04-23T19:50:49.754649+00:00 anti kernel: Hello, DFIR!
```

journalctl -k

InfoGuard
SWISS CYBER SECURITY

- Additionally, there's **`journalctl -k`**. It displays kernel logs collected by `systemd-journald`.
- So even if you've cleared `dmesg` and removed `/var/log/kern.log`, the messages will still appear in `journalctl -k`. More about tainted kernels on my blog.

```
root@anti:~# journalctl -k

Apr 23 19:50:49 anti kernel: dfir: loading out-of-tree module taints kernel.
Apr 23 19:50:49 anti kernel: dfir: module verification failed: signature and/or required key
missing - tainting kernel
Apr 23 19:50:49 anti kernel: Hello, DFIR!
```


Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
Clearing Journal

STEELCORGI (Mandiant)

One of the sneakiest commands we noticed is the “bleach” one, able to delete all btmp wtmp and btmp logs. It is also able to clean Syslog logs in /var/log/syslog, /var/log/messages, /var/log/secure and /var/log/auth.log or optionally all of them with the “-A” flag (utmp+wtmp+lastlog+syslog) which is the default.

Is clear that the usage of the “bleach” parameter during an intrusion results in hard times for the DFIR team.

Source: yoroi.company

We still have the Journal (auth, cron etc.)

InfoGuard
SWISS CYBER SECURITY

```
[..]
Apr 16 15:45:48 anti sshd[588615]: Accepted password for root from 178.X port 48679 ssh2
Apr 16 17:49:57 anti sshd[589837]: Accepted password for root from 85.X port 59229 ssh2
Apr 17 12:38:37 anti sshd[601821]: Accepted password for root from 85.X port 60148 ssh2
Apr 17 13:09:41 anti sshd[603434]: Accepted password for root from 85.X port 61884 ssh2

[..]
Mar 17 01:10:07 anti sshd[47992]: Invalid user user from 20.163.71.109 port 50524
Mar 17 01:10:15 anti sshd[47994]: Invalid user ossuser from 20.163.71.109 port 58136
Mar 17 01:11:17 anti sshd[48009]: Invalid user dbuser from 20.163.71.109 port 51794
Mar 17 01:12:20 anti sshd[48024]: Invalid user user from 20.163.71.109 port 39848
```

Clearing the Journal

InfoGuard
SWISS CYBER SECURITY

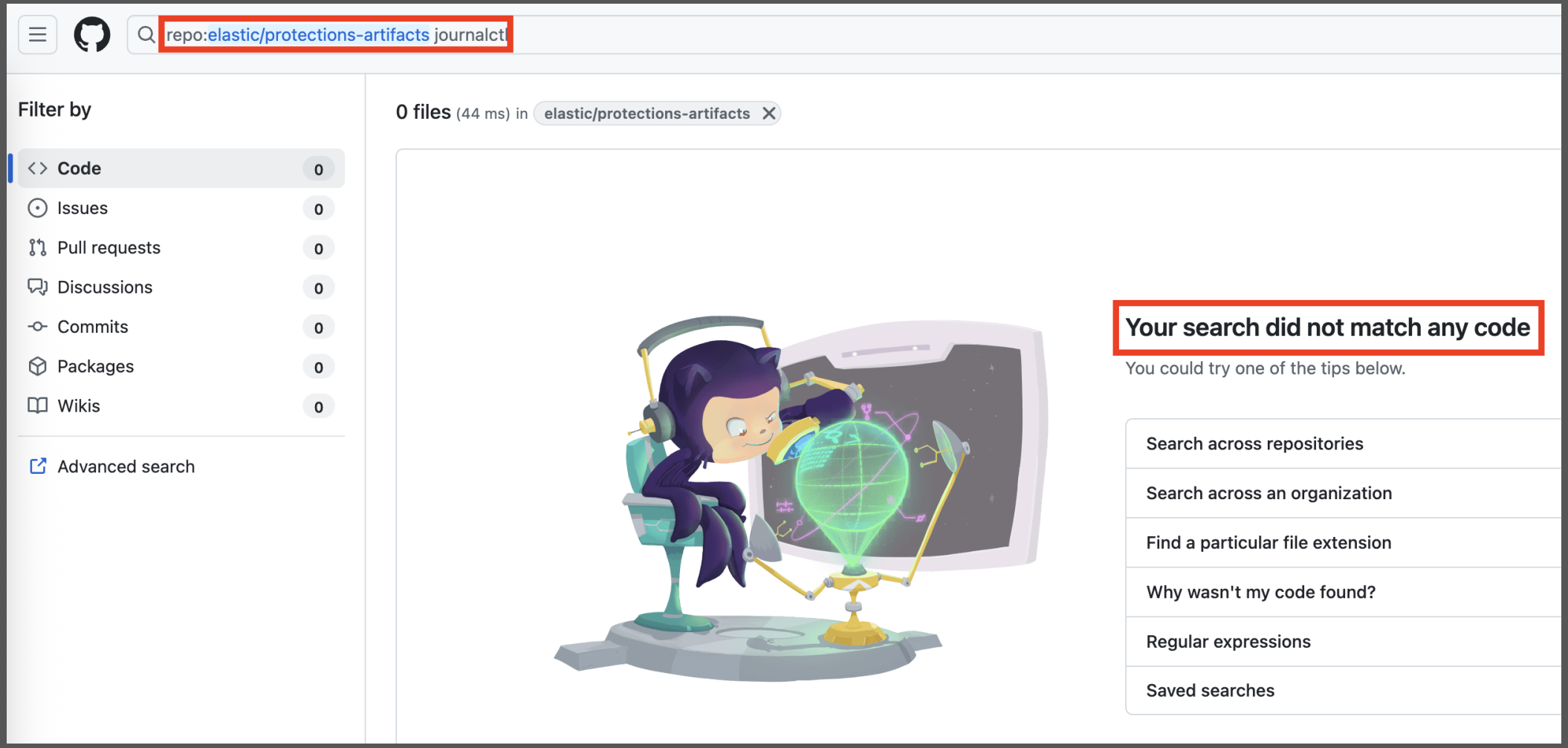
```
# journalctl --rotate
# journalctl --vacuum-time=1s

Deleted archived journal
/var/log/journal/53d3dae872b75fd5b8b4abb067d4a62d/system@75c9cb1517aa471d9bb0d9a7aa75e8ec-
0000000000000edf-0006305bfcaadc70.journal (38.1M).
[..]
system@75c9cb1517aa471d9bb0d9a7aa75e8ec-00000000000cd9e3-000632c7b3335546.journal (37.5M).
Deleted archived journal
/var/log/journal/53d3dae872b75fd5b8b4abb067d4a62d/system@75c9cb1517aa471d9bb0d9a7aa75e8ec-
00000000000da972-000632f4f03b4ff5.journal (10.4M).
Vacuuming done, freed 622.4M of archived journals from
/var/log/journal/53d3dae872b75fd5b8b4abb067d4a62d.
Vacuuming done, freed 0B of archived journals from /var/log/journal.
Vacuuming done, freed 0B of archived journals from /run/log/journal.
```

Clearing logs generates, well.. other logs

InfoGuard
SWISS CYBER SECURITY

```
[2930799.848474] systemd-journald[25627]: Received client request to rotate journal, rotating.
[2930799.863494] systemd-journald[25627]: Vacuuming done, freed 0B of archived journals from
/var/log/journal/53d3dae872b75fd5b8b4abb067d4a62d.
```

However, who will notice anyway :)



Questions?