



Securing  
Your Digital  
World

infoGuard  
SWISS CYBER SECURITY

# 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

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

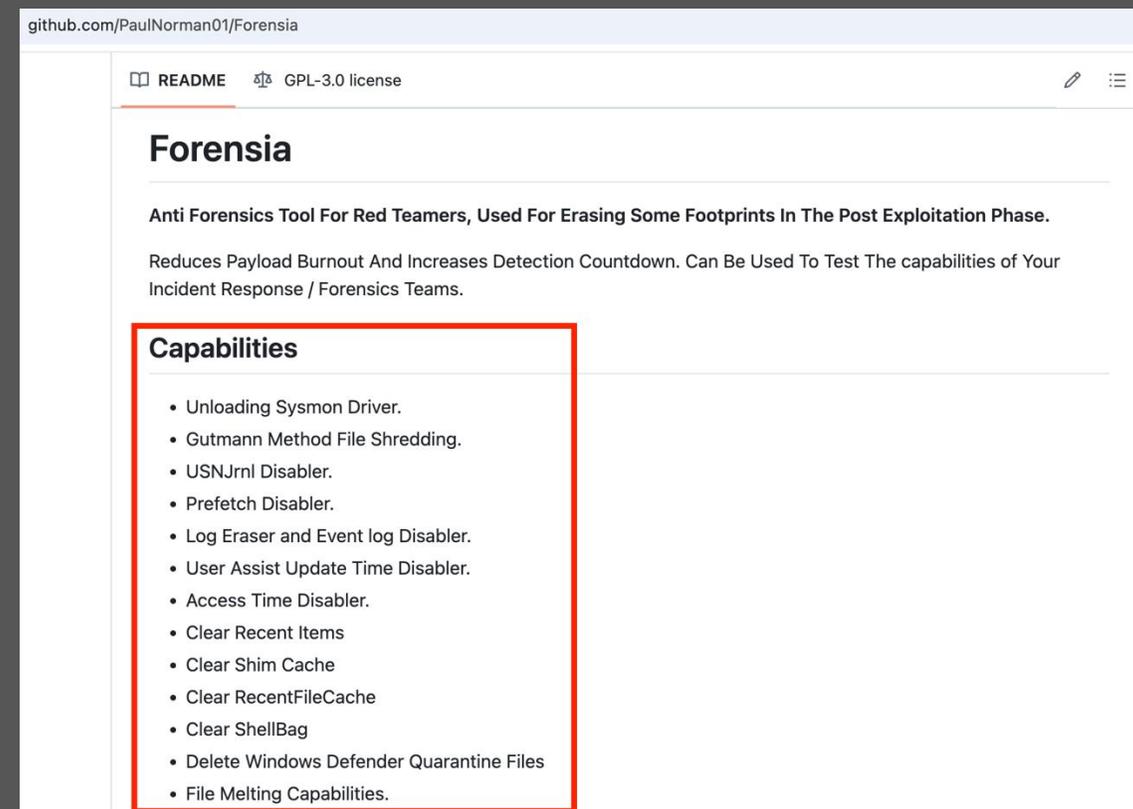
## PART ONE : THEORY & BACKGROUND

- 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 ;)



github.com/PaulNorman01/Forensia

README GPL-3.0 license

## Forensia

Anti Forensics Tool For Red Teamers, Used For Erasing Some Footprints In The Post Exploitation Phase.

Reduces Payload Burnout And Increases Detection Countdown. Can Be Used To Test The capabilities of Your Incident Response / Forensics Teams.

### Capabilities

- Unloading Sysmon Driver.
- Gutmann Method File Shredding.
- USNJrnl Disabler.
- Prefetch Disabler.
- Log Eraser and Event log Disabler.
- User Assist Update Time Disabler.
- Access Time Disabler.
- Clear Recent Items
- Clear Shim Cache
- Clear RecentFileCache
- Clear ShellBag
- Delete Windows Defender Quarantine Files
- File Melting Capabilities.



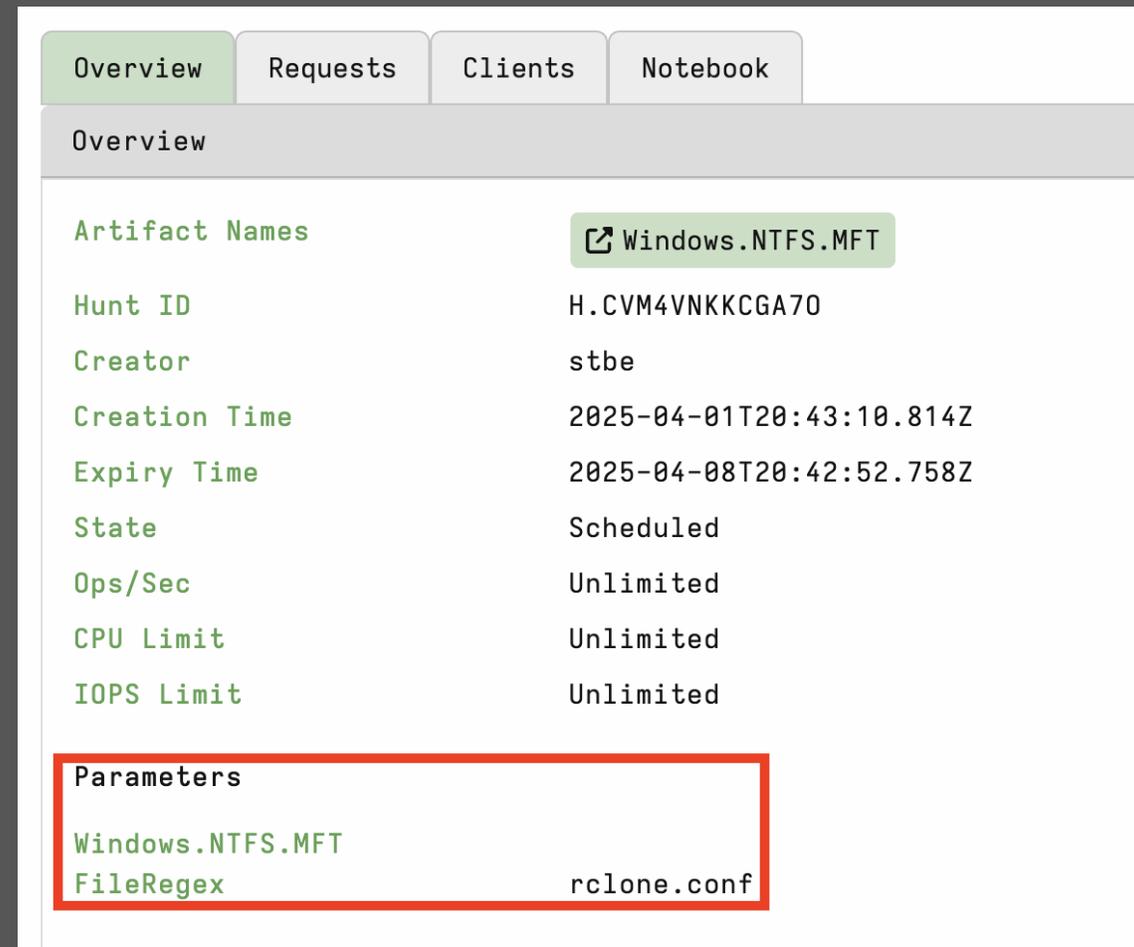
Securing  
Your Digital  
World

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.



The screenshot shows the 'Overview' tab of the InfoGuard interface. It displays the configuration for a task named 'Windows.NTFS.MFT'. The configuration includes the following details:

| Artifact Names | Windows.NTFS.MFT         |
|----------------|--------------------------|
| Hunt ID        | H.CVM4VNKKCGA70          |
| Creator        | stbe                     |
| Creation Time  | 2025-04-01T20:43:10.814Z |
| Expiry Time    | 2025-04-08T20:42:52.758Z |
| State          | Scheduled                |
| Ops/Sec        | Unlimited                |
| CPU Limit      | Unlimited                |
| IOPS Limit     | Unlimited                |

Below the configuration table, the 'Parameters' section is highlighted with a red box. It shows the following configuration:

| Parameters       |             |
|------------------|-------------|
| Windows.NTFS.MFT |             |
| FileRegex        | rclone.conf |

# NFTS Recover

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

Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook

Overview

|                       |                          |
|-----------------------|--------------------------|
| <b>Artifact Names</b> | Windows.NTFS.Recover     |
| Flow ID               | F.CVM526E08L7FE          |
| Creator               | stbe                     |
| Create Time           | 2025-04-01T20:48:25.872Z |
| Start Time            | 2025-04-01T20:48:25.351Z |
| Last Active           | 2025-04-01T20:48:25.646Z |
| Duration              | 0.30 seconds             |
| State                 | Completed                |
| Ops/Sec               | Unlimited                |
| CPU Limit             | Unlimited                |
| IOPS Limit            | Unlimited                |
| Timeout               | 600 seconds              |
| Max Rows              | 1m rows                  |
| Max Mb                | 1000.00 Mb               |

**Parameters**

|                      |        |
|----------------------|--------|
| Windows.NTFS.Recover |        |
| MFTId                | 223485 |

Results

|                               |                             |
|-------------------------------|-----------------------------|
| <b>Artifacts with Results</b> | Windows.NTFS.Recover/Upload |
| <b>Total Rows</b>             | 4                           |
| <b>Uploaded Bytes</b>         | 346 / 346                   |
| <b>Files uploaded</b>         | 4                           |

**Download Results**

Select a download method

# Recovered rclone.conf

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

| Timestamp  | started                                    | vfs_path  | Type | file_size | uploaded_size | Preview                |
|------------|--|---|------|-----------|---------------|------------------------|
| 1743540507 | 2025-04-01<br>20:48:27.005576375 +0000 UTC | \\.\C:\<Err>\<Parent 220671-12 need<br>11>\rclone.conf\223485-12-0  |      | 72        | 72            | ®> ;Û - JT ;Û òòBù...  |
| 1743540507 | 2025-04-01<br>20:48:27.005779039 +0000 UTC | \\.\C:\<Err>\<Parent 220671-12 need<br>11>\rclone.conf\223485-48-4  |      | 88        | 88            | ÿ] - JT-;Û - JT...     |
| 1743540507 | 2025-04-01<br>20:48:27.005958863 +0000 UTC | \\.\C:\<Err>\<Parent 220671-12 need<br>11>\rclone.conf\223485-48-5  |      | 90        | 90            | ÿ] - JT-;Û - JT...     |
| 1743540507 | 2025-04-01<br>20:48:27.006113189 +0000 UTC | \\.\C:\<Err>\<Parent 220671-12 need<br>11>\rclone.conf\223485-128-1 |      | 96        | 96            | [mega1] type = mega... |



Securing  
Your Digital  
World

infoGuard  
SWISS CYBER SECURITY

# More deleted files fun

# USN Journal

- 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, **juX7H.png is an LSASS dump** (and deleted..).

 **Stephan Berger** 10:02 AM

UAt9zmRt

```
%COMSPEC% /Q /c cmd.exe /Q /c for /f "tokens=1,2 delims= " ^%A in ("tasklist /fi "Imagename eq lsass.exe" |
find "lsass""") do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\juX7H.png
```

full user mode service demand start LocalSystem 2024-08-05T22:24:16Z [TC-MS.schlatter.ch](#) System  
Service Control Manager 7045 45688 S-1-5-21-2065722868-766919781-6498272-6693  
adminmuenster

 **1 reply** 8 months ago

 **Stephan Berger** 10:12 AM

File juX7H.png was created on the file system at 2024-08-05T22:24:16Z  
And then deleted at 2024-08-05T22:25:36Z  
Source: USN (edited)

 1 

# Disable / Delete the USN Journal

```
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     |



The screenshot shows the Elastic website interface. The top navigation bar includes the Elastic logo, links for Platform, Solutions, Customers, Resources, Pricing, and Docs, a search icon, and a user profile icon. A left sidebar menu is visible with categories: Reference (selected), Security, and Observability. The main content area features a document titled "Delete Volume USN Journal with Fsutil". A red box highlights a key detection rule description: "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."

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

- 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).

 **Stephan Berger** 4:25 PM

SRUM - FNY-VeeamEntMan. .com

```

2024-06-07T14:32:00Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T15:31:59Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T16:33:00Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T17:34:00Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T18:34:59Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T19:36:00Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T20:37:00Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T21:38:00Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T22:38:59Z \Device\HarddiskVolume3\Windows\write86.exe
2024-06-07T23:39:59Z \Device\HarddiskVolume3\Windows\write86.exe
    
```

(edited)

 **Stephan Berger** 4:34 PM

The first time the write86.exe was picked up by SRUM matches the birth date of the rclone folder on this host:  
 C:\Windows\System32\config\systemprofile\AppData\Local\rclone  
 2024-06-07T14:28:42.803992Z

FNY-VeeamEntMan.: .com

 1

But no traces of write86 on that host (FNY-VeeamEntMan), checked MFT and USN



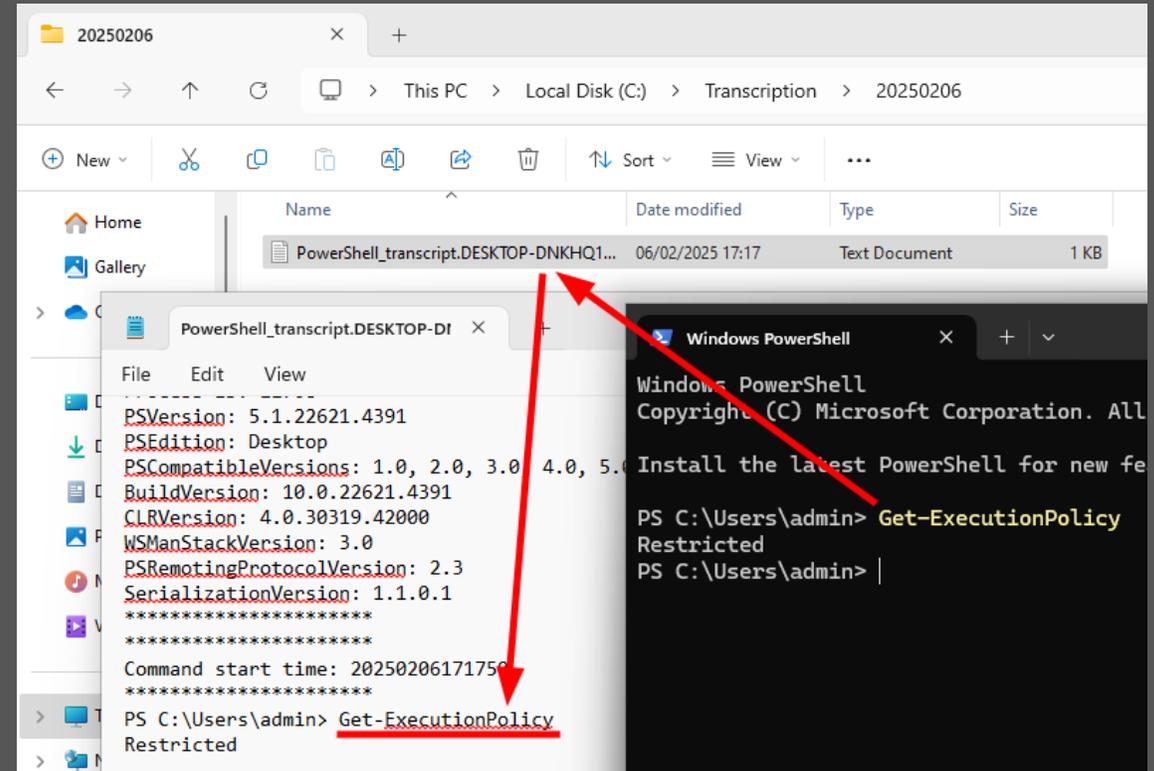
Securing  
Your Digital  
World

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

- 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:\0365\SACT"
5: $archiveName = Join-Path $rarDir (Get-Random -max 9999999999 -min 999999999)
6: & "C:\Program Files\WinRar\Rar.exe" a -r -ep1 -vlg -n*pdf -n*doc -n*docx -n*xls -n*xlsx
-n*txt -ta20240101000000 -tb20260101000000 -sl2000000000 -ed "$archiveName" "$filesDir1\*"

7: $filesDir1 = 'D:\Group_FR\01_BE'
8: $rarDir = "D:\0365\SACT"
9: $archiveName = Join-Path $rarDir (Get-Random -max 9999999999 -min 999999999)
10: & "C:\Program Files\WinRar\Rar.exe" a -r -ep1 -vlg -n*pdf -n*doc -n*docx -n*xls -
n*xlsx -n*txt -ta20240101000000 -tb20260101000000 -sl2000000000 -ed "$archiveName"
"$filesDir1\*"

11: $filesDir1 = 'D:\Group_FR\04_COMMERCIAL'
12: $rarDir = "D:\0365\SACT"
13: $archiveName = Join-Path $rarDir (Get-Random -max 9999999999 -min 999999999)
14: & "C:\Program Files\WinRar\Rar.exe" a -r -ep1 -vlg -n*pdf -n*doc -n*docx -n*xls -
n*xlsx -n*txt -ta20240101000000 -tb20260101000000 -sl2000000000 -ed "$archiveName"
"$filesDir1\*"

```

## Tampering with the History file

- Change where these logs are saved using `Set-PSReadLineOption -HistorySavePath {FilePath}`.

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

[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**

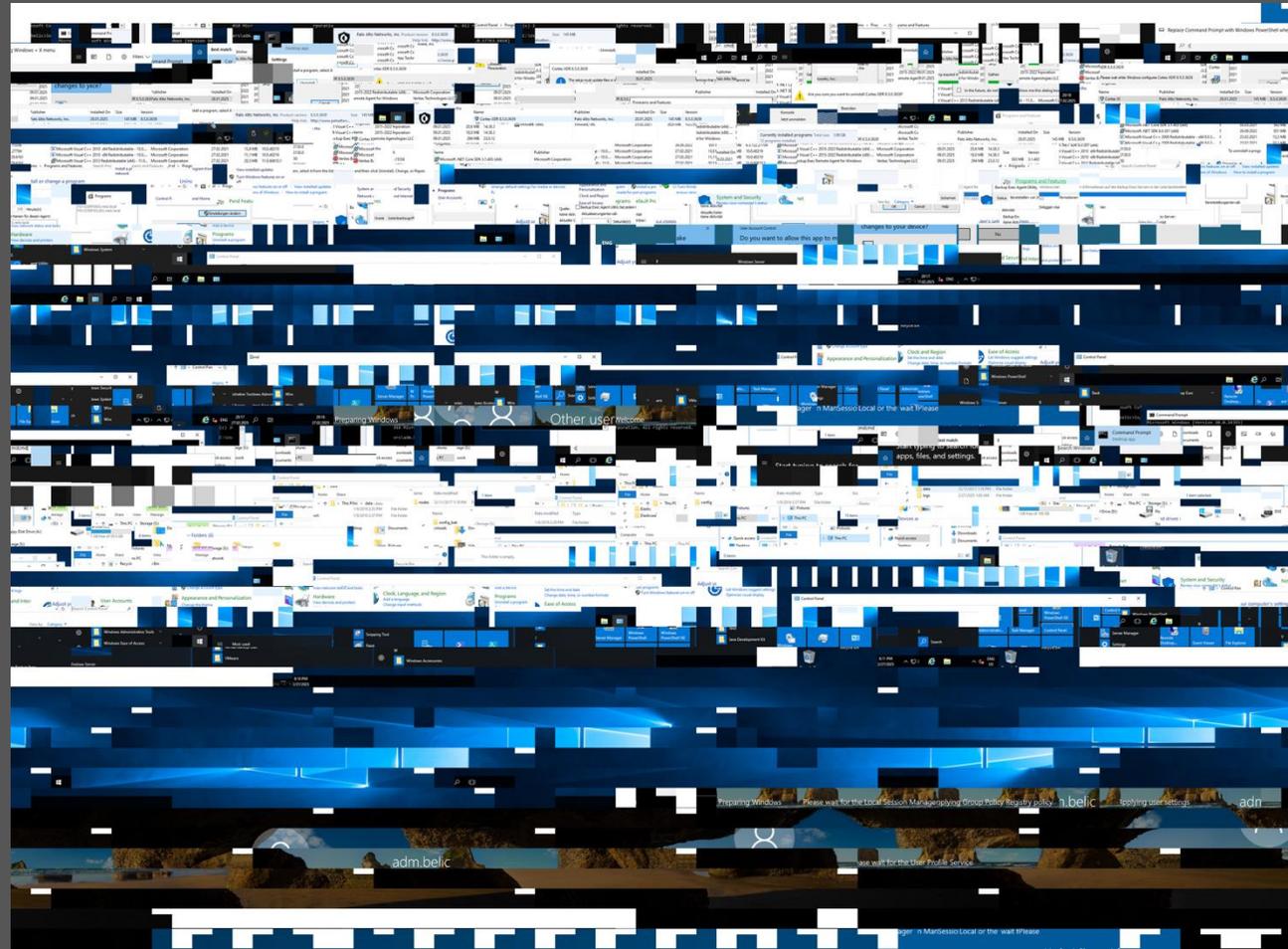
## From a recent case

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

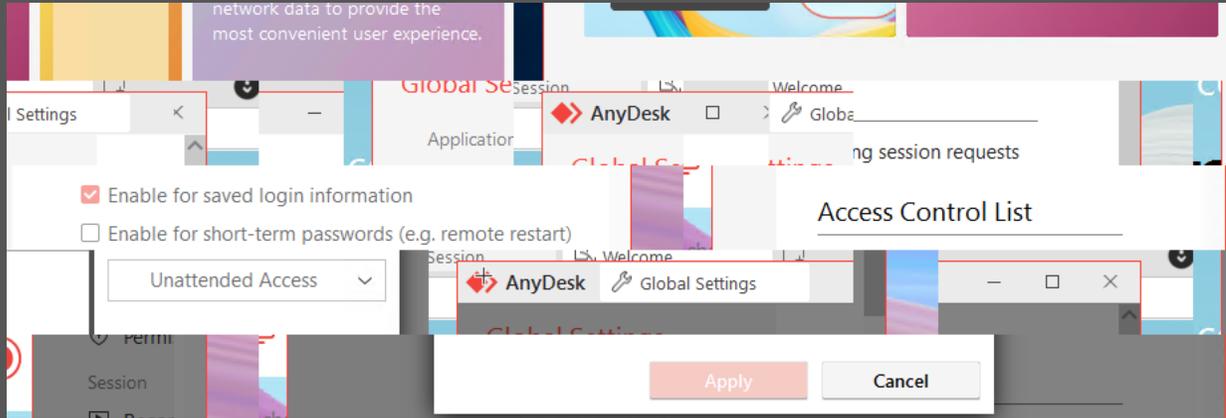
```
@echo off
reg.exe delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg.exe delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg.exe add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
attrib -s -h %userprofile%\documents\Default.rdp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

A screenshot of a Windows installation progress window for 'Cortex XDR 8.5.0.3639'. The window shows a progress bar and a message: 'Please wait while Windows configures Cortex XDR 8.5.0.3639'. Below the progress bar is a table with the following data:

| Name      | Publisher                | Installed |
|-----------|--------------------------|-----------|
| Cortex XI | Palo Alto Networks, Inc. | 28.01.2   |

Below the table, a command prompt window is open, showing the following command and output:

```
C:\ProgramData> cd c:\programdata\log.txt
```

The command prompt also shows a file explorer path: 'C:\ProgramData\log.txt'.



Securing  
Your Digital  
World

infoGuard  
SWISS CYBER SECURITY

# Clearing dmesg

# Anti-Forensics, Mandiant, January 2025

cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en

## Anti-Forensics

Following exploitation, the threat actor has been observed removing evidence of exploitation from several key areas of the appliance:

### Mandiant Incident Response

Investigate, contain, and remediate security incidents.

[Learn more](#)

1. Clearing kernel messages using `dmesg` and removing entries from the debug logs that are generated during the exploit
2. Deleting troubleshoot information packages (state dumps) and any core dumps generated from process crashes
3. Removing log application event log entries related to syslog failures, internal ICT failures, crash traces, and certificate handling errors
4. Removing executed commands from the SELinux audit log

```
dmesg -C
cd /data/var/dlogs/
sed -i '/segfault/d' debuglog
sed -i '/segfault/d' debuglog.old
sed -i '/SystemError/d' debuglog
```

## Anti-Forensics, in action

- 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

- 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

- 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 bttmp wttmp and bttmp 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+wttmp+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.)

```

[.]
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

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

```
Deleted archived journal
/var/log/journal/53d3dae872b75fd5b8b4abb067d4a62d/system@75c9cb1517aa471d9bb0d9a7aa75e8ec-
0000000000000edf-0006305bfcaadc70.journal (38.1M).
[.]
system@75c9cb1517aa471d9bb0d9a7aa75e8ec-000000000000cd9e3-000632c7b3335546.journal (37.5M).
Deleted archived journal
/var/log/journal/53d3dae872b75fd5b8b4abb067d4a62d/system@75c9cb1517aa471d9bb0d9a7aa75e8ec-
000000000000da972-000632f4f03b4ff5.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

```
[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 :)

repo:elastic/protections-artifacts journalctf

Filter by

- <> Code 0
- Issues 0
- Pull requests 0
- Discussions 0
- Commits 0
- Packages 0
- Wikis 0

Advanced search

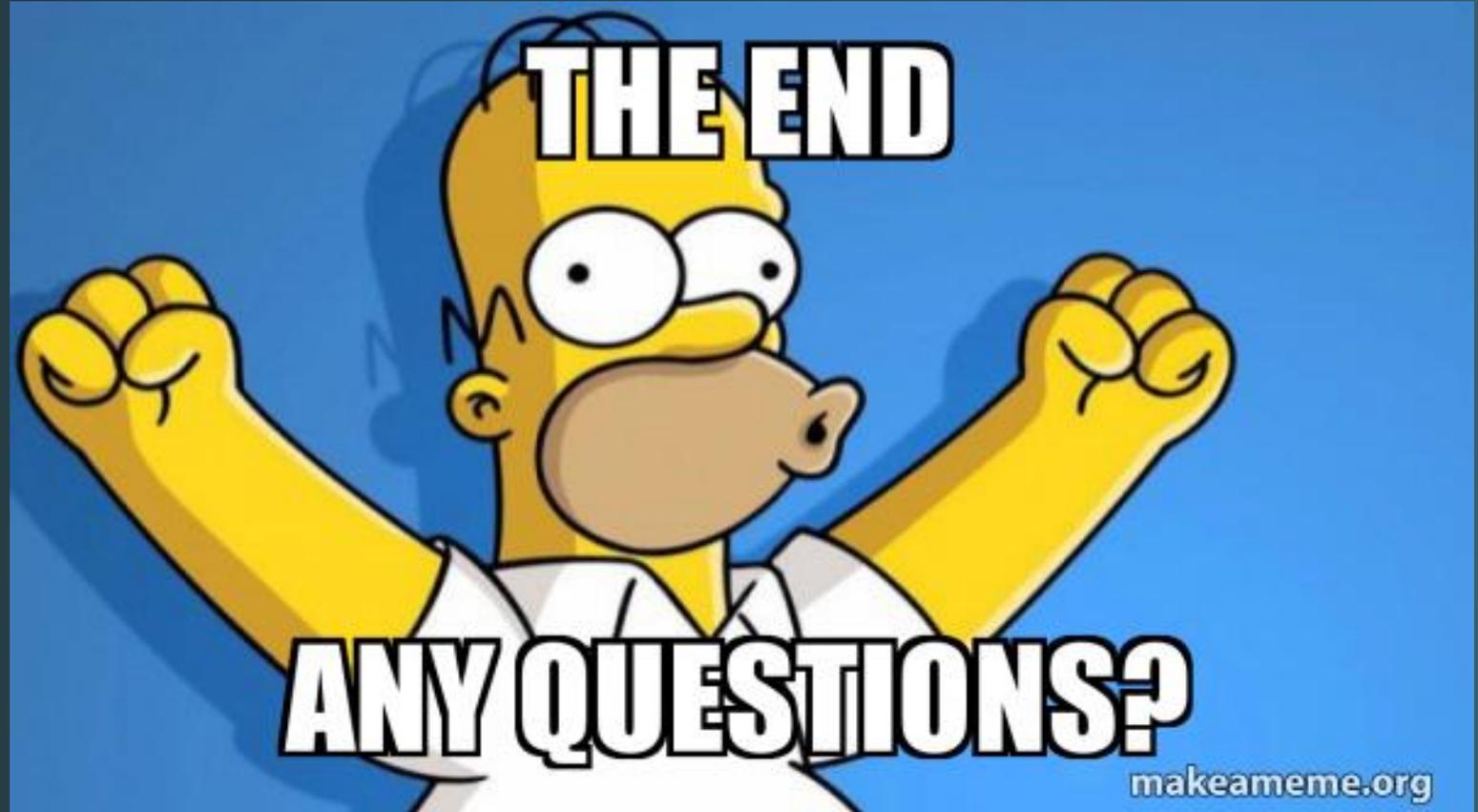
0 files (44 ms) in elastic/protections-artifacts

**Your search did not match any code**

You could try one of the tips below.

- Search across repositories
- Search across an organization
- Find a particular file extension
- Why wasn't my code found?
- Regular expressions
- Saved searches

Questions?



Let's connect :)