# N-IOC TO RULE THEM ALL

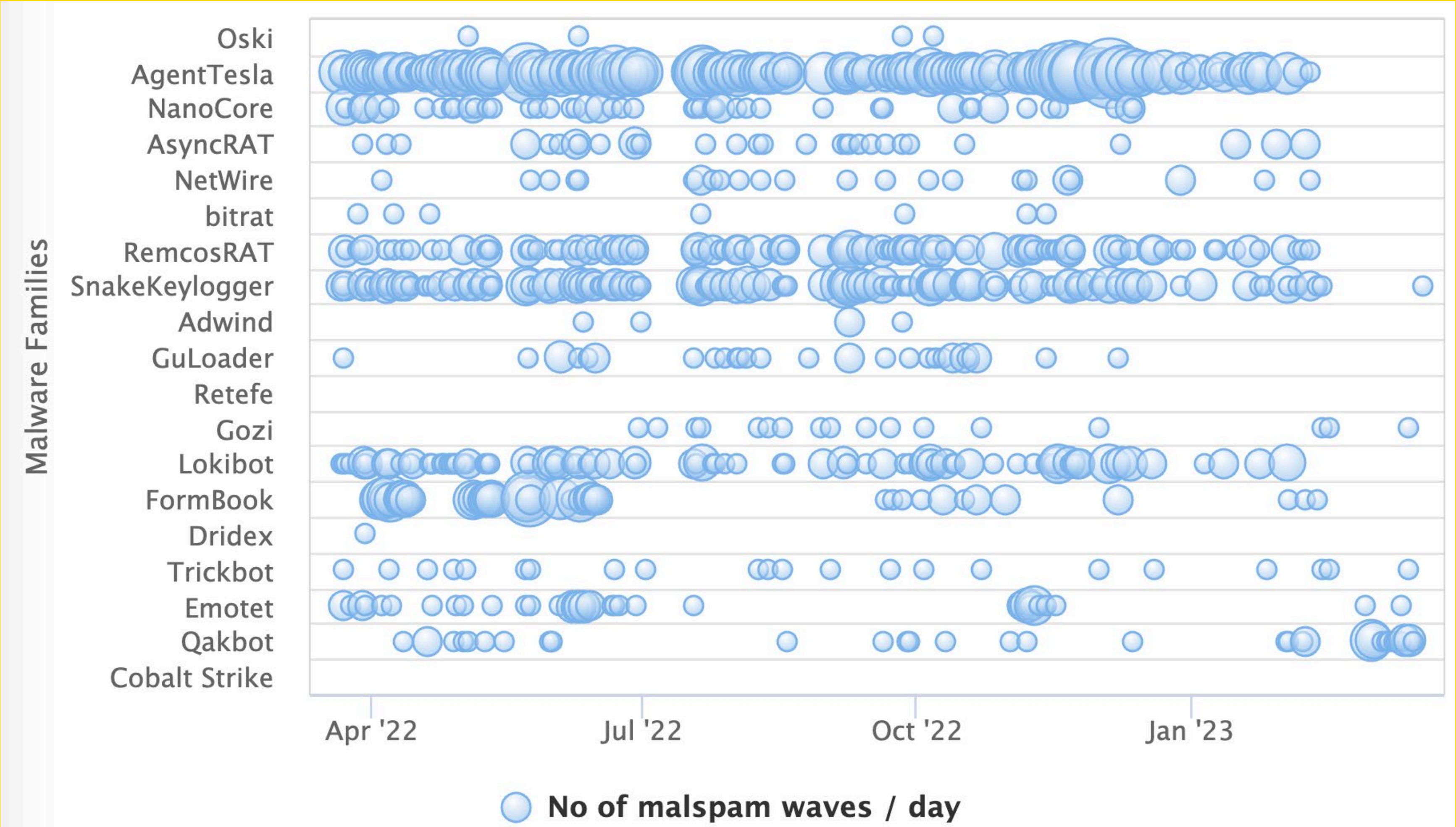
InfoGuard
SWISS CYBER SECURITY

# ABOUT ME (STEPHAN BERGER)

## Head of Investigations at InfoGuard AG

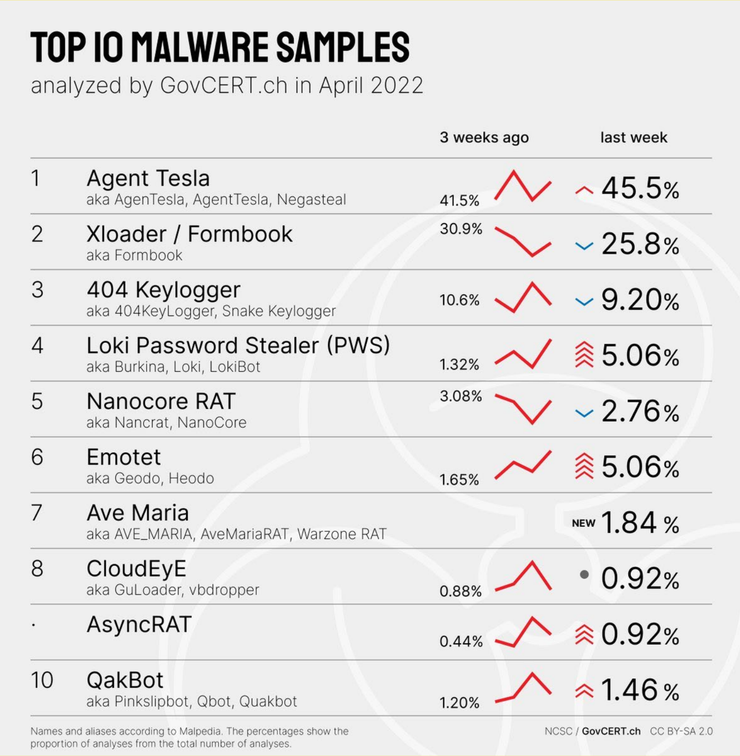
- Spending probably too much time on 🐦
- Luckily I have an excellent team covering my back 🤩
- Master of musical song references ♫
- SysAdmin / SOC-Analyst / CSIRT / Consultant

# MALWARE EVENTS IN SWITZERLAND



*Source: govcert.ch*

# TOP 10 MALWARE SAMPLES (*GOVCERT.CH*)



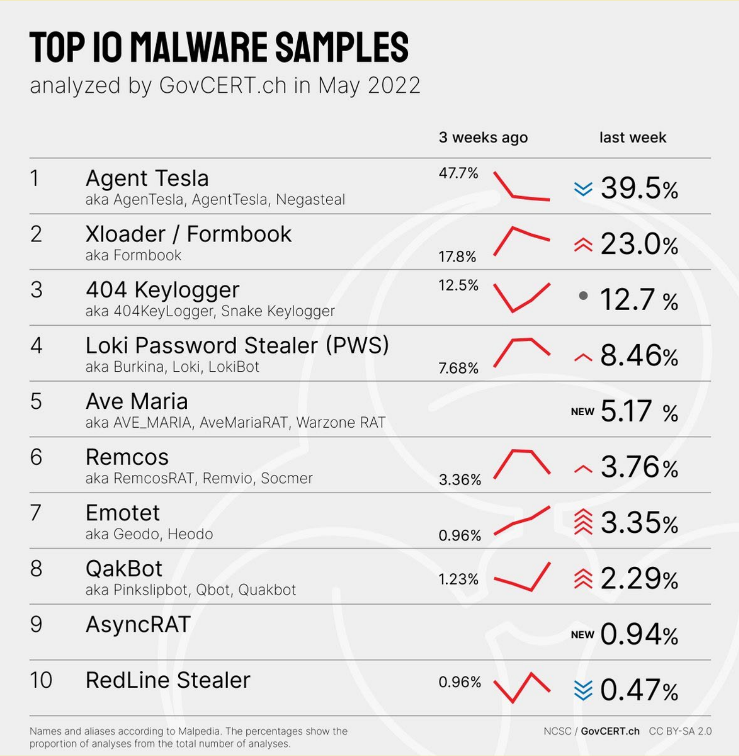
## TOP 10 MALWARE SAMPLES

analyzed by GovCERT.ch in April 2022

| | | 3 weeks ago | last week |
|---|---|---|---|
| 1 | Agent Tesla<br>aka AgenTesla, AgentTesla, Negasteal | 41.5% | ˄ 45.5% |
| 2 | Xloader / Formbook<br>aka Formbook | 30.9% | ˅ 25.8% |
| 3 | 404 Keylogger<br>aka 404KeyLogger, Snake Keylogger | 10.6% | ˅ 9.20% |
| 4 | Loki Password Stealer (PWS)<br>aka Burkina, Loki, LokiBot | 1.32% | ⇈ 5.06% |
| 5 | Nanocore RAT<br>aka Nancrat, NanoCore | 3.08% | ˅ 2.76% |
| 6 | Emotet<br>aka Geodo, Heodo | 1.65% | ⇈ 5.06% |
| 7 | Ave Maria<br>aka AVE_MARIA, AveMariaRAT, Warzone RAT | | NEW 1.84 % |
| 8 | CloudEyE<br>aka GuLoader, vbdropper | 0.88% | ● 0.92% |
| · | AsyncRAT | 0.44% | ⇈ 0.92% |
| 10 | QakBot<br>aka Pinkslipbot, Qbot, Quakbot | 1.20% | ⇈ 1.46 % |

Names and aliases according to Malpedia. The percentages show the proportion of analyses from the total number of analyses.

NCSC / **GovCERT.ch** CC BY-SA 2.0



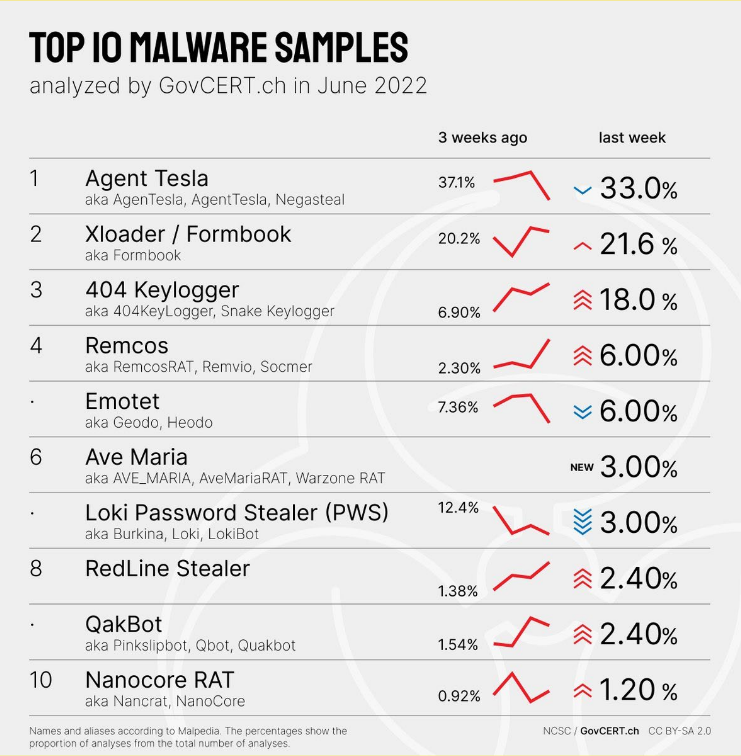
## TOP 10 MALWARE SAMPLES

analyzed by GovCERT.ch in May 2022

| | | 3 weeks ago | last week |
|---|---|---|---|
| 1 | Agent Tesla<br>aka AgenTesla, AgentTesla, Negasteal | 47.7% | ⇊ 39.5% |
| 2 | Xloader / Formbook<br>aka Formbook | 17.8% | ⇈ 23.0% |
| 3 | 404 Keylogger<br>aka 404KeyLogger, Snake Keylogger | 12.5% | ● 12.7 % |
| 4 | Loki Password Stealer (PWS)<br>aka Burkina, Loki, LokiBot | 7.68% | ˄ 8.46% |
| 5 | Ave Maria<br>aka AVE_MARIA, AveMariaRAT, Warzone RAT | | NEW 5.17 % |
| 6 | Remcos<br>aka RemcosRAT, Remvio, Socmer | 3.36% | ˄ 3.76% |
| 7 | Emotet<br>aka Geodo, Heodo | 0.96% | ⇈ 3.35% |
| 8 | QakBot<br>aka Pinkslipbot, Qbot, Quakbot | 1.23% | ⇈ 2.29% |
| 9 | AsyncRAT | | NEW 0.94% |
| 10 | RedLine Stealer | 0.96% | ⇊ 0.47% |

Names and aliases according to Malpedia. The percentages show the proportion of analyses from the total number of analyses.

NCSC / **GovCERT.ch** CC BY-SA 2.0



## TOP 10 MALWARE SAMPLES

analyzed by GovCERT.ch in June 2022

| | | 3 weeks ago | last week |
|---|---|---|---|
| 1 | Agent Tesla<br>aka AgenTesla, AgentTesla, Negasteal | 37.1% | ˅ 33.0% |
| 2 | Xloader / Formbook<br>aka Formbook | 20.2% | ˄ 21.6 % |
| 3 | 404 Keylogger<br>aka 404KeyLogger, Snake Keylogger | 6.90% | ⇈ 18.0 % |
| 4 | Remcos<br>aka RemcosRAT, Remvio, Socmer | 2.30% | ⇈ 6.00% |
| · | Emotet<br>aka Geodo, Heodo | 7.36% | ⇊ 6.00% |
| 6 | Ave Maria<br>aka AVE_MARIA, AveMariaRAT, Warzone RAT | | NEW 3.00% |
| · | Loki Password Stealer (PWS)<br>aka Burkina, Loki, LokiBot | 12.4% | ⇊ 3.00% |
| 8 | RedLine Stealer | 1.38% | ⇈ 2.40% |
| · | QakBot<br>aka Pinkslipbot, Qbot, Quakbot | 1.54% | ⇈ 2.40% |
| 10 | Nanocore RAT<br>aka Nancrat, NanoCore | 0.92% | ⇈ 1.20 % |

Names and aliases according to Malpedia. The percentages show the proportion of analyses from the total number of analyses.

NCSC / **GovCERT.ch** CC BY-SA 2.0

*Source: govcert.ch*

# TOP 10 MALWARE FAMILIES (*GOVCERT.CH*)

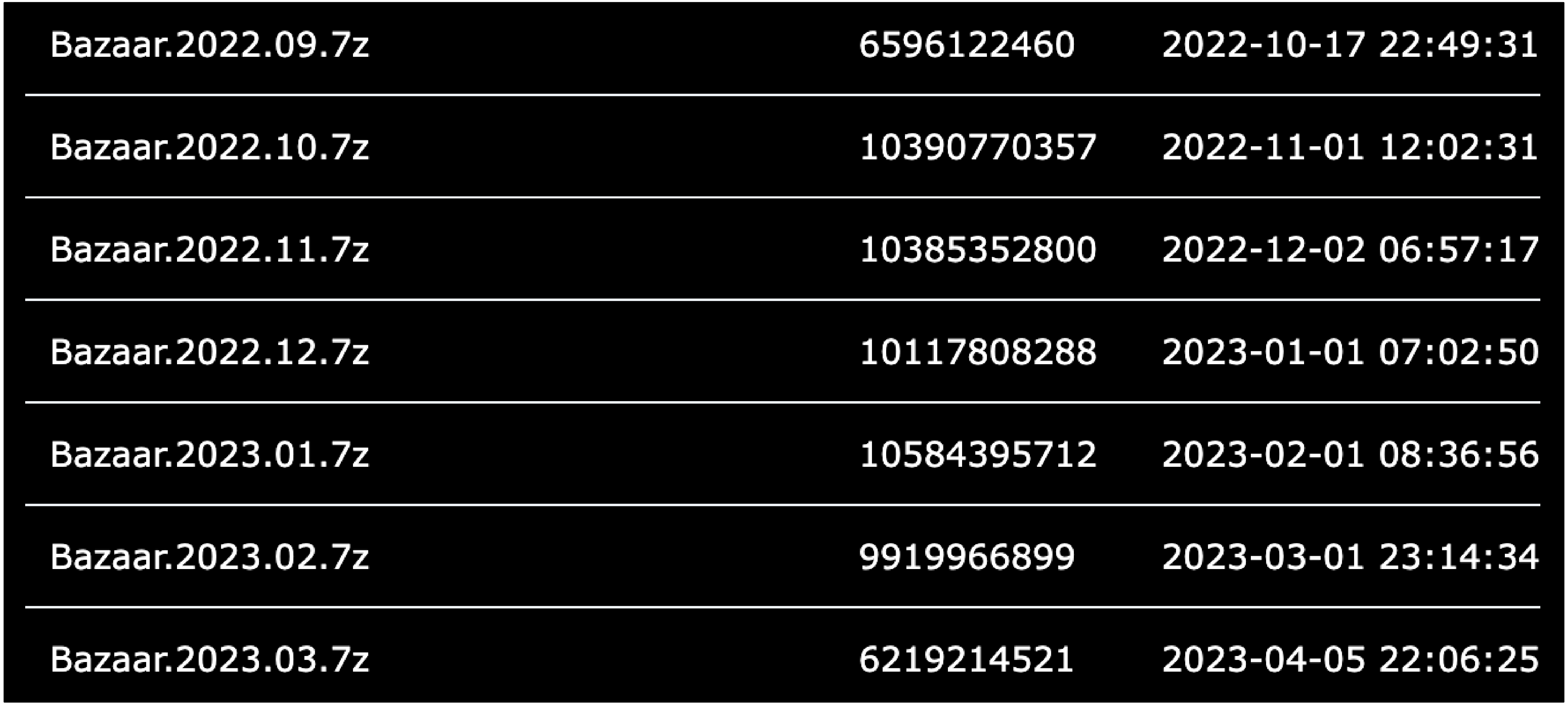
- Agent Tesla
- Formbook
- 404 Keylogger
- Loki Password Stealer
- Ave Maria RAT
- Remcos
- Nanocore RAT
- QakBot
- Redline Stealer
- Netwire RAT

*Source: April 2022 – December 2022*

# REVERSE ENGINEERING..

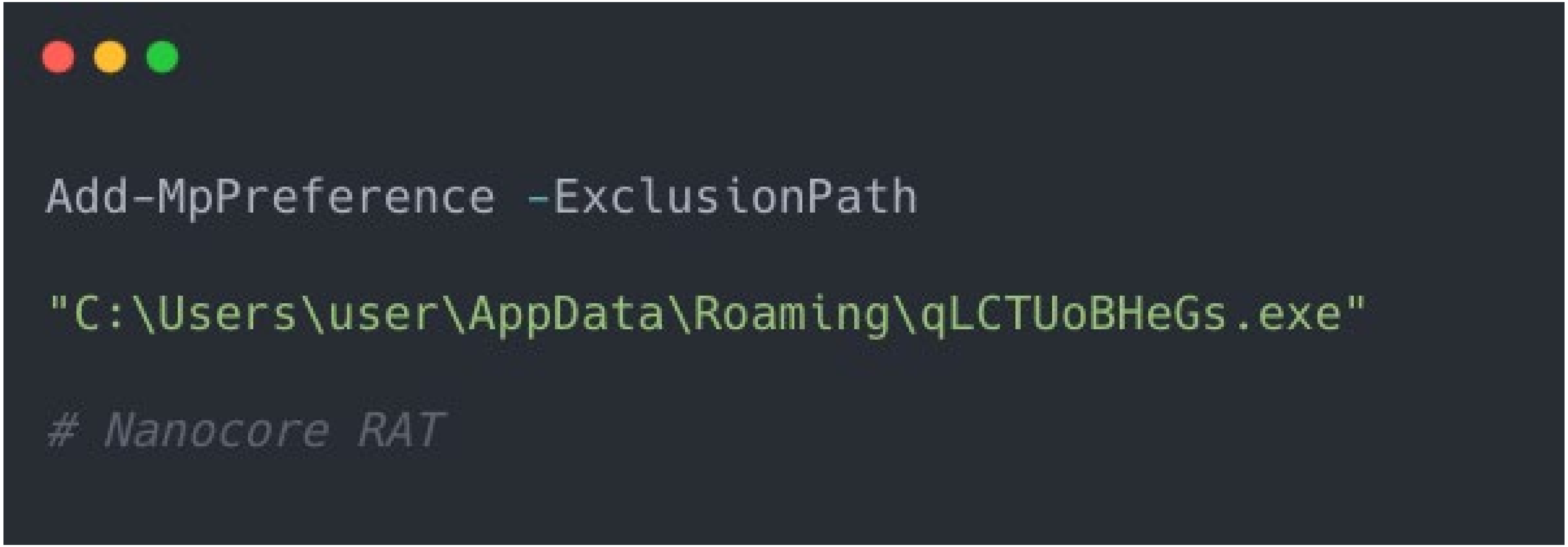
# WORK SMARTER, NOT HARDER

# SAMPLES: VX-UNDERGROUND



| | | |
|---|---|---|
| Bazaar.2022.09.7z | 6596122460 | 2022-10-17 22:49:31 |
| Bazaar.2022.10.7z | 10390770357 | 2022-11-01 12:02:31 |
| Bazaar.2022.11.7z | 10385352800 | 2022-12-02 06:57:17 |
| Bazaar.2022.12.7z | 10117808288 | 2023-01-01 07:02:50 |
| Bazaar.2023.01.7z | 10584395712 | 2023-02-01 08:36:56 |
| Bazaar.2023.02.7z | 9919966899 | 2023-03-01 23:14:34 |
| Bazaar.2023.03.7z | 6219214521 | 2023-04-05 22:06:25 |

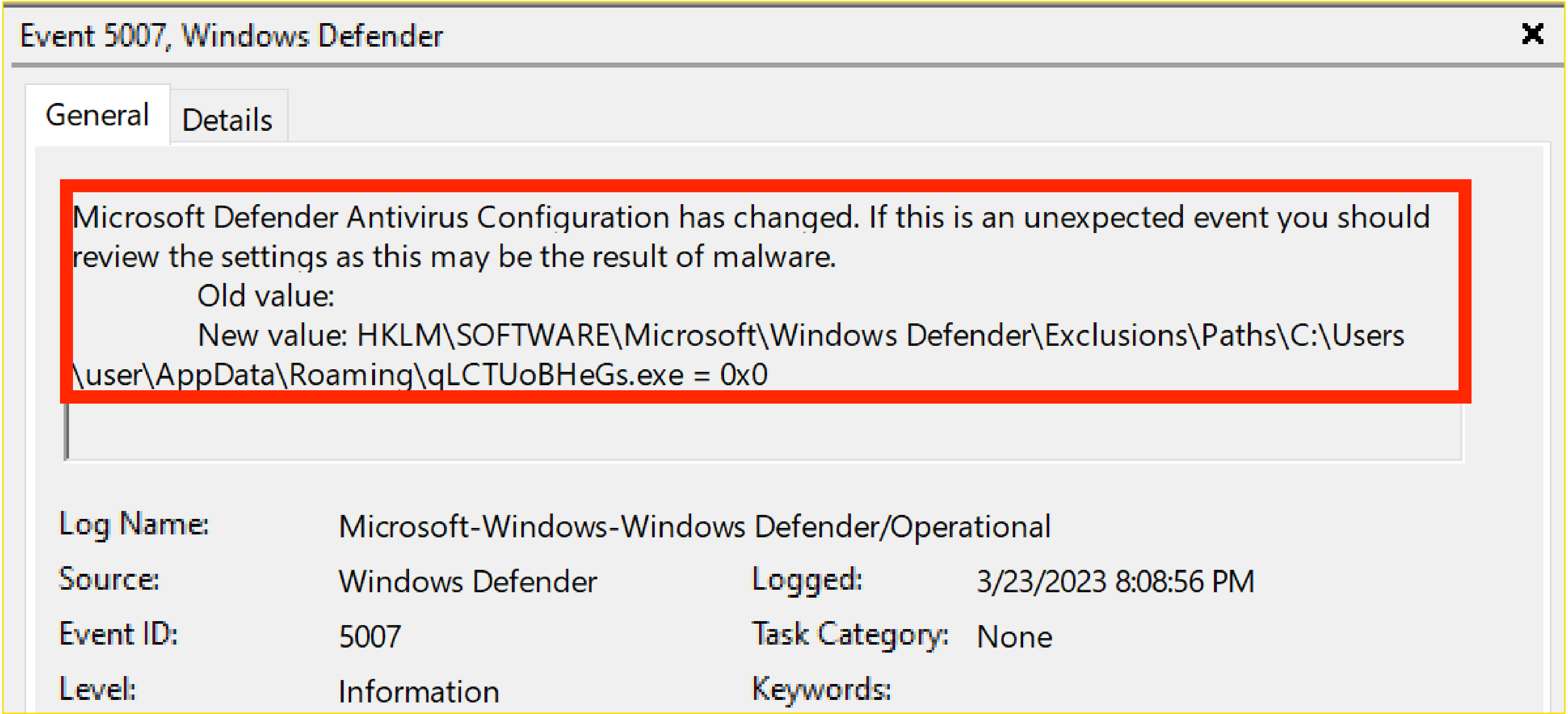
# IOC #1: DEFENDER EXCLUSIONS



```
Add-MpPreference -ExclusionPath

"C:\Users\user\AppData\Roaming\qLCTUoBHeGs.exe"

# Nanocore RAT
```

| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | ☑ | ☑ | ☒ | ☑ | ☒ | ☑ | ☑ | ☑ | ☒ |

# ARTIFACTS: EVENT 5007



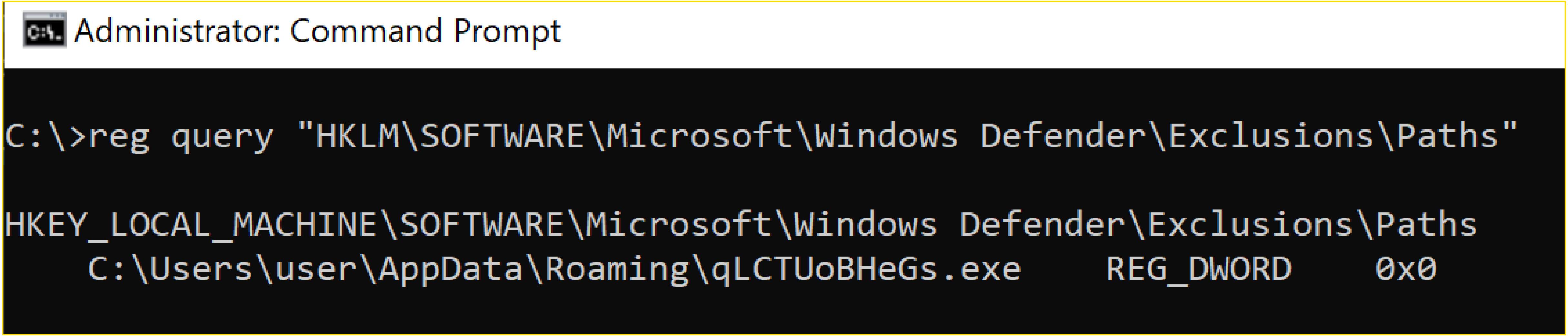
Event 5007, Windows Defender

Microsoft Defender Antivirus Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.

```
Old value:
New value: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\Users\user\AppData\Roaming\qLCTUoBHeGs.exe = 0x0
```

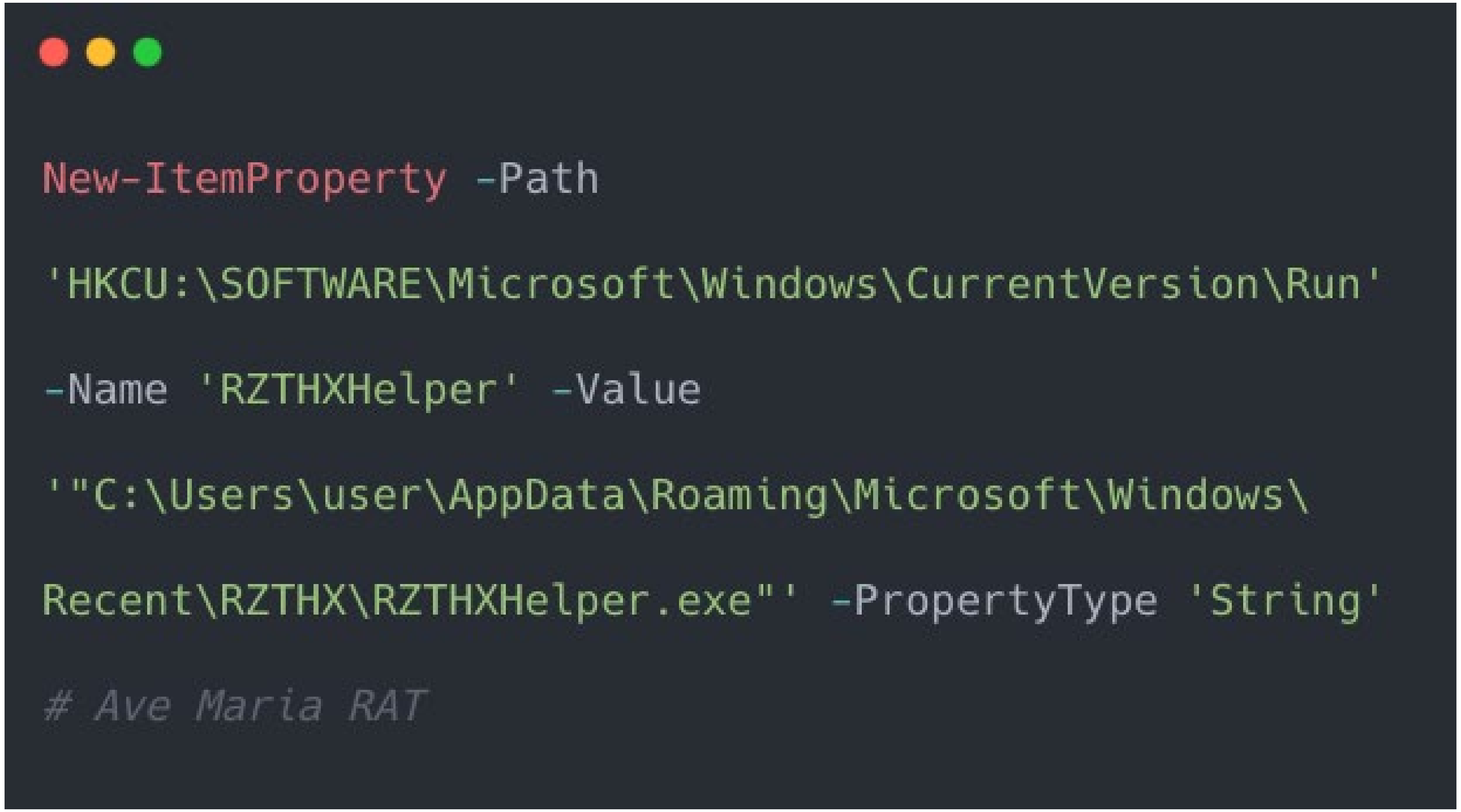
| | | | |
|---|---|---|---|
| Log Name: | Microsoft-Windows-Windows Defender/Operational | | |
| Source: | Windows Defender | Logged: | 3/23/2023 8:08:56 PM |
| Event ID: | 5007 | Task Category: | None |
| Level: | Information | Keywords: | |

# ARTIFACTS: REGISTRY



```
C:\>reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths
    C:\Users\user\AppData\Roaming\qLCTUoBHeGs.exe    REG_DWORD    0x0
```

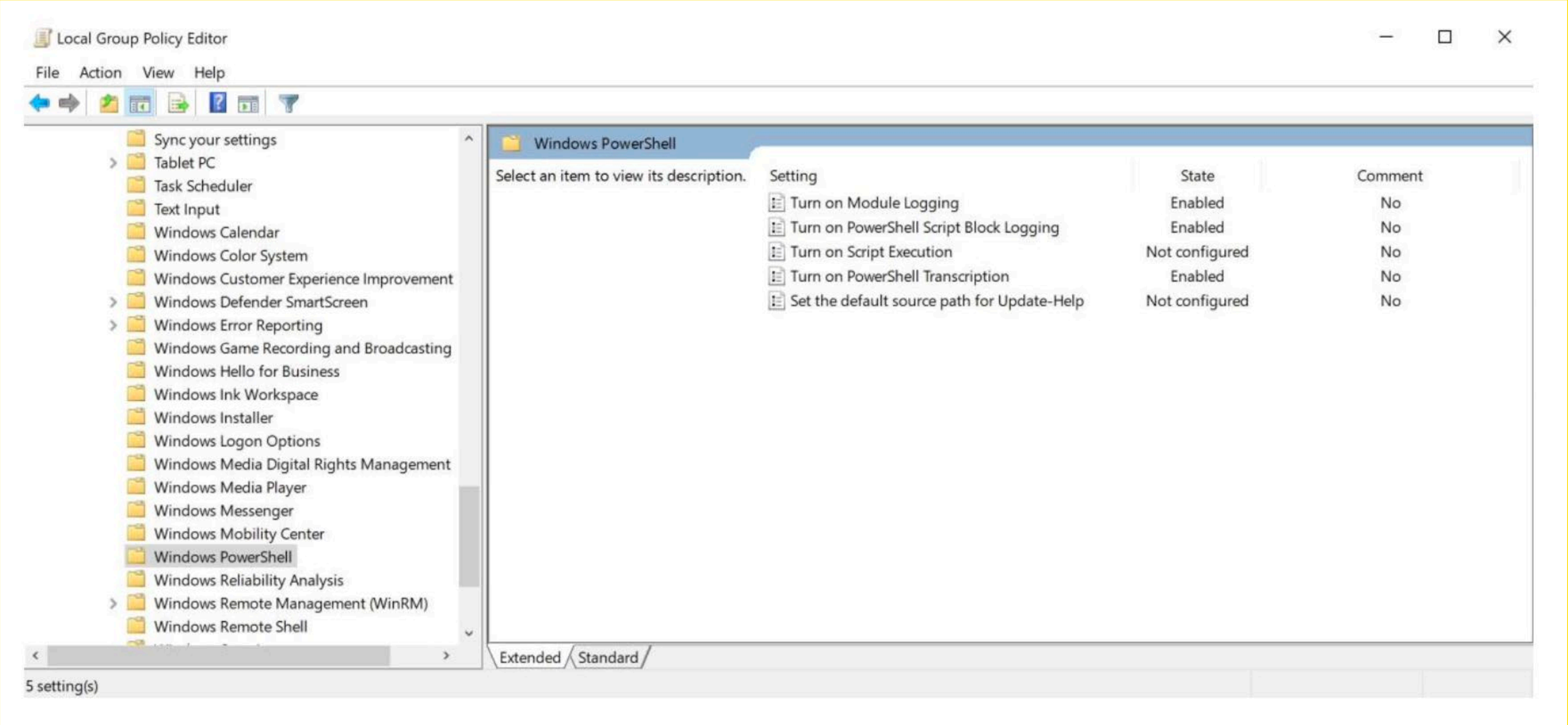
# IOC #2: POWERSHELL



```
New-ItemProperty -Path

'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'

-Name 'RZTHXHelper' -Value

'"C:\Users\user\AppData\Roaming\Microsoft\Windows\

Recent\RZTHX\RZTHXHelper.exe"' -PropertyType 'String'

# Ave Maria RAT
```

| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| (☑) | ☒ | ☑ | ☒ | (☑) | (☑) | (☑) | ☒ | ☑ | ☑ |

# ARTIFACTS: EVENT 4104

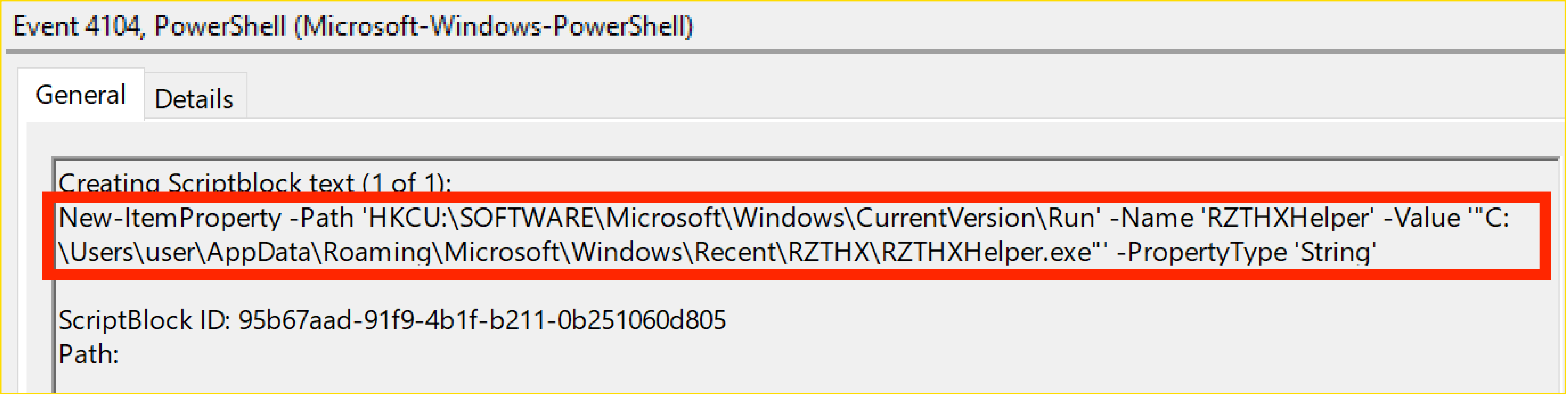


Select an item to view its description.

| Setting | State | Comment |
|---|---|---|
| Turn on Module Logging | Enabled | No |
| Turn on PowerShell Script Block Logging | Enabled | No |
| Turn on Script Execution | Not configured | No |
| Turn on PowerShell Transcription | Enabled | No |
| Set the default source path for Update-Help | Not configured | No |

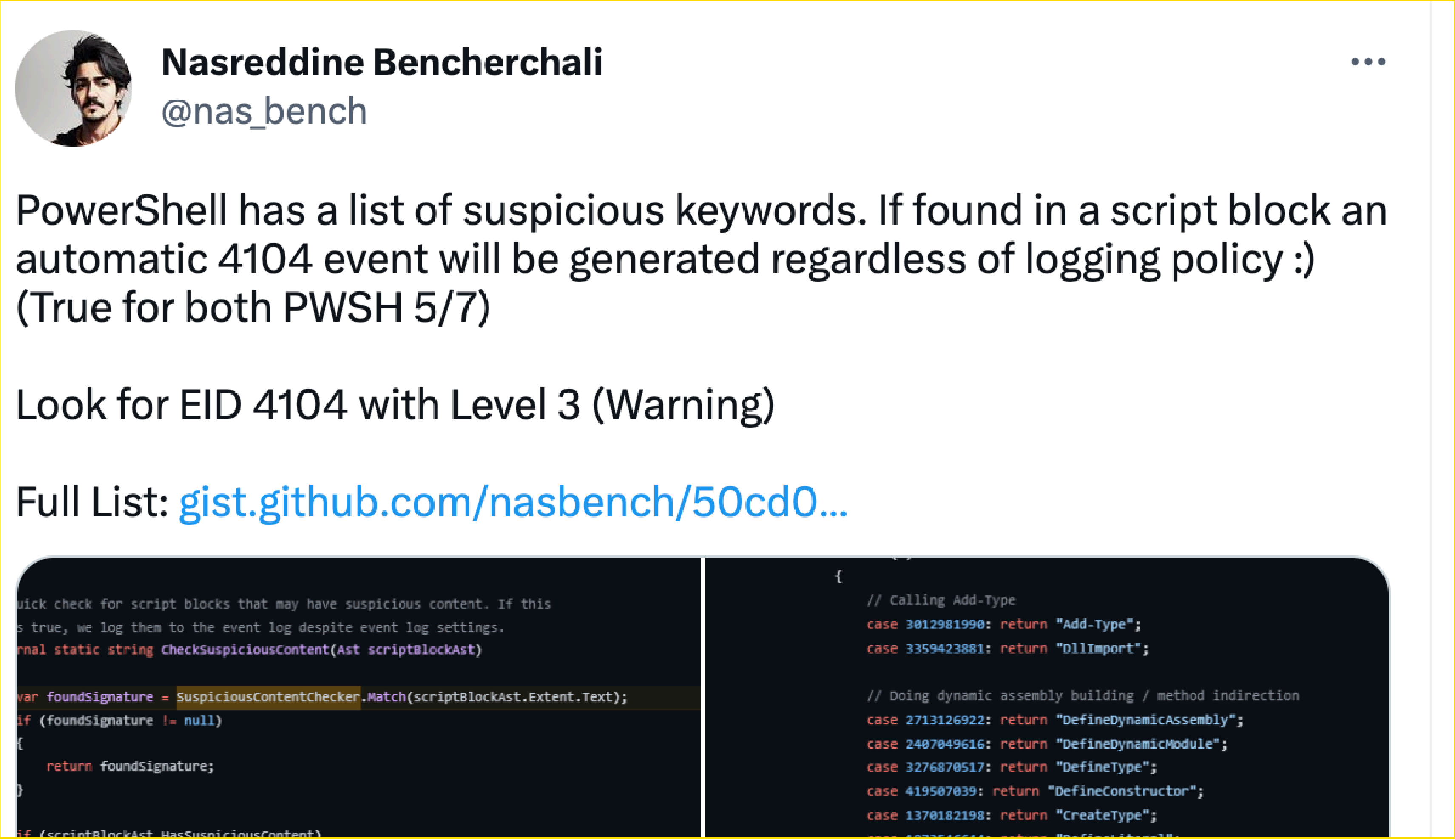
5 setting(s)

# ARTIFACTS: EVENT 4104



```
Creating Scriptblock text (1 of 1):
New-ItemProperty -Path 'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -Name 'RZTHXHelper' -Value '"C:
\Users\user\AppData\Roaming\Microsoft\Windows\Recent\RZTHX\RZTHXHelper.exe"' -PropertyType 'String'

ScriptBlock ID: 95b67aad-91f9-4b1f-b211-0b251060d805
Path:
```

# ARTIFACTS: EVENT 4104



**Nasreddine Bencherchali**
@nas_bench

PowerShell has a list of suspicious keywords. If found in a script block an automatic 4104 event will be generated regardless of logging policy :)
(True for both PWSH 5/7)

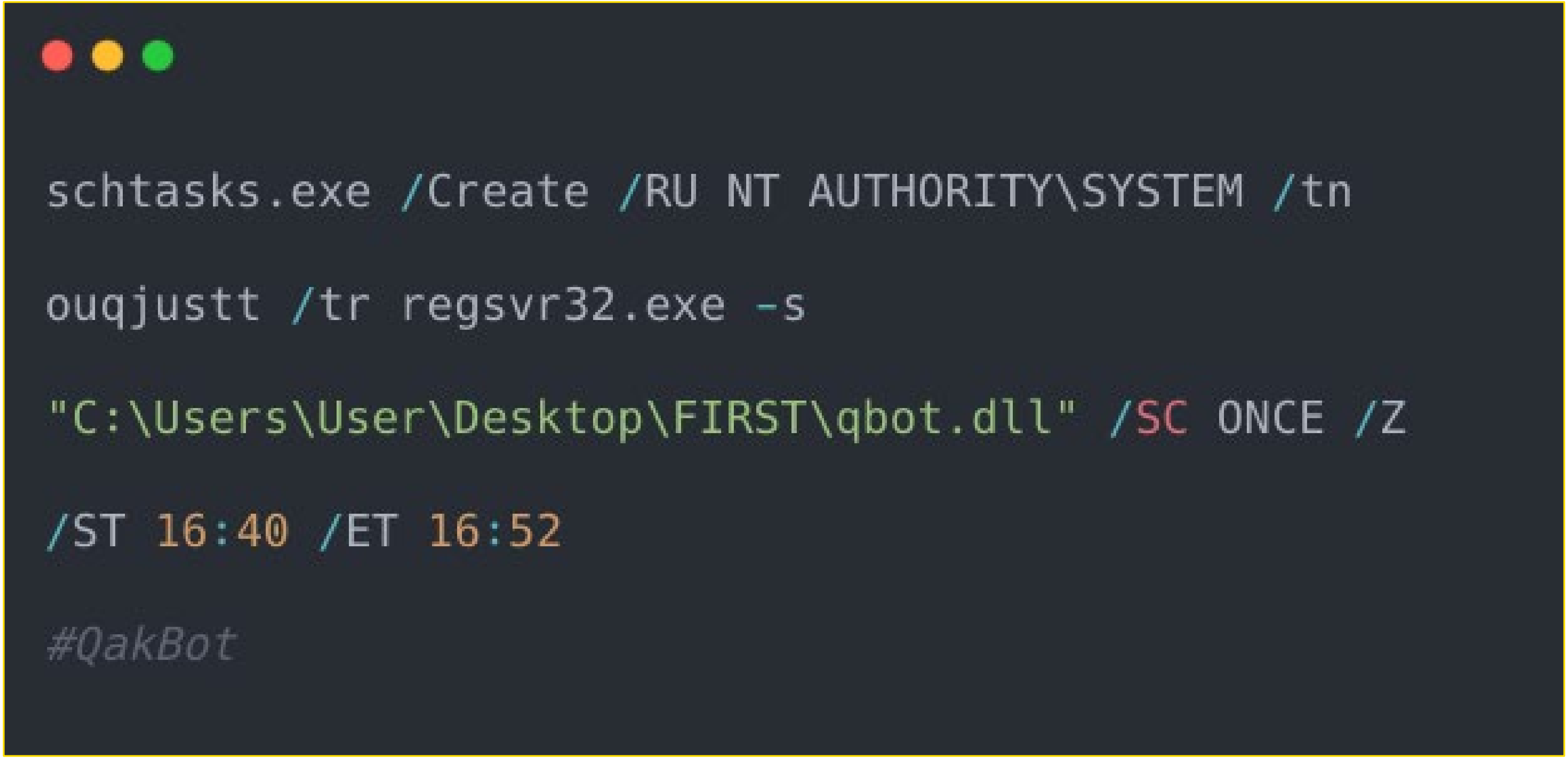
Look for EID 4104 with Level 3 (Warning)

Full List: gist.github.com/nasbench/50cd0...

```
uick check for script blocks that may have suspicious content. If this
s true, we log them to the event log despite event log settings.
rnal static string CheckSuspiciousContent(Ast scriptBlockAst)

var foundSignature = SuspiciousContentChecker.Match(scriptBlockAst.Extent.Text);
if (foundSignature != null)
{
    return foundSignature;
}

if (scriptBlockAst.HasSuspiciousContent)
```

```
    {
        // Calling Add-Type
        case 3012981990: return "Add-Type";
        case 3359423881: return "DllImport";

        // Doing dynamic assembly building / method indirection
        case 2713126922: return "DefineDynamicAssembly";
        case 2407049616: return "DefineDynamicModule";
        case 3276870517: return "DefineType";
        case 419507039: return "DefineConstructor";
        case 1370182198: return "CreateType";
```

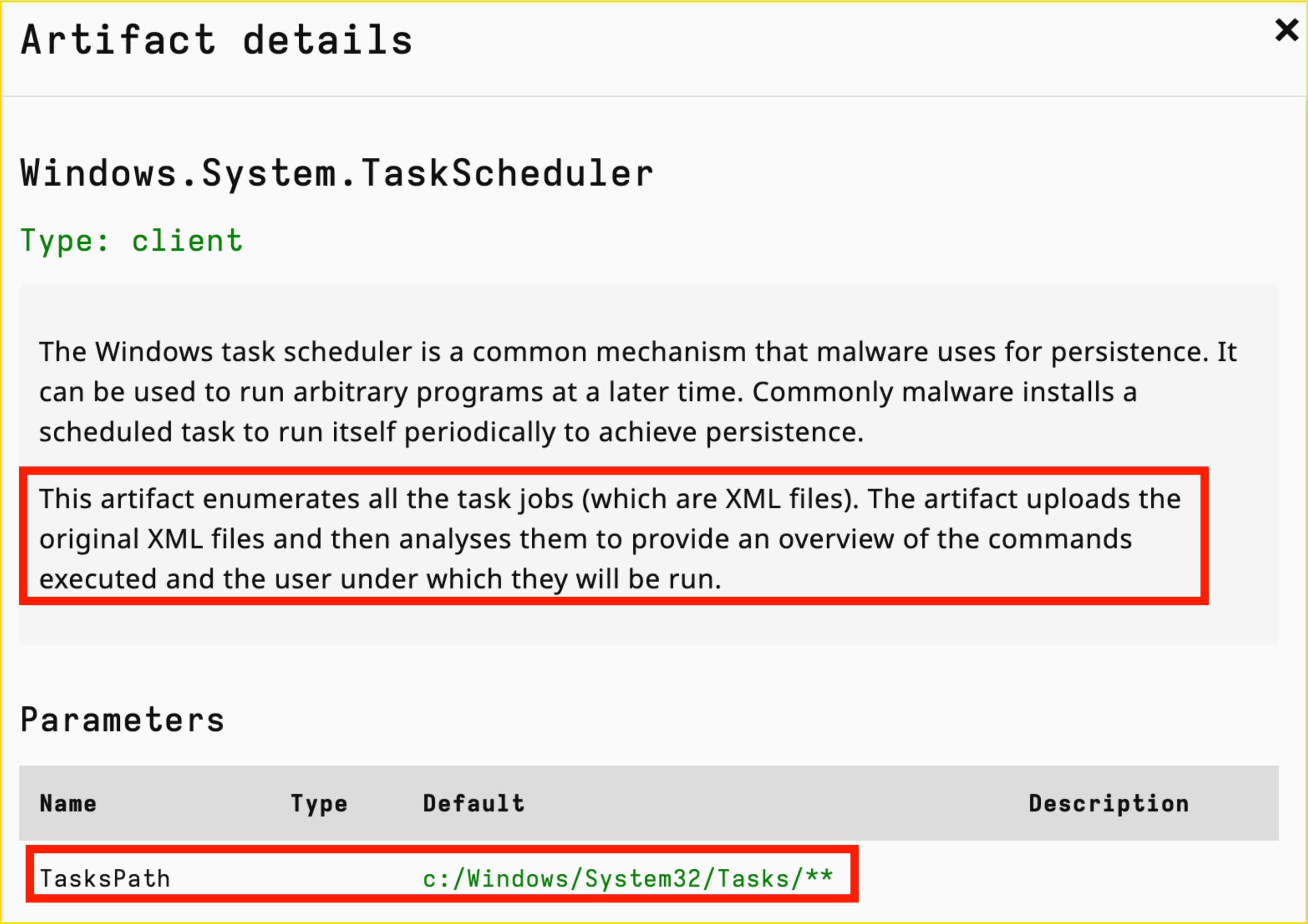
# IOC #3: SCHEDULED TASKS



```
schtasks.exe /Create /RU NT AUTHORITY\SYSTEM /tn

ouqjustt /tr regsvr32.exe -s

"C:\Users\User\Desktop\FIRST\qbot.dll" /SC ONCE /Z

/ST 16:40 /ET 16:52

#QakBot
```

| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | ☑ | ☑ | ☒ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

# ARTIFACTS: C:/WINDOWS/SYSTEM32/TASKS/*



## Windows.System.TaskScheduler

Type: client

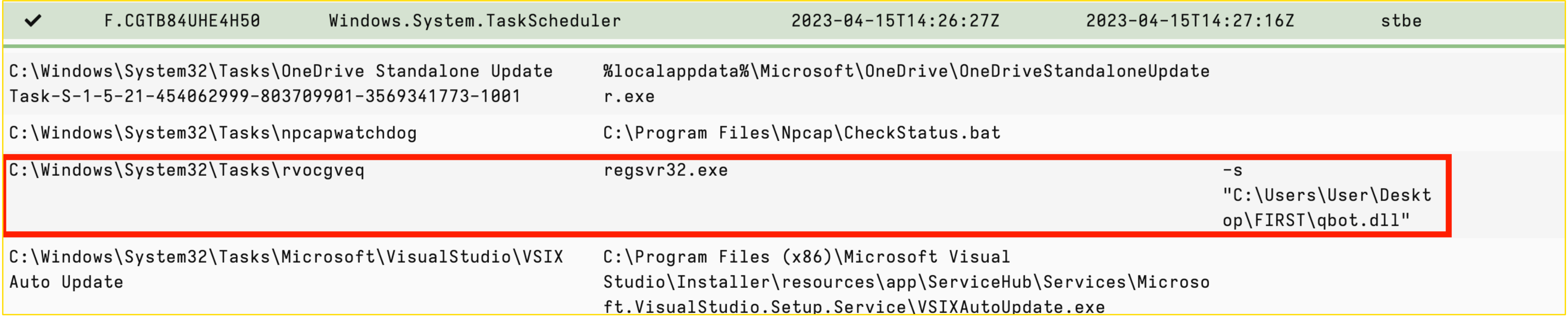
The Windows task scheduler is a common mechanism that malware uses for persistence. It can be used to run arbitrary programs at a later time. Commonly malware installs a scheduled task to run itself periodically to achieve persistence.

This artifact enumerates all the task jobs (which are XML files). The artifact uploads the original XML files and then analyses them to provide an overview of the commands executed and the user under which they will be run.

### Parameters

| Name | Type | Default | Description |
|---|---|---|---|
| TasksPath |  | c:/Windows/System32/Tasks/** |  |

# ARTIFACTS: TASKS WITH COMMAND & LAUNCHSTRING



✓ F.CGTB84UHE4H50 Windows.System.TaskScheduler 2023-04-15T14:26:27Z 2023-04-15T14:27:16Z stbe

| | | |
|---|---|---|
| C:\Windows\System32\Tasks\OneDrive Standalone Update Task-S-1-5-21-454062999-803709901-3569341773-1001 | %localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe | |
| C:\Windows\System32\Tasks\npcapwatchdog | C:\Program Files\Npcap\CheckStatus.bat | |
| C:\Windows\System32\Tasks\rvocgveq | regsvr32.exe | -s "C:\Users\User\Desktop\FIRST\qbot.dll" |
| C:\Windows\System32\Tasks\Microsoft\VisualStudio\VSIX Auto Update | C:\Program Files (x86)\Microsoft Visual Studio\Installer\resources\app\ServiceHub\Services\Microsoft.VisualStudio.Setup.Service\VSIXAutoUpdate.exe | |

# ARTIFACTS: EVENT LOGS

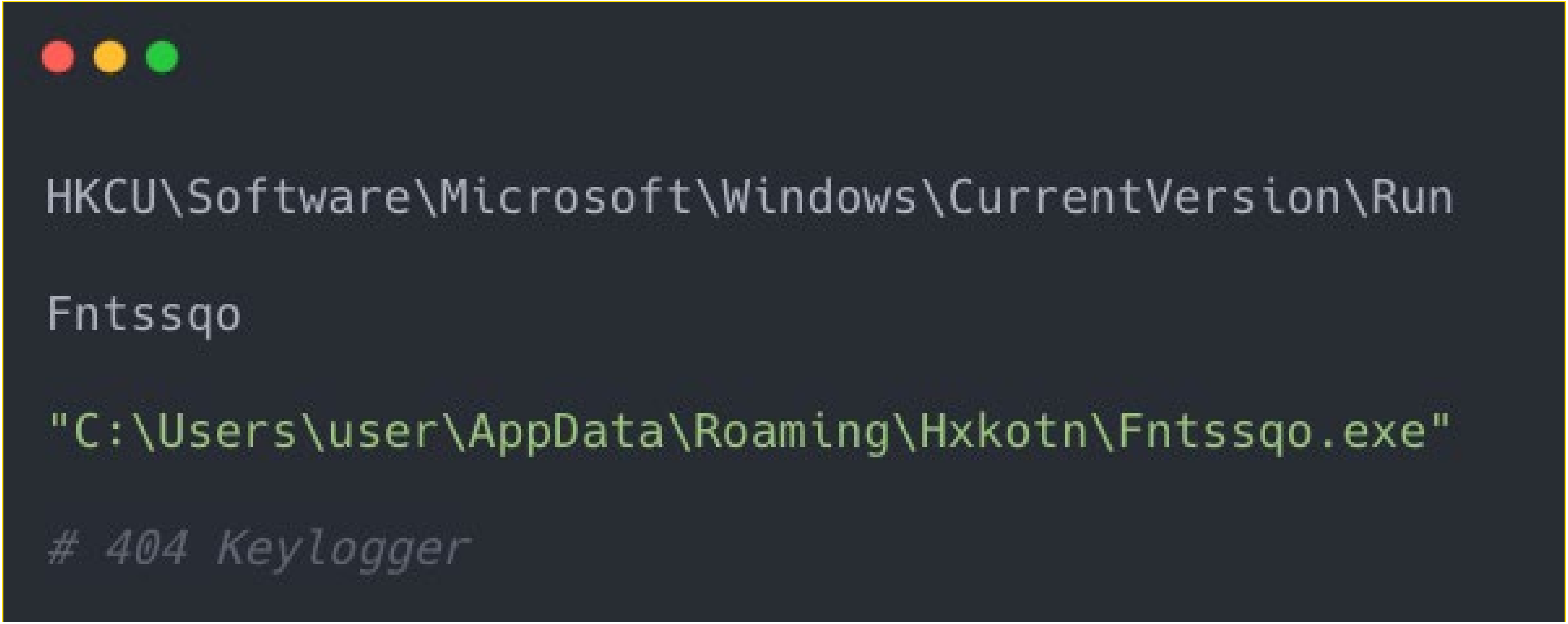
## SECURITY.EVTX

- 4698: A scheduled task was created
- 4699: A scheduled task was deleted
- 4700: A scheduled task was enabled
- 4701: A scheduled task was disabled
- 4702: A scheduled task was updated

## MICROSOFT-WINDOWS-TASKSCHEDULER%4OPERATIONAL.EVTX

- 140: User <user> updated Task Scheduler task <task_name>
- 141: User <user> deleted Task Scheduler task <task_name>

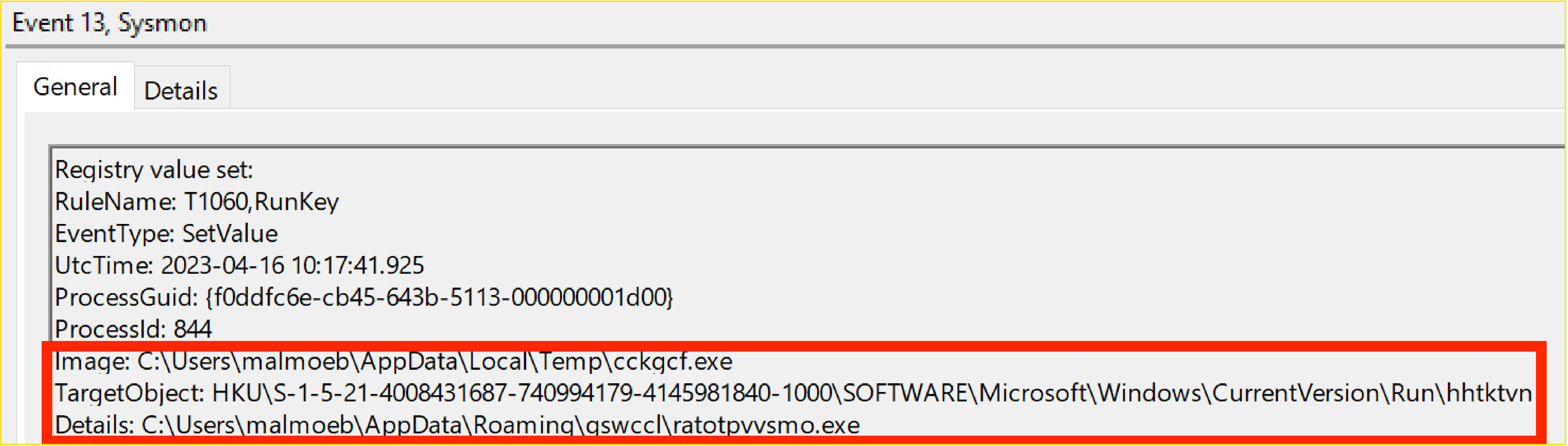
# IOC #4: RUN KEYS



```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Fntssqo

"C:\Users\user\AppData\Roaming\Hxkotn\Fntssqo.exe"

# 404 Keylogger
```

| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| ☒ | ☑ | ☑ | ☒ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

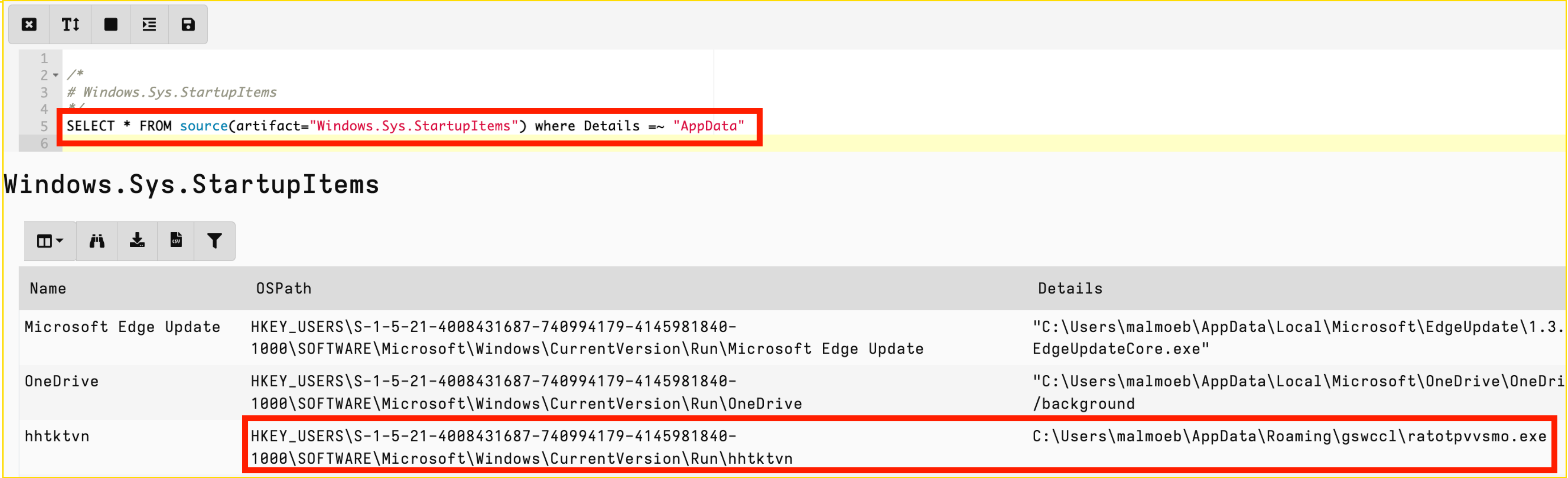
# ARTIFACTS: SYSMON EVENT ID 13 - REGISTRY SET



```
Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2023-04-16 10:17:41.925
ProcessGuid: {f0ddfc6e-cb45-643b-5113-000000001d00}
ProcessId: 844
Image: C:\Users\malmoeb\AppData\Local\Temp\cckgcf.exe
TargetObject: HKU\S-1-5-21-4008431687-740994179-4145981840-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\hhtktvn
Details: C:\Users\malmoeb\AppData\Roaming\gswccl\ratotpvvsmo.exe
```

# ARTIFACTS: WHEN IN DOUBT..

```
KeyGlobs
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run*
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*
HKEY_USERS*\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
HKEY_USERS*\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run*
HKEY_USERS*\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*
```

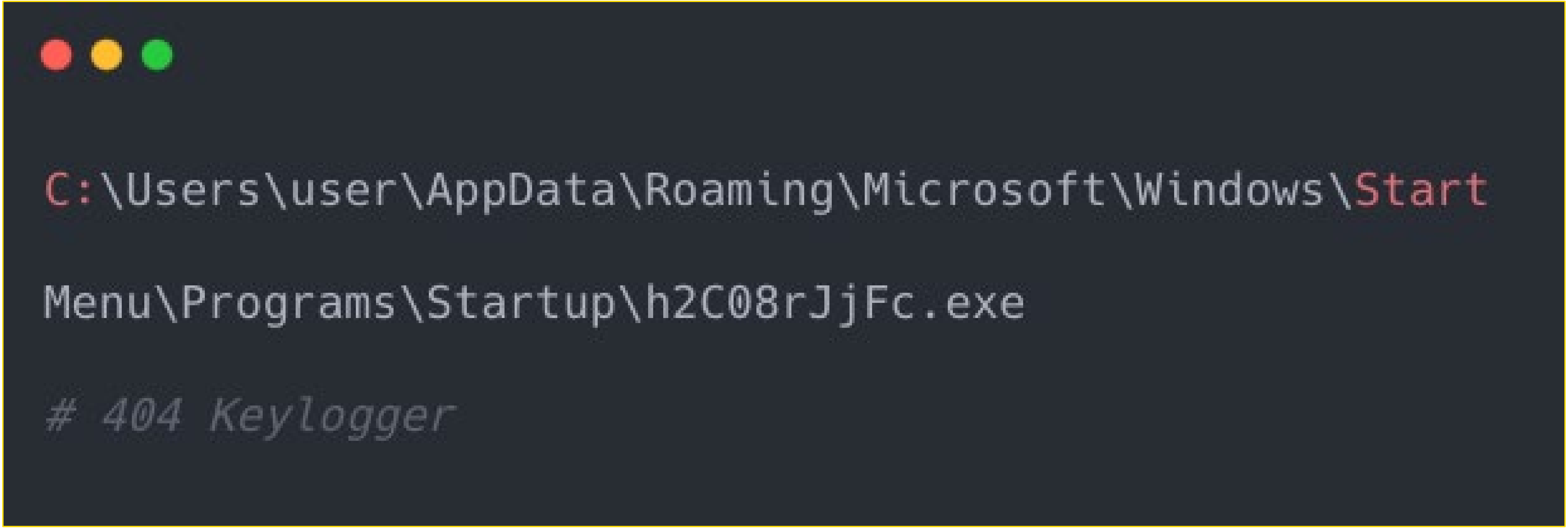


```

/*
# Windows.Sys.StartupItems
*/
SELECT * FROM source(artifact="Windows.Sys.StartupItems") where Details =~ "AppData"

```

## Windows.Sys.StartupItems

| Name | OSPath | Details |
|---|---|---|
| Microsoft Edge Update | HKEY_USERS\S-1-5-21-4008431687-740994179-4145981840-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Edge Update | "C:\Users\malmoeb\AppData\Local\Microsoft\EdgeUpdate\1.3. EdgeUpdateCore.exe" |
| OneDrive | HKEY_USERS\S-1-5-21-4008431687-740994179-4145981840-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OneDrive | "C:\Users\malmoeb\AppData\Local\Microsoft\OneDrive\OneDri /background |
| hhtktvn | HKEY_USERS\S-1-5-21-4008431687-740994179-4145981840-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\hhtktvn | C:\Users\malmoeb\AppData\Roaming\gswccl\ratotpvvsmo.exe |

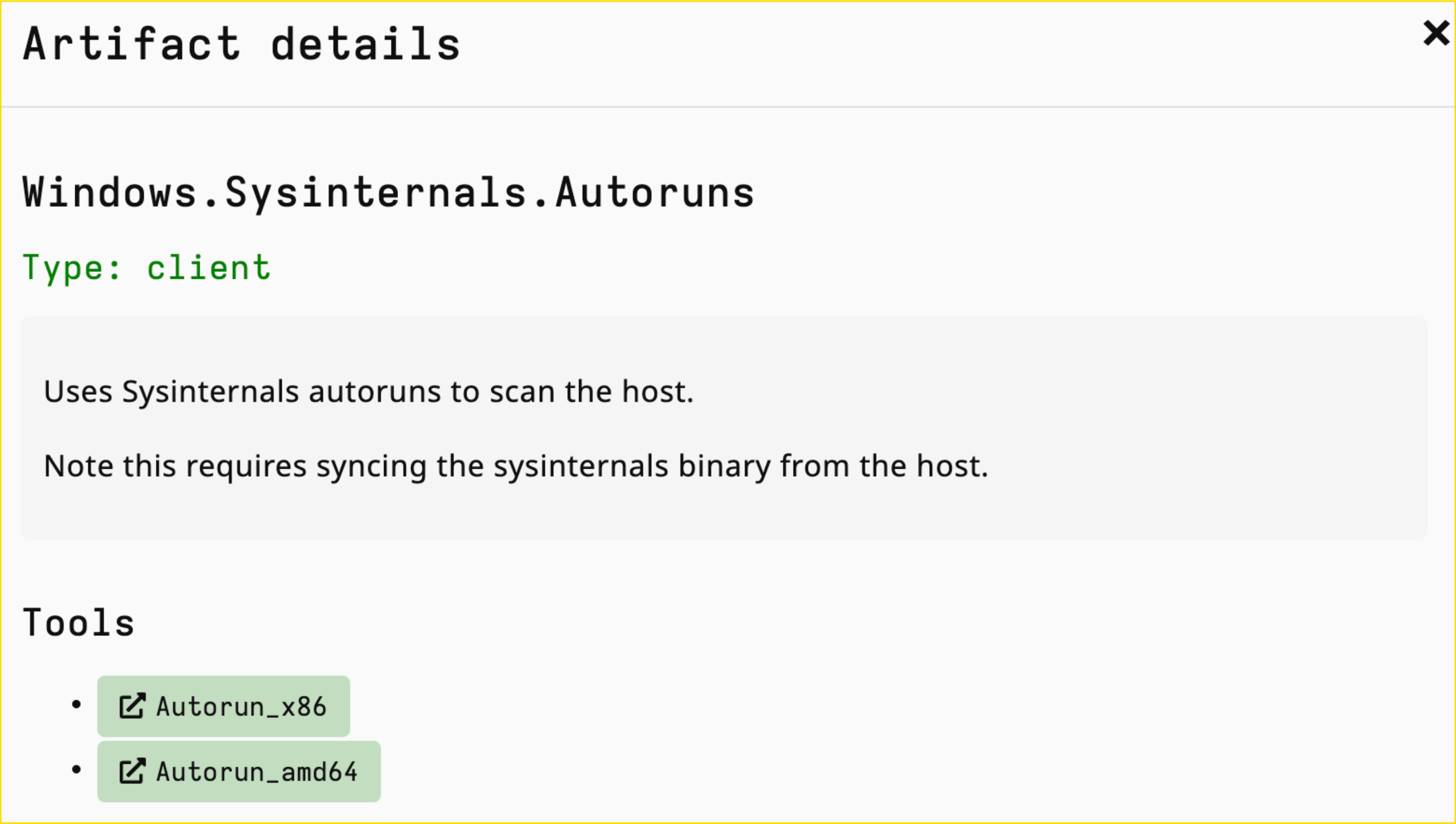
# IOC #5: STARTUP FOLDER



```
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\h2C08rJjFc.exe
# 404 Keylogger
```

| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| ☒ | ☑ | ☑ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☑ |

# ARTIFACTS: AUTORUNS



Artifact details

×

Windows.Sysinternals.Autoruns

Type: client

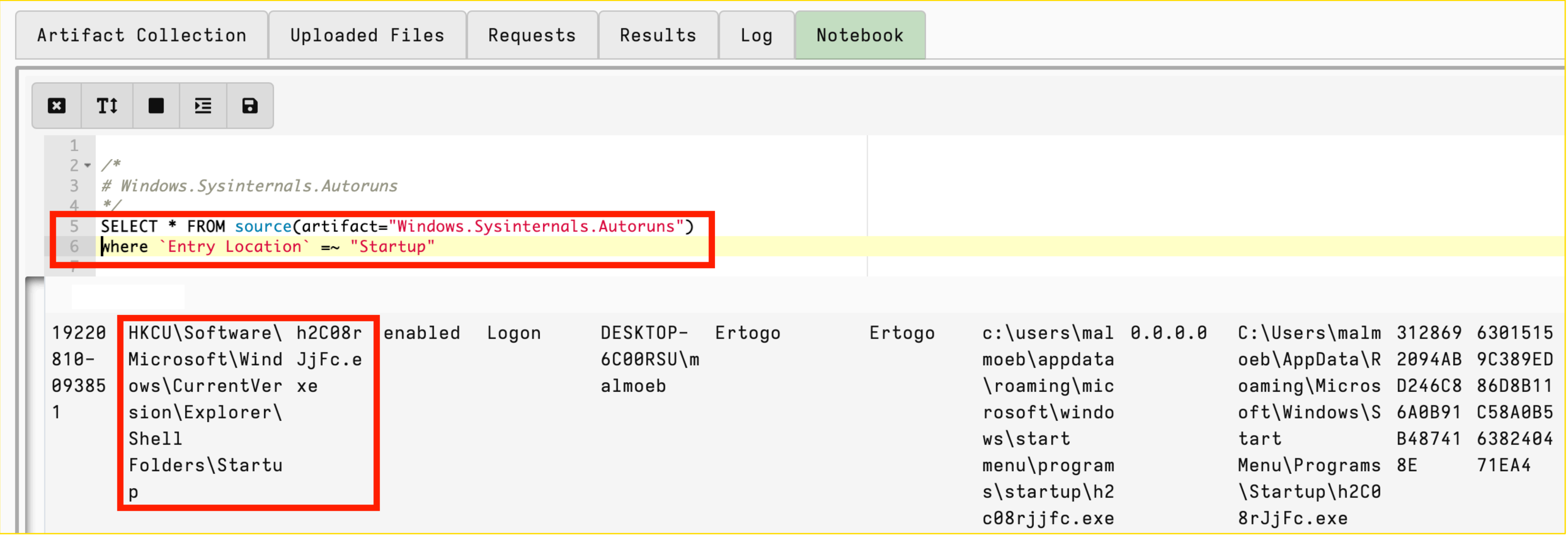
Uses Sysinternals autoruns to scan the host.

Note this requires syncing the sysinternals binary from the host.

Tools

- Autorun_x86
- Autorun_amd64

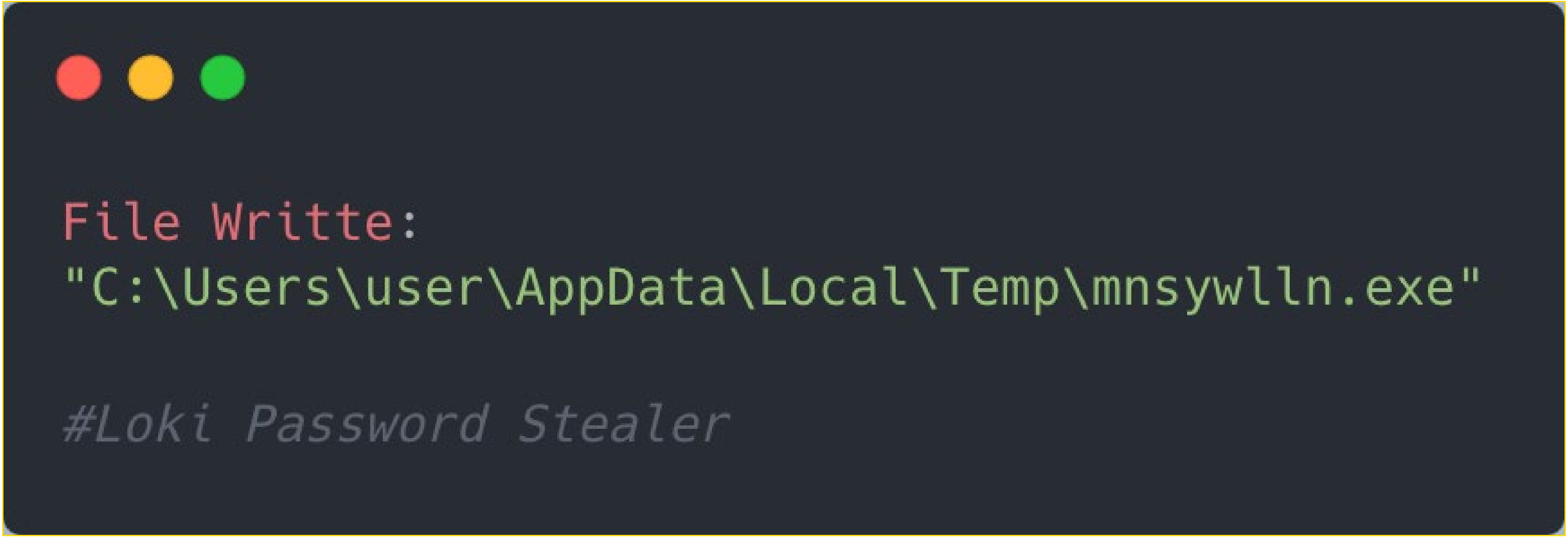
# ARTIFACTS: AUTORUNS



```
/*
# Windows.Sysinternals.Autoruns
*/
SELECT * FROM source(artifact="Windows.Sysinternals.Autoruns")
where `Entry Location` =~ "Startup"
```

```
19220 HKCU\Software\ h2C08r enabled  Logon   DESKTOP-   Ertogo     Ertogo   c:\users\mal 0.0.0.0   C:\Users\malm 312869 6301515
810-  Microsoft\Wind JjFc.e                  6C00RSU\m                      moeb\appdata           oeb\AppData\R 2094AB 9C389ED
09385 ows\CurrentVer xe                      almoeb                         \roaming\mic           oaming\Micros D246C8 86D8B11
1     sion\Explorer\                                                        rosoft\windo           oft\Windows\S 6A0B91 C58A0B5
      Shell                                                                 ws\start               tart          B48741 6382404
      Folders\Startu                                                        menu\program           Menu\Programs 8E     71EA4
      p                                                                     s\startup\h2           \Startup\h2C0
                                                                            c08rjjfc.exe           8rJjFc.exe
```

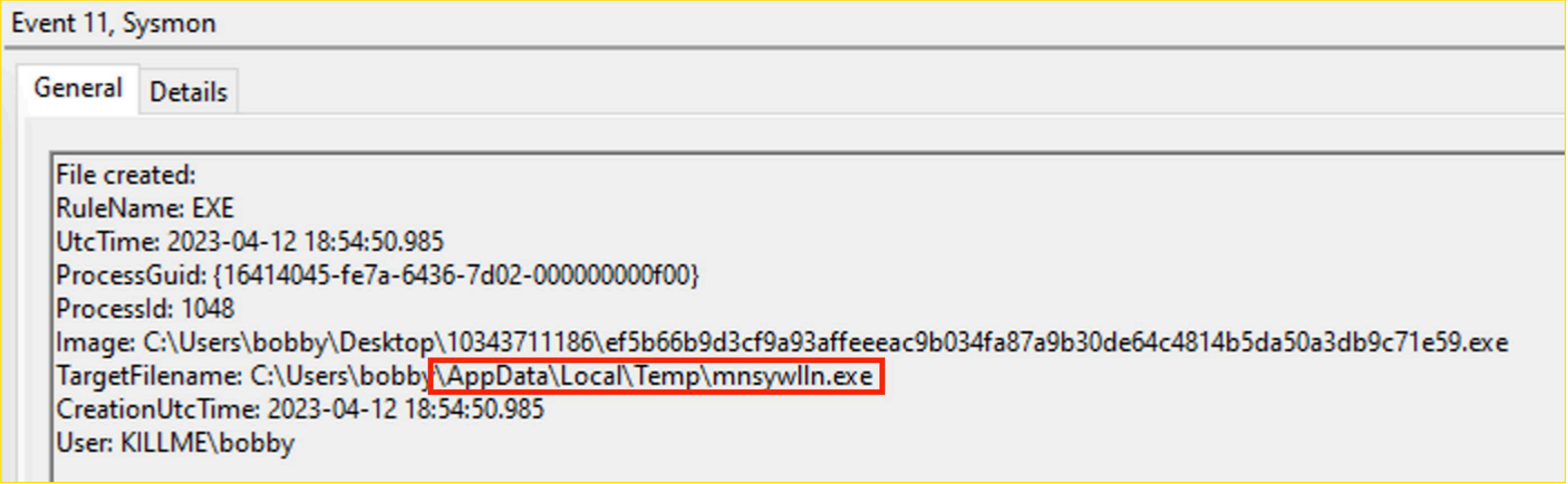
# IOC #6: APPDATA



```
File Writte:
"C:\Users\user\AppData\Local\Temp\mnsywlln.exe"

#Loki Password Stealer
```

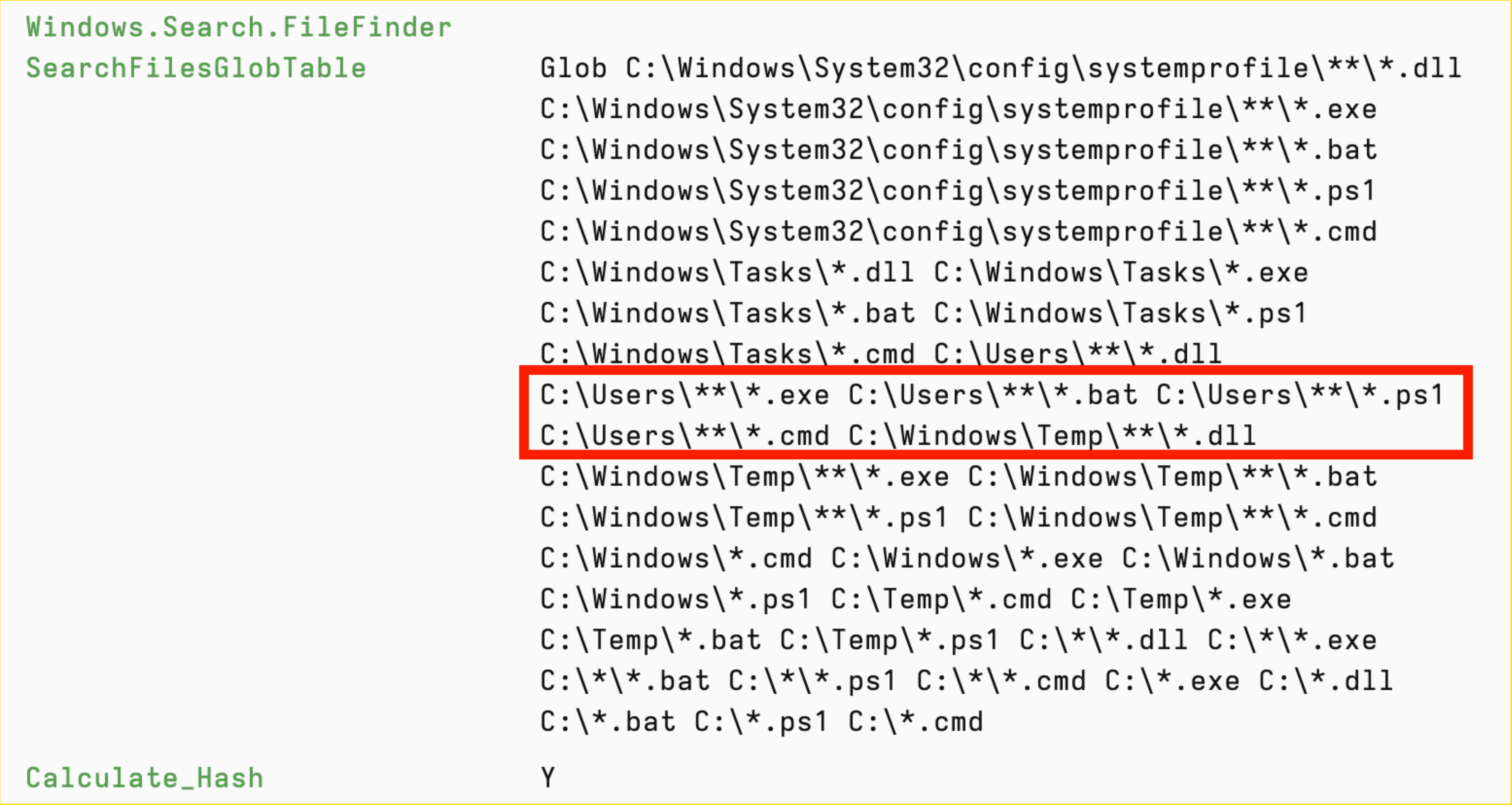
| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

# ARTIFACTS: SYSMON EVENT ID 11 - FILE WRITE



```
File created:
RuleName: EXE
UtcTime: 2023-04-12 18:54:50.985
ProcessGuid: {16414045-fe7a-6436-7d02-000000000f00}
ProcessId: 1048
Image: C:\Users\bobby\Desktop\10343711186\ef5b66b9d3cf9a93affeeeac9b034fa87a9b30de64c4814b5da50a3db9c71e59.exe
TargetFilename: C:\Users\bobby\AppData\Local\Temp\mnsywlln.exe
CreationUtcTime: 2023-04-12 18:54:50.985
User: KILLME\bobby
```

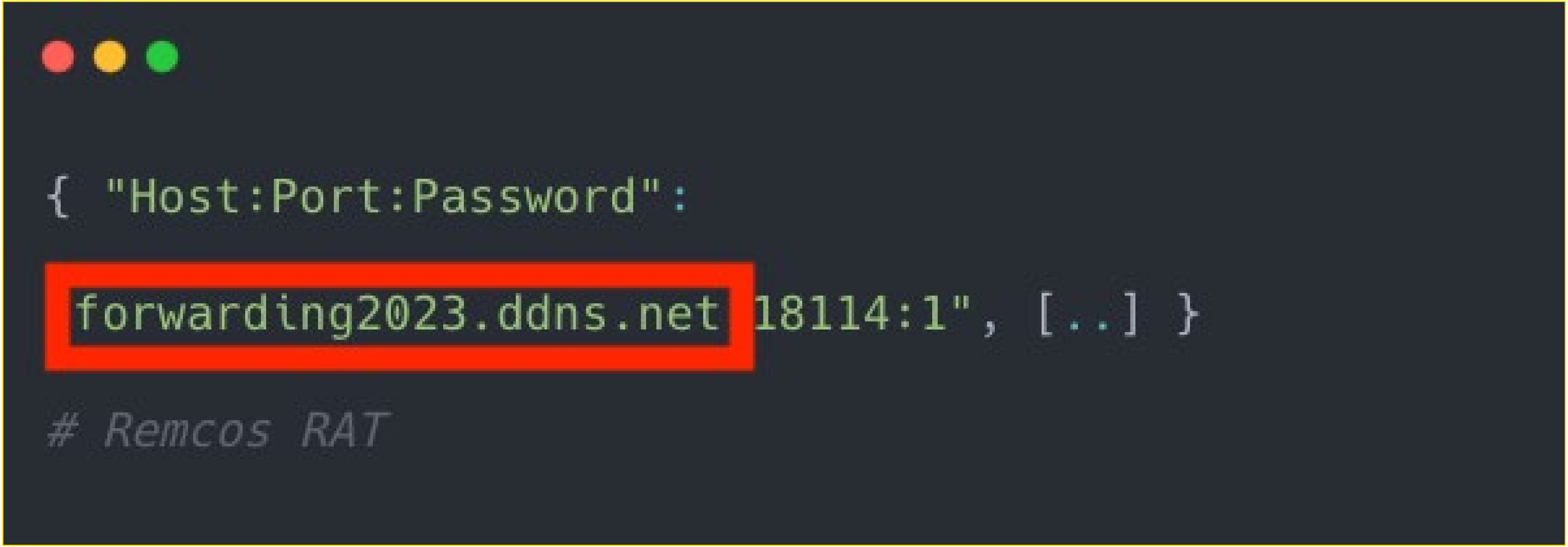
# ARTIFACTS: FILEFINDER (VELOCIRAPTOR)



```
Windows.Search.FileFinder
SearchFilesGlobTable          Glob C:\Windows\System32\config\systemprofile\**\*.dll
                              C:\Windows\System32\config\systemprofile\**\*.exe
                              C:\Windows\System32\config\systemprofile\**\*.bat
                              C:\Windows\System32\config\systemprofile\**\*.ps1
                              C:\Windows\System32\config\systemprofile\**\*.cmd
                              C:\Windows\Tasks\*.dll C:\Windows\Tasks\*.exe
                              C:\Windows\Tasks\*.bat C:\Windows\Tasks\*.ps1
                              C:\Windows\Tasks\*.cmd C:\Users\**\*.dll
                              C:\Users\**\*.exe C:\Users\**\*.bat C:\Users\**\*.ps1
                              C:\Users\**\*.cmd C:\Windows\Temp\**\*.dll
                              C:\Windows\Temp\**\*.exe C:\Windows\Temp\**\*.bat
                              C:\Windows\Temp\**\*.ps1 C:\Windows\Temp\**\*.cmd
                              C:\Windows\*.cmd C:\Windows\*.exe C:\Windows\*.bat
                              C:\Windows\*.ps1 C:\Temp\*.cmd C:\Temp\*.exe
                              C:\Temp\*.bat C:\Temp\*.ps1 C:\*\*.dll C:\*\*.exe
                              C:\*\*.bat C:\*\*.ps1 C:\*\*.cmd C:\*.exe C:\*.dll
                              C:\*.bat C:\*.ps1 C:\*.cmd

Calculate_Hash                Y
```

# EXTRA MILE: C:\USERS\PUBLIC

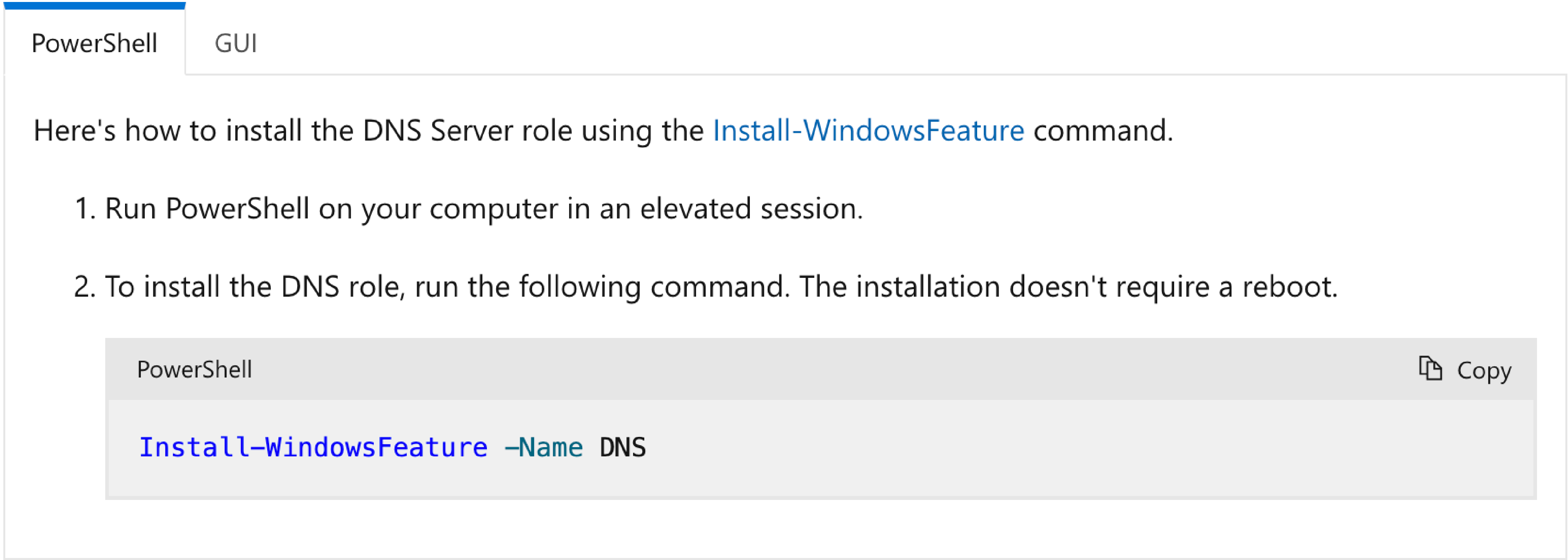
# IOC #7: DYNDNS



```
{ "Host:Port:Password":
forwarding2023.ddns.net 18114:1", [..] }
# Remcos RAT
```

| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| ☒ | ☒ | ☑ | ☒ | ☑ | ☑ | ☑ | ☒ | ☒ | ☑ |

# ARTIFACTS: DNS LOGS



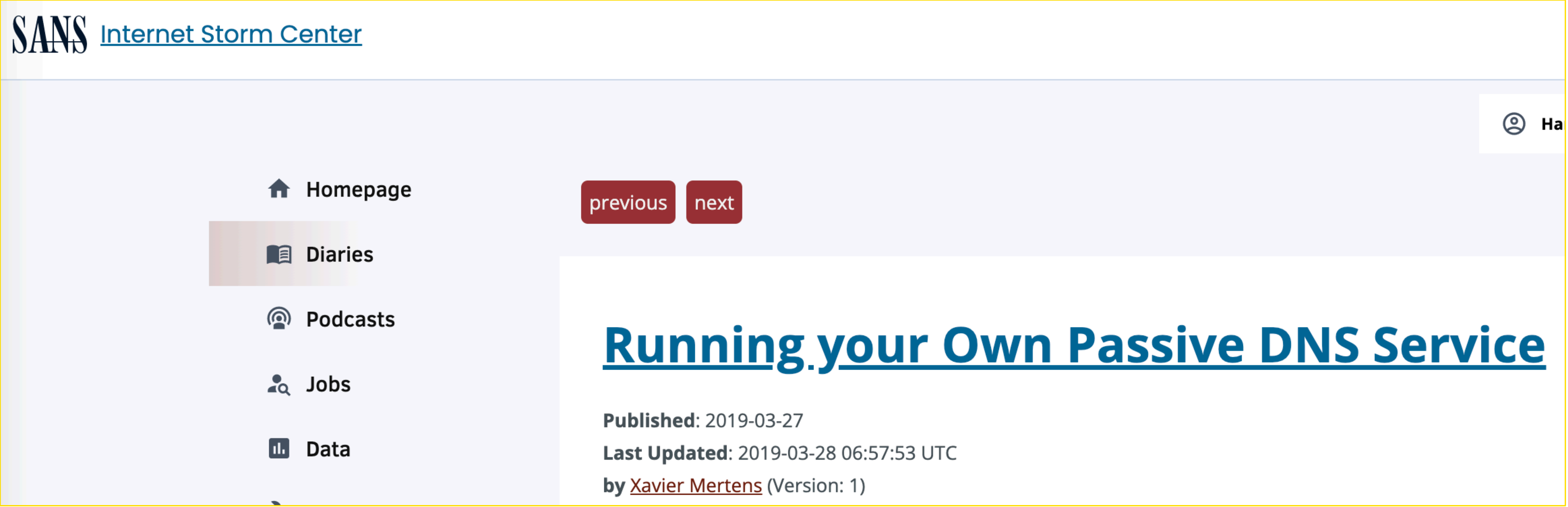
Here's how to install the DNS Server role using the Install-WindowsFeature command.

1. Run PowerShell on your computer in an elevated session.
2. To install the DNS role, run the following command. The installation doesn't require a reboot.

```
Install-WindowsFeature -Name DNS
```

*Source: learn.microsoft.com*

# ARTIFACTS: PASSIVE DNS

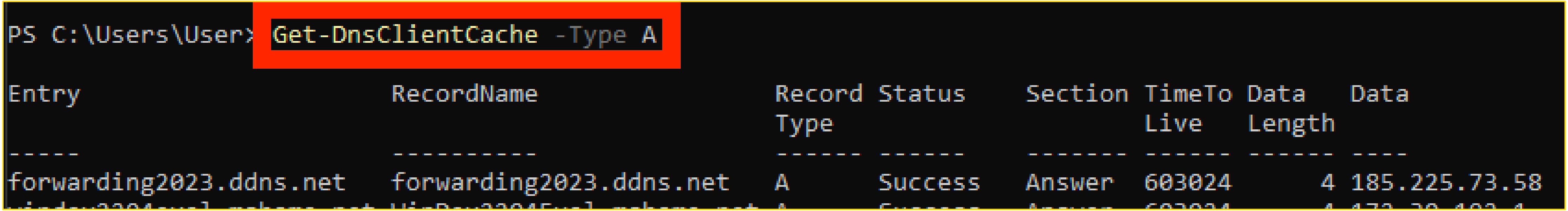


## Running your Own Passive DNS Service

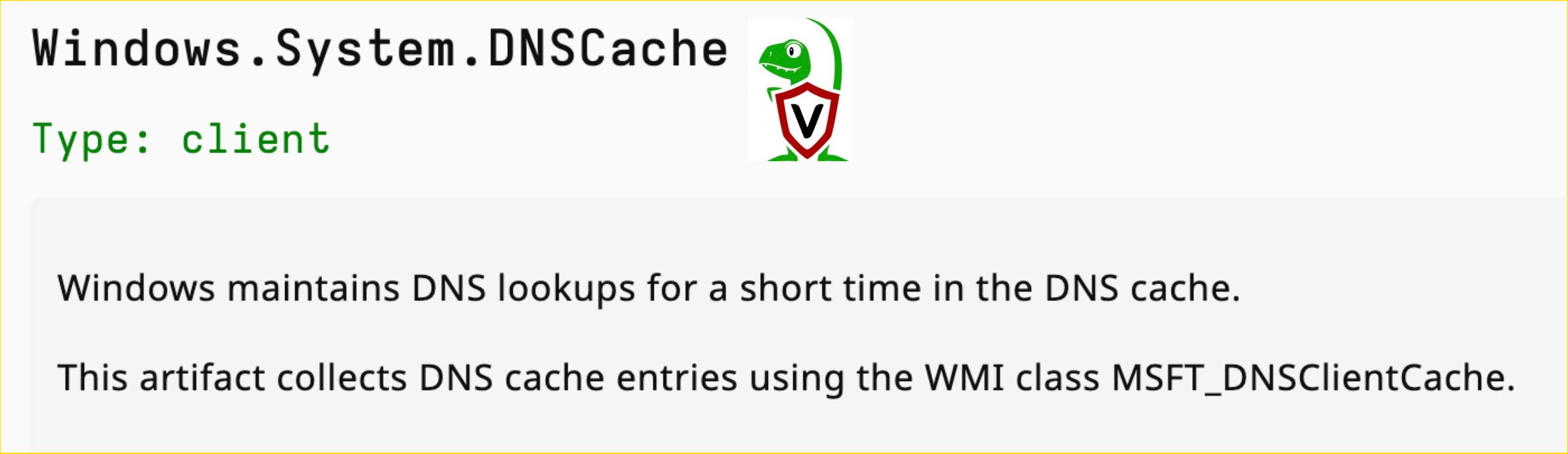
**Published**: 2019-03-27
**Last Updated**: 2019-03-28 06:57:53 UTC
by Xavier Mertens (Version: 1)

*Source: isc.sand.edu*

# ARTIFACTS: DNS CACHE



```
PS C:\Users\User> Get-DnsClientCache -Type A

Entry                   RecordName              Record Status   Section TimeTo Data   Data
                                                Type                    Live   Length
-----                   ----------              ------ ------   ------- ------ ------ ----
forwarding2023.ddns.net forwarding2023.ddns.net A      Success  Answer  603024      4 185.225.73.58
```



## Windows.System.DNSCache

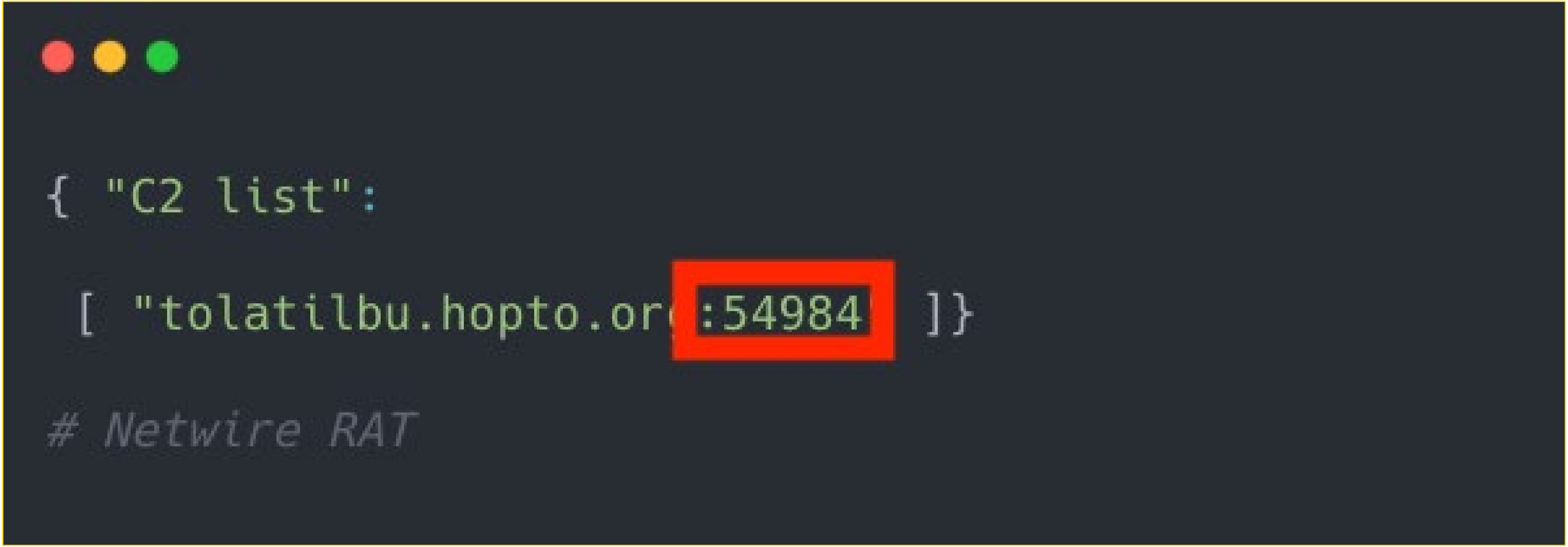
Type: client

Windows maintains DNS lookups for a short time in the DNS cache.

This artifact collects DNS cache entries using the WMI class MSFT_DNSClientCache.

Source: Velociraptor

# IOC #8: HIGH-PORT || IP-ONLY



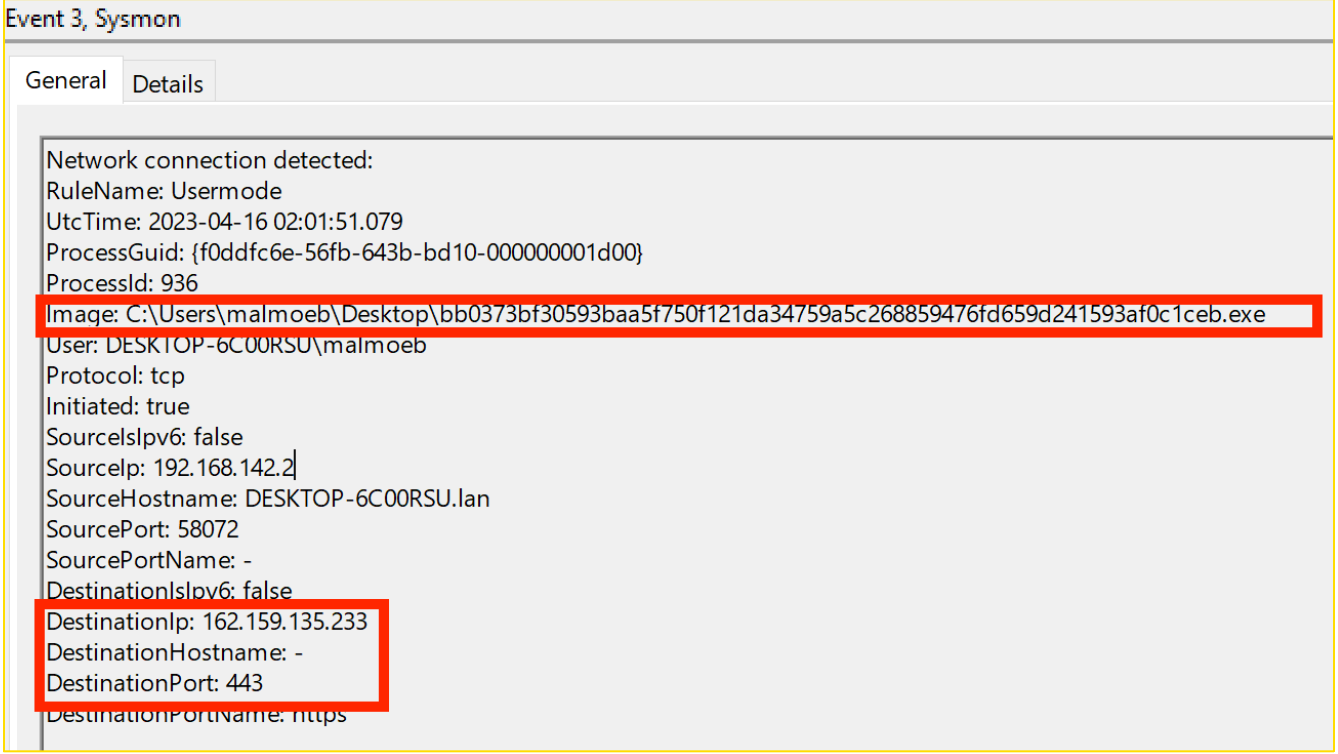
```
{ "C2 list":

  [ "tolatilbu.hopto.org:54984  ]}

# Netwire RAT
```

| AT | FB | 404 | LPS | AM | RC | NCR | QB | RLS | NWR |
|---|---|---|---|---|---|---|---|---|---|
| ☒ | ☒ | ☒ | ☒ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

# ARTIFACTS: FIREWALL LOGS

## MIGHT BE NOISY!

## BETTER FILTER ON THE IMAGE (SYSMON EVENT ID 3) *404 Keylogger sample below*



```
Network connection detected:
RuleName: Usermode
UtcTime: 2023-04-16 02:01:51.079
ProcessGuid: {f0ddfc6e-56fb-643b-bd10-000000001d00}
ProcessId: 936
Image: C:\Users\malmoeb\Desktop\bb0373bf30593baa5f750f121da34759a5c268859476fd659d241593af0c1ceb.exe
User: DESKTOP-6C00RSU\malmoeb
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.142.2
SourceHostname: DESKTOP-6C00RSU.lan
SourcePort: 58072
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 162.159.135.233
DestinationHostname: -
DestinationPort: 443
DestinationPortName: https
```

# RECAP

- Defender Exclusions
- Powershell
- Scheduled Tasks
- Run Keys
- Startup Folder
- AppData
- DNS Logs
- High Port || IP Only

# CASE SOLVED: CATCHING EVIL ON THE FLY!

June 8, 2023 15:50-16:25

## CASE SOLVED: CATCHING EVIL ON THE FLY

Andreas Klaus and Sandro Bachmann
InfoGuard AG

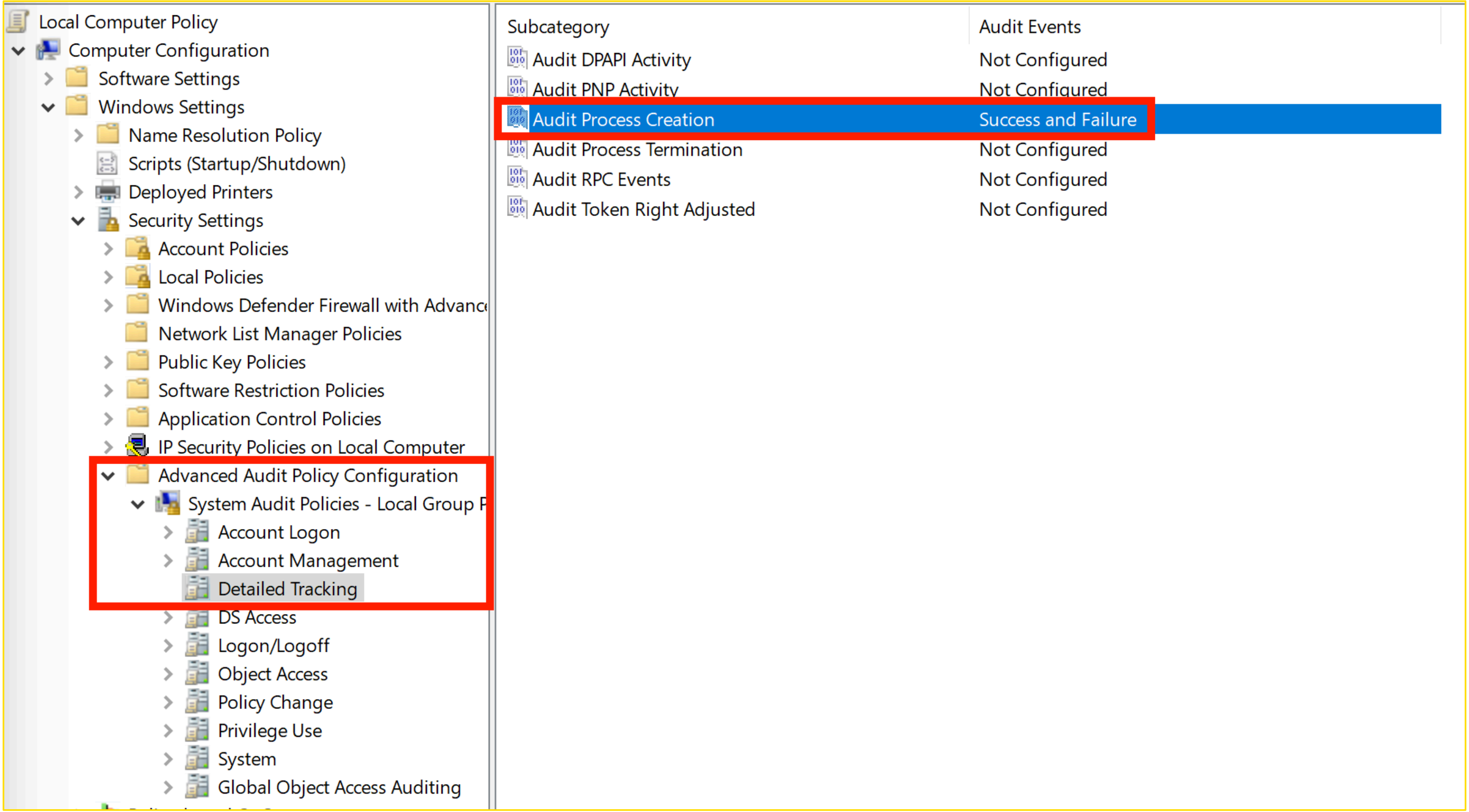
InfoGuard
SWISS CYBER SECURITY

# QUESTIONS?

Twitter

LinkedIn

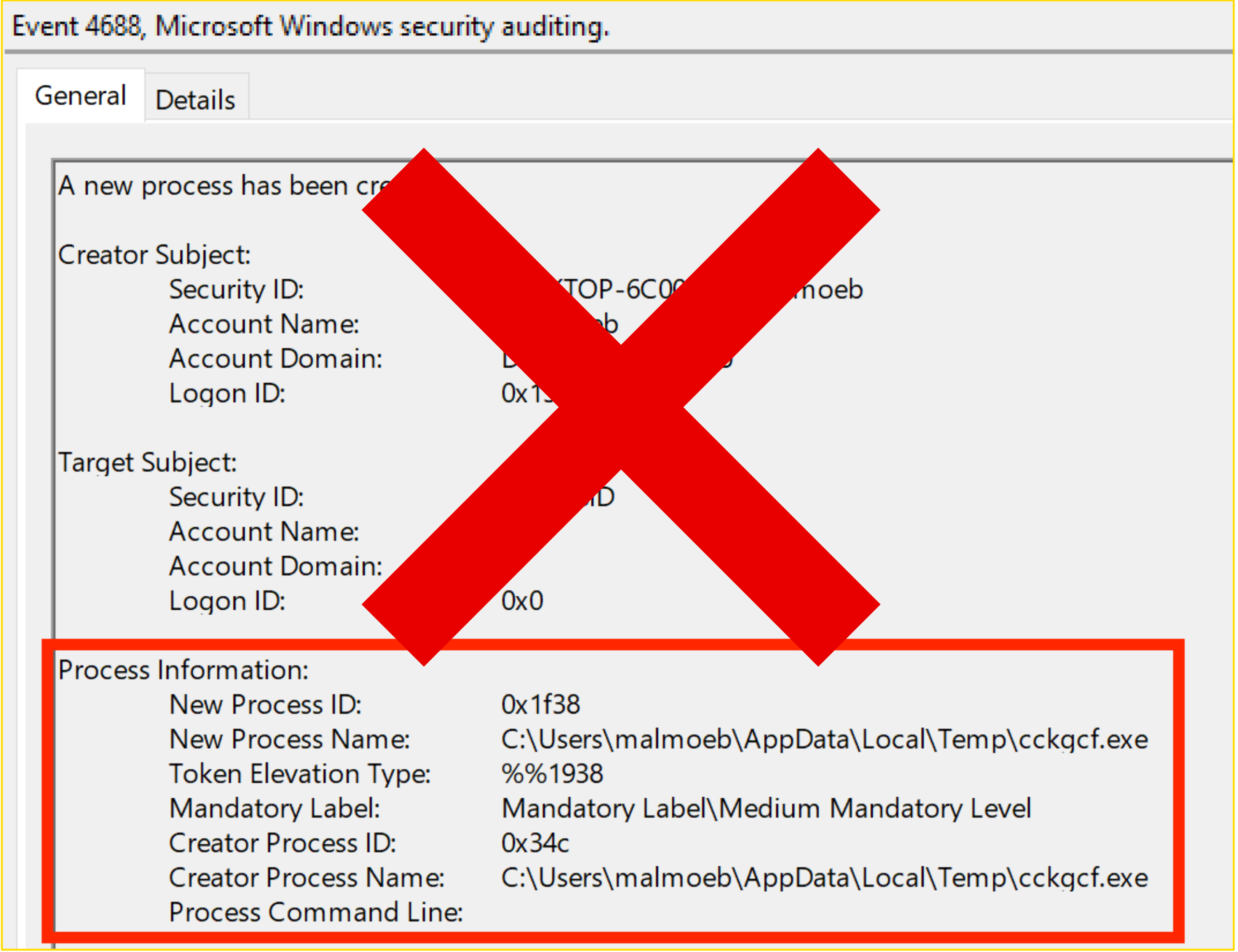
# ARTIFACTS: 4688 REGEDIT



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Windows Defender Firewall with Advanc
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
          - System Audit Policies - Local Group P
            - Account Logon
            - Account Management
            - Detailed Tracking
            - DS Access
            - Logon/Logoff
            - Object Access
            - Policy Change
            - Privilege Use
            - System
            - Global Object Access Auditing

| Subcategory | Audit Events |
|---|---|
| Audit DPAPI Activity | Not Configured |
| Audit PNP Activity | Not Configured |
| Audit Process Creation | Success and Failure |
| Audit Process Termination | Not Configured |
| Audit RPC Events | Not Configured |
| Audit Token Right Adjusted | Not Configured |

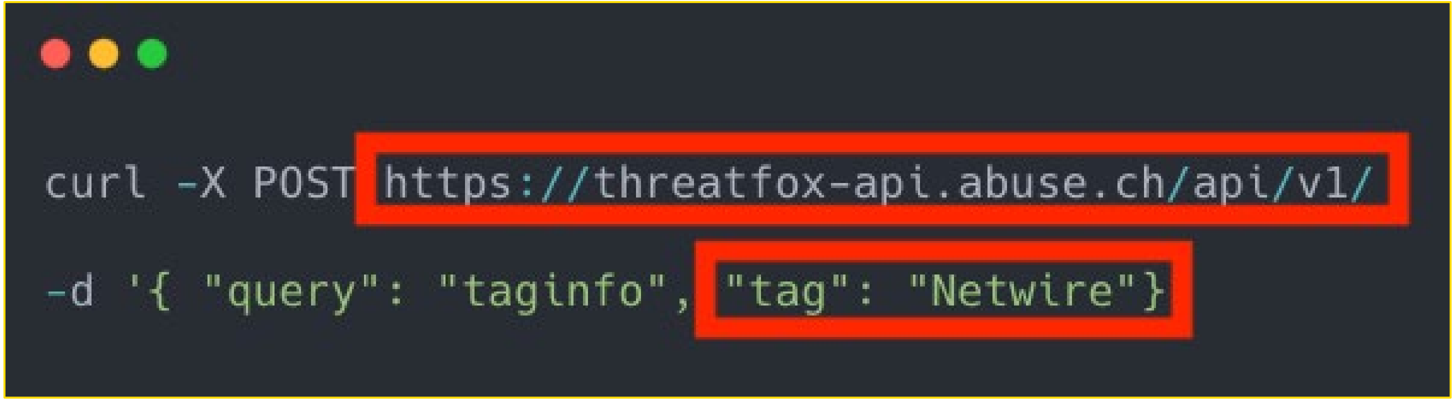
# ARTIFACTS: «ONLY» PROCESS INFORMATION



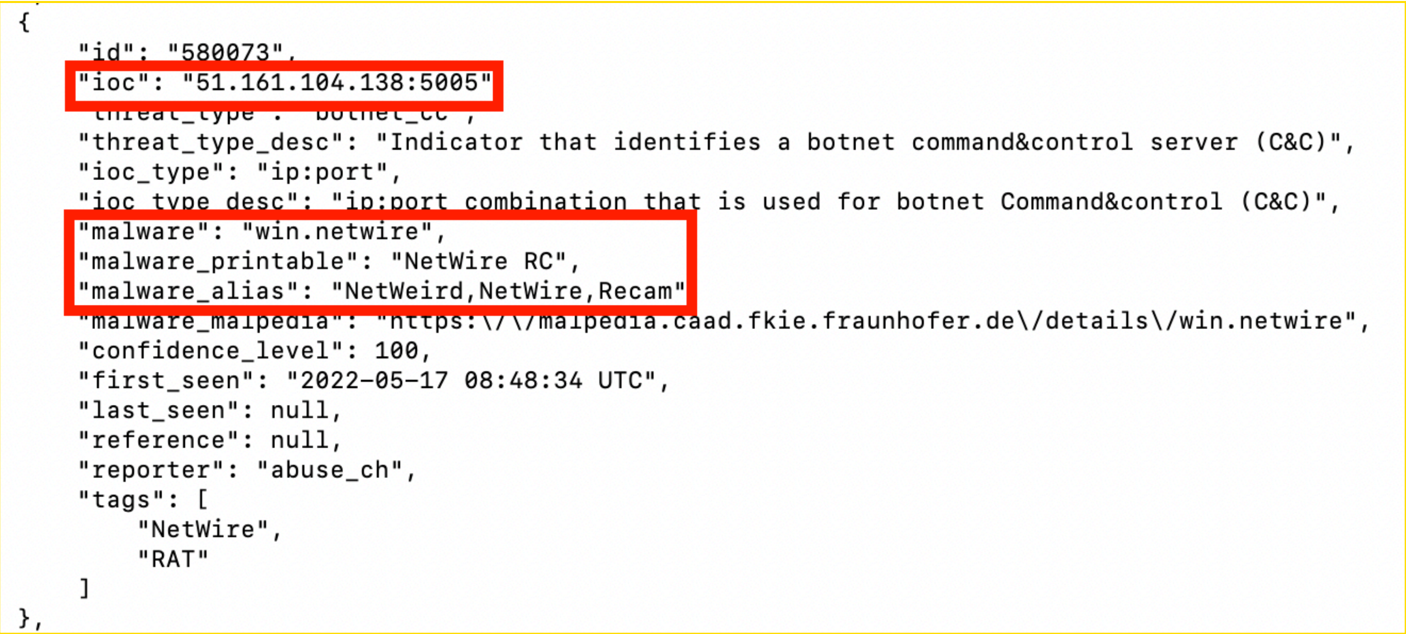
Event 4688, Microsoft Windows security auditing.

```
A new process has been cre

Creator Subject:
        Security ID:            TOP-6C0          moeb
        Account Name:                  b
        Account Domain:         D
        Logon ID:               0x1

Target Subject:
        Security ID:                   D
        Account Name:
        Account Domain:
        Logon ID:               0x0

Process Information:
        New Process ID:         0x1f38
        New Process Name:       C:\Users\malmoeb\AppData\Local\Temp\cckgcf.exe
        Token Elevation Type:   %%1938
        Mandatory Label:        Mandatory Label\Medium Mandatory Level
        Creator Process ID:     0x34c
        Creator Process Name:   C:\Users\malmoeb\AppData\Local\Temp\cckgcf.exe
        Process Command Line:
```

# EXTRA MILE: THREATFOX



```
curl -X POST https://threatfox-api.abuse.ch/api/v1/
-d '{ "query": "taginfo", "tag": "Netwire"}
```



```
{
    "id": "580073",
    "ioc": "51.161.104.138:5005"
    "threat_type": "botnet_cc",
    "threat_type_desc": "Indicator that identifies a botnet command&control server (C&C)",
    "ioc_type": "ip:port",
    "ioc_type_desc": "ip:port combination that is used for botnet Command&control (C&C)",
    "malware": "win.netwire",
    "malware_printable": "NetWire RC",
    "malware_alias": "NetWeird,NetWire,Recam"
    "malware_malpedia": "https:\/\/malpedia.caad.fkie.fraunhofer.de\/details\/win.netwire",
    "confidence_level": 100,
    "first_seen": "2022-05-17 08:48:34 UTC",
    "last_seen": null,
    "reference": null,
    "reporter": "abuse_ch",
    "tags": [
        "NetWire",
        "RAT"
    ]
},
```