N-IOC TO RULE THEM ALL
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

<table>
<thead>
<tr>
<th>Rank</th>
<th>Malware Name</th>
<th>3 weeks ago</th>
<th>Last week</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Agent Tesla aka AgentTesla, AgentTesla, NegaRatbot</td>
<td>41.5%</td>
<td>45.5%</td>
</tr>
<tr>
<td>2</td>
<td>Xloader / Formbook aka Formbook</td>
<td>30.9%</td>
<td>25.8%</td>
</tr>
<tr>
<td>3</td>
<td>404 Keylogger aka 404Keylogger, Snake Keylogger</td>
<td>10.6%</td>
<td>9.20%</td>
</tr>
<tr>
<td>4</td>
<td>Loki Password Stealer (PWS) aka Brunina, Loki, LoKibot</td>
<td>1.32%</td>
<td>5.06%</td>
</tr>
<tr>
<td>5</td>
<td>Nanocore RAT aka Nanocore</td>
<td>3.08%</td>
<td>2.76%</td>
</tr>
<tr>
<td>6</td>
<td>Emotet aka Geodo, Herdo</td>
<td>1.65%</td>
<td>5.06%</td>
</tr>
<tr>
<td>7</td>
<td>Ave Maria aka AVE_MAIBA, AveMariaRAT, Warzone RAT</td>
<td>1.84%</td>
<td>5.17%</td>
</tr>
<tr>
<td>8</td>
<td>CloudEYE aka Malodurer, vidtropper</td>
<td>0.88%</td>
<td>0.92%</td>
</tr>
<tr>
<td>9</td>
<td>AsyncRAT</td>
<td>0.44%</td>
<td>0.92%</td>
</tr>
<tr>
<td>10</td>
<td>QakBot aka PinkBot, Qbot, QuakBot</td>
<td>1.20%</td>
<td>1.46%</td>
</tr>
</tbody>
</table>

### Notes and Sources
- Names and aliases according to malware. The percentages show the proportion of analyses from the total number of analyses.
- Source: govcert.ch

## TOP 10 MALWARE SAMPLES
analyzed by GovCERT.ch in May 2022

<table>
<thead>
<tr>
<th>Rank</th>
<th>Malware Name</th>
<th>3 weeks ago</th>
<th>Last week</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Agent Tesla aka AgentTesla, AgentTesla, NegaRatbot</td>
<td>47.7%</td>
<td>39.5%</td>
</tr>
<tr>
<td>2</td>
<td>Xloader / Formbook aka Formbook</td>
<td>17.8%</td>
<td>23.0%</td>
</tr>
<tr>
<td>3</td>
<td>404 Keylogger aka 404Keylogger, Snake Keylogger</td>
<td>12.5%</td>
<td>12.7%</td>
</tr>
<tr>
<td>4</td>
<td>Loki Password Stealer (PWS) aka Brunina, Loki, LoKibot</td>
<td>7.68%</td>
<td>8.46%</td>
</tr>
<tr>
<td>5</td>
<td>Ave Maria aka AVE_MAIBA, AveMariaRAT, Warzone RAT</td>
<td>3.36%</td>
<td>5.17%</td>
</tr>
<tr>
<td>6</td>
<td>Remcos aka RemcosRAT, Remco, Socmer</td>
<td>0.96%</td>
<td>3.35%</td>
</tr>
<tr>
<td>7</td>
<td>Emotet aka Geodo, Herdo</td>
<td>1.32%</td>
<td>2.29%</td>
</tr>
<tr>
<td>8</td>
<td>QakBot aka PinkBot, Qbot, QuakBot</td>
<td>0.94%</td>
<td>0.94%</td>
</tr>
<tr>
<td>9</td>
<td>AsyncRAT</td>
<td>0.44%</td>
<td>0.92%</td>
</tr>
<tr>
<td>10</td>
<td>RedLine Stealer</td>
<td>0.44%</td>
<td>0.47%</td>
</tr>
</tbody>
</table>

### Notes and Sources
- Names and aliases according to malware. The percentages show the proportion of analyses from the total number of analyses.
- Source: govcert.ch

## TOP 10 MALWARE SAMPLES
analyzed by GovCERT.ch in June 2022

<table>
<thead>
<tr>
<th>Rank</th>
<th>Malware Name</th>
<th>3 weeks ago</th>
<th>Last week</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Agent Tesla aka AgentTesla, AgentTesla, NegaRatbot</td>
<td>3.71%</td>
<td>33.0%</td>
</tr>
<tr>
<td>2</td>
<td>Xloader / Formbook aka Formbook</td>
<td>20.2%</td>
<td>21.6%</td>
</tr>
<tr>
<td>3</td>
<td>404 Keylogger aka 404Keylogger, Snake Keylogger</td>
<td>6.90%</td>
<td>18.0%</td>
</tr>
<tr>
<td>4</td>
<td>Remcos aka RemcosRAT, Remco, Socmer</td>
<td>2.30%</td>
<td>6.00%</td>
</tr>
<tr>
<td>5</td>
<td>Ave Maria aka AVE_MAIBA, AveMariaRAT, Warzone RAT</td>
<td>7.36%</td>
<td>6.00%</td>
</tr>
<tr>
<td>6</td>
<td>Emotet aka Geodo, Herdo</td>
<td>1.84%</td>
<td>3.00%</td>
</tr>
<tr>
<td>7</td>
<td>Loki Password Stealer (PWS) aka Brunina, Loki, LoKibot</td>
<td>12.4%</td>
<td>3.00%</td>
</tr>
<tr>
<td>8</td>
<td>RedLine Stealer</td>
<td>1.33%</td>
<td>2.40%</td>
</tr>
<tr>
<td>9</td>
<td>QakBot aka PinkBot, Qbot, QuakBot</td>
<td>1.54%</td>
<td>2.40%</td>
</tr>
<tr>
<td>10</td>
<td>Nanocore RAT aka Nanocore</td>
<td>0.92%</td>
<td>1.20%</td>
</tr>
</tbody>
</table>

### Notes and Sources
- Names and aliases according to malware. The percentages show the proportion of analyses from the total number of analyses.
- Source: govcert.ch
TOP 10 MALWARE FAMILIES (GOVCERT.CH)

- Agent Tesla
- Formbook
- Ave Maria RAT
- Remcos
- Nanocore RAT
- QakBot
- Redline Stealer
- Netwire RAT

Source: April 2022 – December 2022
REVERSE ENGINEERING..
WORK SMARTER, NOT HARDER

DELIVERY MECHANISM CHANGES

ARTIFACTS NOT
### SAMPLES: VX-UNDERGROUND

<table>
<thead>
<tr>
<th>Filename</th>
<th>Hash</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bazaar.2022.09.7z</td>
<td>6596122460</td>
<td>2022-10-17 22:49:31</td>
</tr>
<tr>
<td>Bazaar.2022.10.7z</td>
<td>10390770357</td>
<td>2022-11-01 12:02:31</td>
</tr>
<tr>
<td>Bazaar.2022.11.7z</td>
<td>10385352800</td>
<td>2022-12-02 06:57:17</td>
</tr>
<tr>
<td>Bazaar.2022.12.7z</td>
<td>10117808288</td>
<td>2023-01-01 07:02:50</td>
</tr>
<tr>
<td>Bazaar.2023.01.7z</td>
<td>10584395712</td>
<td>2023-02-01 08:36:56</td>
</tr>
<tr>
<td>Bazaar.2023.02.7z</td>
<td>9919966899</td>
<td>2023-03-01 23:14:34</td>
</tr>
<tr>
<td>Bazaar.2023.03.7z</td>
<td>6219214521</td>
<td>2023-04-05 22:06:25</td>
</tr>
</tbody>
</table>
IOC #1: DEFENDER EXCLUSIONS

Add-MpPreference -ExclusionPath

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

# Nanocore RAT
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
ARTIFACTS: REGISTRY

Administrator: Command Prompt

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**

```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
```

<table>
<thead>
<tr>
<th>AT</th>
<th>FB</th>
<th>404</th>
<th>LPS</th>
<th>AM</th>
<th>RC</th>
<th>NCR</th>
<th>QB</th>
<th>RLS</th>
<th>NWR</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>✗</td>
<td>✔️</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
ARTIFACTS: EVENT 4104
Event 4104, PowerShell (Microsoft-Windows-PowerShell)

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...
IOC #3: SCHEDULED TASKS

```bash
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
```
**Artifact details**

**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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TasksPath</td>
<td>String</td>
<td>c:/Windows/System32/Tasks/*</td>
<td></td>
</tr>
</tbody>
</table>
## ARTIFACTS: TASKS WITH COMMAND & LAUNCHSTRING

<table>
<thead>
<tr>
<th>Task Location</th>
<th>Command/Path</th>
<th>Launchstring</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>C:\Windows\System32\Tasks\OneDrive Standalone Update</code></td>
<td><code>%localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdate</code></td>
<td><code>r.exe</code></td>
</tr>
<tr>
<td><code>C:\Windows\System32\Tasks\npcapwatchdog</code></td>
<td><code>C:\Program Files\Npcap\CheckStatus.bat</code></td>
<td></td>
</tr>
<tr>
<td><code>C:\Windows\System32\Tasks\rvocgveq</code></td>
<td><code>regsvr32.exe</code></td>
<td><code>-s &quot;C:\Users\User\Desktop\op\FIRST\qbot.dll&quot;</code></td>
</tr>
<tr>
<td><code>C:\Windows\System32\Tasks\Microsoft\VisualStudio\VSIX Auto Update</code></td>
<td><code>C:\Program Files (x86)\Microsoft Visual Studio\Installer\resources\app\ServiceHub\Services\Microsof</code></td>
<td><code>ft.VisualStudio.Setup.Service\VSIXAutoUpdate.exe</code></td>
</tr>
</tbody>
</table>
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
**ARTIFACTS:** SYSMON EVENT ID 13 - REGISTRY SET

**Event 13, Sysmon**

*General*

- Registry value set:
- RuleName: T1060, RunKey
- EventType: SetValue
- UtcTime: 2023-04-16 10:17:41.925
- ProcessGuid: {f0ddfc6e-cb45-643b-5113-000000001d00}
- ProcessId: 844

**Details**

- Image: C:\Users\malmoeb\AppData\Local\Temp\cckqcf.exe
- TargetObject: HKUS-1-5-21-4008431687-740994179-4145981840-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\hhtktvn
- Details: C:\Users\malmoeb\AppData\Roaming\gswcc\ratotpvyvmo.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

<table>
<thead>
<tr>
<th>Name</th>
<th>OPath</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Edge Update</td>
<td>HKEY_USERS\S-1-5-21-4088431687-740994179-4145981840-1081\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Edge Update</td>
<td>&quot;C:\Users\malmoeb\AppData\Local\Microsoft\EdgeUpdate\1.3.EdgeUpdateCore.exe&quot;</td>
</tr>
<tr>
<td>OneDrive</td>
<td>HKEY_USERS\S-1-5-21-4088431687-740994179-4145981840-1081\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OneDrive</td>
<td>&quot;C:\Users\malmoeb\AppData\Local\Microsoft\OneDrive\OneDrive\background&quot;</td>
</tr>
<tr>
<td>httktvn</td>
<td>HKEY_USERS\S-1-5-21-4088431687-740994179-4145981840-1081\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\httktvn</td>
<td>C:\Users\malmoeb\AppData\Roaming\gsym\rtotpvvsmo.exe</td>
</tr>
</tbody>
</table>
IOC #5: STARTUP FOLDER

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

# 404 Keylogger
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
```sql
SELECT * FROM `source(Artifact="Windows.Sysinternals.Autoruns")` WHERE 'Entry Location' = ' "Startup"'
```
IOC #6: APPDATA

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

#Loki Password Stealer
ARTIFACTS: SYSMON EVENT ID 11 - FILE WRITE

Event 11, Sysmon

**General**
- File created: [Details]
- RuleName: EXE
- UtcTime: 2023-04-12 18:54:50.985
- ProcessGuid: {16414045-fe7a-6436-7d02-0000000000f00}
- ProcessId: 1048
- Image: C:\Users\bobby\Desktop\10343711186\ef5b66b9d3cf9a93affeeeaec9b034fa87a9b30de64c4814b5da50a3db9c71e59.exe
- TargetFilename: C:\Users\bobby\AppData\Local\Temp\mnsywlln.exe
- CreationUtcTime: 2023-04-12 18:54:50.985
- User: KILLME\bobby

**Details**

In the image, the highlighted file path and filename indicate a file write event captured by the Sysmon tool. The event details include the file path `C:\Users\bobby\AppData\Local\Temp\mnsywlln.exe`, which is a potentially malicious file being written to the temporary directory on the user's system.
Windows.Search.FileFinder
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

```json
{
  "Host:Port:Password":
  "forwarding2023.ddns.net:18114:1",
  "[...]
```

# Remcos RAT

<table>
<thead>
<tr>
<th></th>
<th>AT</th>
<th>FB</th>
<th>404</th>
<th>LPS</th>
<th>AM</th>
<th>RC</th>
<th>NCR</th>
<th>QB</th>
<th>RLS</th>
<th>NWR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
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.

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

Source: learn.microsoft.com
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

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

```json
{ "C2 list":
  [ "tolatilbu.hopto.org:54984"
}
# Netwire RAT
```

<table>
<thead>
<tr>
<th>AT</th>
<th>FB</th>
<th>404</th>
<th>LPS</th>
<th>AM</th>
<th>RC</th>
<th>NCR</th>
<th>QB</th>
<th>RLS</th>
<th>NWR</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
ARTIFACTS: FIREWALL LOGS

MIGHT BE NOISY!

BETTER FILTER ON THE IMAGE (SYSMON EVENT ID 3) 404 Keylogger sample below.
<table>
<thead>
<tr>
<th>RECAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defender Exclusions</td>
</tr>
<tr>
<td>Powershell</td>
</tr>
<tr>
<td>Scheduled Tasks</td>
</tr>
<tr>
<td>Run Keys</td>
</tr>
<tr>
<td>Startup Folder</td>
</tr>
<tr>
<td>AppData</td>
</tr>
<tr>
<td>DNS Logs</td>
</tr>
<tr>
<td>High Port</td>
</tr>
</tbody>
</table>
June 8, 2023 15:50-16:25

CASE SOLVED: CATCHING EVIL ON THE FLY

Andreas Klaus and Sandro Bachmann
InfoGuard AG

CASE SOLVED: CATCHING EVIL ON THE FLY!
QUESTIONS?

Twitter

LinkedIn
## ARTIFACTS: 4688 REGEDIT

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit DPAPI Activity</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Audit RBP Activity</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Audit Process Creation</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Process Termination</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Audit RPC Events</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Audit Token Right Adjusted</td>
<td>Not Configured</td>
</tr>
</tbody>
</table>
**ARTIFACTS:** «ONLY» PROCESS INFORMATION

<table>
<thead>
<tr>
<th>Event 4688, Microsoft Windows security auditing.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td><strong>Creator Subject:</strong></td>
</tr>
<tr>
<td>Security ID: T0P-6C09-1E6b5b55-9018-4550-9f71-9a4293475de3</td>
</tr>
<tr>
<td>Account Name:</td>
</tr>
<tr>
<td>Account Domain:</td>
</tr>
<tr>
<td>Logon ID: 0x154626d0013</td>
</tr>
<tr>
<td><strong>Target Subject:</strong></td>
</tr>
<tr>
<td>Security ID:</td>
</tr>
<tr>
<td>Account Name:</td>
</tr>
<tr>
<td>Account Domain:</td>
</tr>
<tr>
<td>Logon ID: 0x0</td>
</tr>
<tr>
<td><strong>Process Information:</strong></td>
</tr>
<tr>
<td>New Process ID: 0x1f38</td>
</tr>
<tr>
<td>New Process Name: C:\Users\malmoeb\AppData\Local\Temp\cckqcf.exe</td>
</tr>
<tr>
<td>Token Elevation Type: %1938</td>
</tr>
<tr>
<td>Mandatory Label: Mandatory Label\Medium Mandatory Level</td>
</tr>
<tr>
<td>Creator Process ID: 0x34c</td>
</tr>
<tr>
<td>Creator Process Name: C:\Users\malmoeb\AppData\Local\Temp\cckqcf.exe</td>
</tr>
<tr>
<td>Process Command Line:</td>
</tr>
</tbody>
</table>
curl -X POST https://threatfox-api.abuse.ch/api/v1/
-d '{ "query": "taginfo", "tag": "Netwire"}'

```json
{
    "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"
    ]
}
```