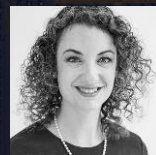




# Endpoint Detection super powers on the cheap



**Olaf Hartong**  
Blue Team Specialist Leader  
Deloitte



Chair  
**Emma Bickerstaffe**  
ISF

```
PS C:\> echo "Why am I here?"
```

---

- The Endpoint is an often used entry way into a network
- Endpoint Detection & Remediation (EDR) solutions are great, however often quite costly
- There is an alternative approach to the detection aspect, using an adversarial framework
- It allows you to leverage your existing data platform, in this case Splunk

PS C:\> type agenda

---

- MITRE ATT&CK
- What is Sysmon
- Sysmon configuration
- Sysmon deployment and maintenance at scale
- Threat Hunting app + Demo
- Lessons learned



# DISCLAIMER

This is not a magic bullet.  
It will require tuning and real investigative work to be  
truly effective in your environment

PS C:\> set MITRE ATT&CK

---

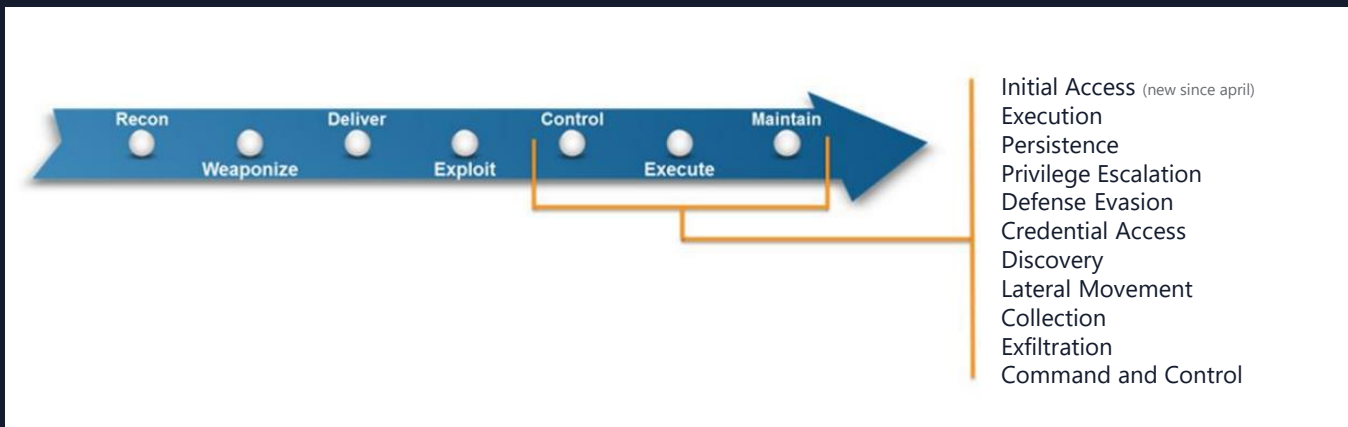
*" A framework for describing the behavior of cyber adversaries operating within enterprise networks. "*



- Comprehensive library of "what to look for"
- Threat model & framework
- Library of attacker activity (TTPs)

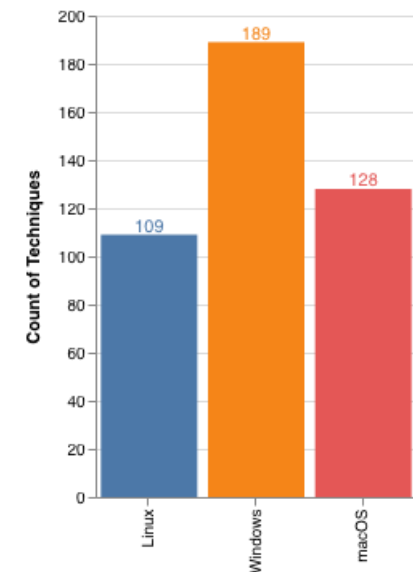
<https://attack.mitre.org>  
<https://mitre.github.io/attack-navigator/>  
[@MITREattack](#)

PS C:\> type Mitre ATT&CK



PS C:\ATT&CK> Is

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	lateral Movement	Collection	Exfiltration	Command And Control
10 Items	31 Items	56 Items	28 Items	59 Items	20 Items	19 Items	17 Items	13 Items	9 Items	21 Items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through
	Command-Line Interface	AppCert DLLs	AppCert DLLs	Brute Force	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Exploitation of Remote Services	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Authentication Package	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bootkit	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Medium	Data Encoding
Spearphishing via Service Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Data Obfuscation
Trusted Relationship	Graphical User Interface	Change Default File Association	Dylib Hijacking	Control Panel Items	Hooking	Peripheral Device Discovery	Remote Desktop Protocol	Email Collection	Exfiltration Over Physical Medium	Domain Fronting
Valid Accounts	InstallUtil	Component Firmware	Exploitation for Privilege Escalation	DCShadow	Kerberoasting	Permission Groups Discovery	Remote Services	Input Capture	Scheduled Transfer	Multi-Stage Channels
	Launchctl	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Keychain	Process Discovery	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	File System Permissions Weakness	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Query Registry	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	DLL Search Order Hijacking	Hooking	DLL Search Order Hijacking	Network Sniffing	Remote System Discovery	Taint Shared Content			Port Knocking
	Mshta	Dylib Hijacking	Image File Execution Options Injection	DLL Side-Loading	Password Filter DLL	Security Software Discovery	Third-party Software			Remote Access Tools
	PowerShell	External Remote Services	Launch Daemon	Extra Window Memory Injection	Private Keys	System Information Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	New Service	File Deletion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Path Interception	File System Logical Offsets	Security Memory	System Network Connections Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Plist Modification	Gatekeeper Bypass	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Port Monitors	Hidden Files and Directories		System Service Discovery				Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Process Injection	Hidden Users						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	Hidden Window						
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	HISTCONTROL						
	Source	Launch Daemon	Setuid and Setgid	Image File Execution Options Injection						
	Space after Filename	Launchctl	SID-History Injection	Indicator Blocking						
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Indicator Removal from Tools						
	Trap	Local Job Scheduling	Sudo	Indicator Removal on Host						
	Trusted Developer Utilities	Login Item	Sudo Caching	Indirect Command Execution						
	User Execution	Login Scripts	Valid Accounts	Install Root Certificate						
	Windows Management Instrumentation	LSASS Driver	Web Shell	InstallUtil						
	Windows Remote Management	Modify Existing Service		Launchctl						
		Netsh Helper DLL		LC_MAIN Hijacking						
		New Service		Maskerading						
		Office Application Startup		Modify Registry						
		Path Interception		Metta						
		Plist Modification		Network Share Connection Removal						
		Port Knocking		NTFS File Attributes						
		Port Monitors		Obfuscated Files or Information						
		Rc.common		Plist Modification						
		Re-opened Applications		Port Knocking						
		Redundant Access		Process Doppelganging						
		Registry Run Keys / Start Folder		Process Hollowing						
		Scheduled Task		Process Injection						
		Screensaver		Redundant Access						
		Security Support Provider		Regsvcs/Regasm						
		Service Registry Permissions Weakness		Rootkit						
		Shortcut Modification		Rundll32						
		SIP and Trust Provider Hijacking		Scripting						
		Startup Items		Signed Binary Proxy Execution						
		System Firmware		Signed Script Proxy Execution						
		Time Providers		SIP and Trust Provider Hijacking						
		Trap		Software Packing						
		Valid Accounts		Space after Filename						
		Web Shell		Timestamp						
		Windows Management Instrumentation Event Subscription		Trusted Developer Utilities						
		Winlogon Helper DLL		Valid Accounts						
				Web Service						



219 Techniques!

Covering:

- 187 Windows
- 108 Linux
- 130 MacOS

Thanks to all of our ATT&CKcon participants. [All sessions are here](#), and individual presentations will be posted soon.

## ENTERPRISE ▾

## TECHNIQUES

All

Initial Access +

Execution +

Persistence +

Privilege Escalation +

Defense Evasion +

Credential Access -

Account Manipulation

Bash History

Brute Force

Credential Dumping

Credentials in Files

Credentials in Registry

Exploitation for Credential Access

Forced Authentication

Hooking

Input Capture

Input Prompt

Kerberoasting

Keychain

LLMNR/NBT-NS Poisoning

Network Sniffing

Password Filter DLL

Private Keys

Securityd Memory

Two-Factor Authentication

[Home](#) > [Techniques](#) > [Enterprise](#) > [Credentials in Registry](#)

## Credentials in Registry

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information:<sup>[1]</sup>

- Local Machine Hive: `reg query HKLM /f password /t REG_SZ /s`
- Current User Hive: `reg query HKCU /f password /t REG_SZ /s`

## Examples

Name	Description
<a href="#">PowerSploit</a>	<a href="#">PowerSploit</a> has several modules that search the Windows Registry for stored credentials: <code>Get-UnattendedInstallFile</code> , <code>Get-Webconfig</code> , <code>Get-ApplicationHost</code> , <code>Get-SiteListPassword</code> , <code>Get-CachedGPPPassword</code> , and <code>Get-RegistryAutoLogon</code> . <sup>[1]</sup>
<a href="#">Reg</a>	<a href="#">Reg</a> may be used to find credentials in the Windows Registry. <sup>[1]</sup>

## Mitigation

Do not store credentials within the Registry. Proactively search for credentials within Registry keys and attempt to remediate the risk. If necessary software must store credentials, then ensure those accounts have limited permissions so they cannot be abused if obtained by an adversary.

## Detection

Monitor processes for applications that can be used to query the Registry, such as [Reg](#), and collect command parameters that may indicate credentials are being searched. Correlate activity with related suspicious behavior that may indicate an active intrusion to reduce false positives.

## References

- netbiosX. (2017, April 19). *Stored Credentials*. Retrieved April 6, 2018.

ID: T1214

**Tactic:** Credential Access**Platform:** Windows**Permissions Required:** User, Administrator**Data Sources:** Windows Registry, Process command-line parameters, Process Monitoring**Contributors:** Sudhanshu Chauhan, @Sudhanshu\_C**Version:** 1.0



# PS C:\ type T1214

## Credentials in Registry

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

ID: T1214

Tactic: Credential Access

Platform: Windows

Permissions Required: User, Administrator

Data Sources: Windows Registry, Process command-line parameters, Process Monitoring

Contributors: Sudhanshu Chauhan, @Sudhanshu\_C

Version: 1.0

Example commands to find Registry keys related to password information: <sup>[1]</sup>

Local Machine Hive: `reg query HKLM /f password /t REG_SZ /s`

Current User Hive: `reg query HKCU /f password /t REG_SZ /s`

## Detection

Monitor processes for applications that can be used to query the Registry, such as [Reg](#), and collect command parameters that may indicate credentials are being searched. Correlate activity with related suspicious behavior that may indicate an active intrusion to reduce false positives.

Sysmon



```
PS C:\> sc query "Sysmon"
```

---

- Sysmon is a free, powerful host-level tracing tool, developed by a small team of Microsoft employees
- Initially developed for internal use at Microsoft
- Sysmon is using a device driver and a service that is running in the background and loads very early in the boot process.

PS C:\> .\Sysmon.exe -?

---

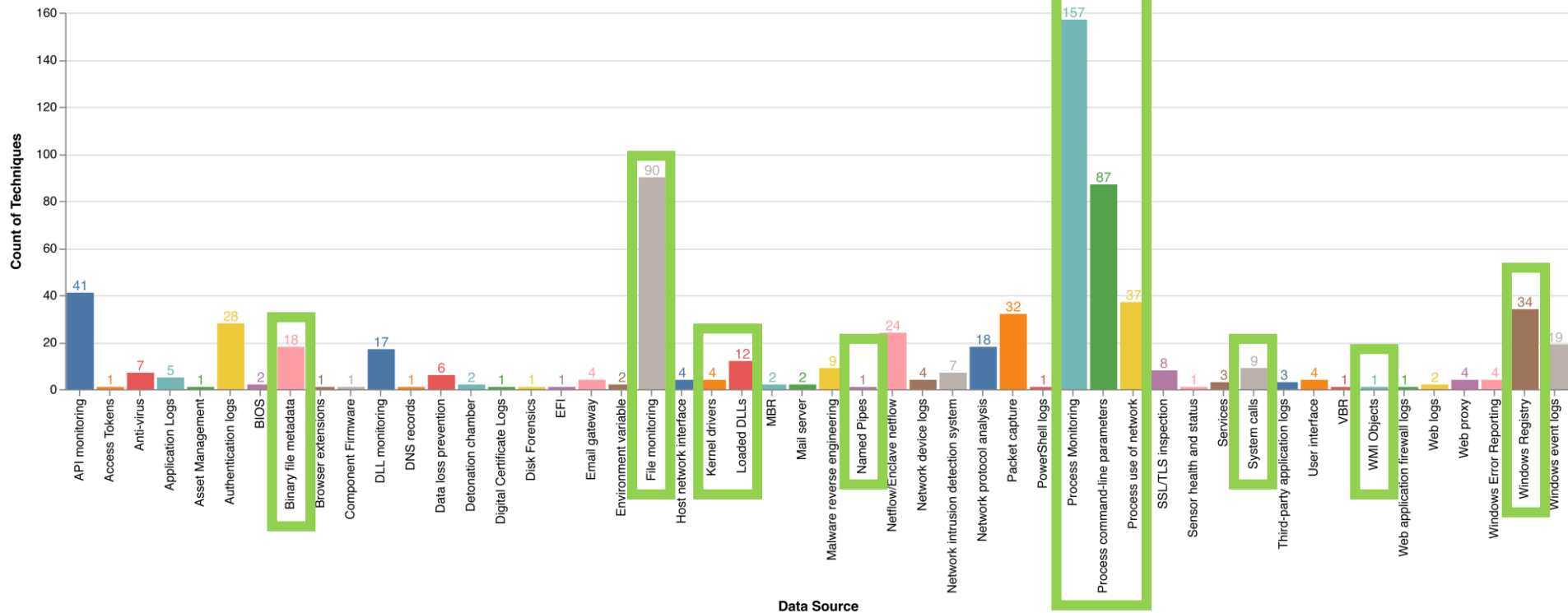
- Process creation (with full command line and hashes)
- Process termination
- Network connections
- File creation timestamp changes
- Driver/image loading
- Create remote threads
- Raw disk access
- Process memory access
- Registry access
- Named pipes
- WMI

PS C:\> echo "Why use Sysmon ?"

MITRE defines the following data sources:

Anti-virus	File monitoring	PowerShell logs	VBR
API monitoring	Host network interface	Process command-line parameters	Windows Error Reporting
Authentication logs	Kernel drivers	Process monitoring	Windows event logs
Binary file metadata	Loaded DLLs	Process use of network	Windows Registry
BIOS	Malware reverse engineering	Sensor health and status	WMI Objects
Data loss prevention	MBR	Services	
Digital Certificate Logs	Netflow/Enclave netflow	SSL/TLS inspection	
DLL monitoring	Network device logs	System calls	
EFI	Network protocol analysis	Third-party application logs	
Environment variable	Packet capture	User interface	

PS C:\> echo "Why use Sysmon ?"



# PS C:\> echo "Shout-out"

SwiftOnSecurity / sysmon-config

Watch 203 Star 1,158 Fork 282

Code Issues 12 Pull requests 9 Projects 0 Insights

Sysmon configuration file template with default high-quality event tracing

sysmon threatintel threat-hunting sysinternals windows netsec monitoring logging

114 commits 1 branch 0 releases 8 contributors

Branch: master New pull request Find file Clone or download

SwiftOnSecurity 64: New monitoring Latest commit #24dc22 on Jan 31

.gitignore	Edit .gitignore	3 months ago
README.md	Update README.md	a year ago
sysmonconfig-export.xml	64: New monitoring	3 months ago

README.md

## sysmon-config | A Sysmon configuration file for everybody to fork

This is a Microsoft Sysinternals Sysmon configuration file template with default high-quality event tracing.

The file provided should function as a great starting point for system change monitoring in a self-contained package. This configuration and results should give you a good idea of what's possible for Sysmon. Note that this does not track things like authentication and other Windows events that are also vital for incident investigation.

<https://github.com/SwiftOnSecurity/sysmon-config>  
[@SwiftOnSecurity](#)

Cyb3rWard0g / ThreatHunter-Playbook

Watch 167 Star 841 Fork 190

Code Issues 2 Pull requests 0 Projects 0 Insights

A Threat hunter's playbook to aid the development of techniques and hypothesis for hunting campaigns.

threat-hunting sysmon hunting-campaigns hypothesis hunting dfir hunter mitre-attack-db mitre

156 commits 2 branches 0 releases 6 contributors MIT

Branch: master New pull request Find file Clone or download

Cyb3rWard0g Update T1117\_regsvr32.xml Latest commit 04f9eb4 on Feb 6

adversary_attribution	Updated Reference Syntax in Description Columns & added IDs	6 months ago
attack_matrix	Update T1117_regsvr32.xml	3 months ago
metrics	Added Data Quality Dimensions to Hunt Scoring	4 months ago
resources	Added Data Quality Dimensions to Hunt Scoring	4 months ago
templates	Added Data Quality Dimensions to Hunt Scoring	4 months ago
.DS_Store	Added Atomic Sysmon Configs per technique	5 months ago
LICENSE	Initial commit	a year ago
README.md	Add new article from Sqrrl	6 months ago

README.md

## The ThreatHunter-Playbook

<https://github.com/Cyb3rWard0g/ThreatHunter-Playbook>  
[@Cyb3rWard0g](#)

PS C:\> type Sysmon-modular

---

- A Sysmon configuration repository, set up in a modular fashion for easier maintenance and generation of tailored configurations.
- Mapped to the MITRE ATT&CK framework
- Frequently updated based on threat reports or new attacker techniques



PS C:\Sysmon-modular\> ls

All available event types

Config template

Complete generated config

olafhartong / sysmon-modular

Watch 53 Star 295 Fork 37

Code Issues 0 Pull requests 0 Projects 0 Insights

A repository of sysmon configuration modules

sysmon dfir threat-hunting mitre-attack modular security-tools

139 commits 1 branch 0 releases 1 contributor MIT

Branch: master New pull request Find file Clone or download

olafhartong generated 08212018 Latest commit 69add8a 6 days ago

10_process_access	MITRE ATT&CK annotation added	14 days ago
11_file_create	Added WMI technique	12 days ago
12_13_14_registry_event	Added SHIM persistence location	12 days ago
15_file_create_stream_hash	Added debug.bin file creation for SafetyKatz	13 days ago
17_18_pipe_event	fixed formatting	10 days ago
19_20_21_wmi_event	MITRE ATT&CK annotation added	14 days ago
1_process_creation	added several ParentImages	6 days ago
2_file_create_time	MITRE ATT&CK annotation added	14 days ago
3_network_connection_initiated	Added common masquerading locations	13 days ago
5_process_ended	schemaversion to 4.1	14 days ago
6_driver_loaded_into_kernel	schemaversion to 4.1	14 days ago
7_image_load	Added dll	13 days ago
8_create_remote_thread	added common injected processes	13 days ago
9_raw_access_read	schemaversion to 4.1	14 days ago
attack_matrix	updated mapping	12 days ago
.gitignore	revocation check added	5 months ago
README.md	added PSSysmonTools repo	10 days ago
baseconfig.xml	schemaversion to 4.1	14 days ago
license.md	Create license.md	4 months ago
sysmonconfig.xml	generated 08212018	6 days ago

The diagram consists of a dark blue background with a light blue stepped border on the right side. Two horizontal light blue lines are positioned in the upper and lower right areas. The text "Excluded processes" is centered between these two lines. The text "Included processes" is centered below the lower line.

Excluded processes

Included processes

olafhartong / sysmon-modular

Watch

53

★ Star

295

🔗 Fork

37

Code

Issues 0

Pull requests 0

Projects 0

Insights

Branch: master

sysmon-modular / 1\_process\_creation /

Create new file

Find file

History

olafhartong added several ParentImages

Latest commit a6ee27 6 days ago

..

exclude\_adobe\_acrobat.xml

schemaversion to 4.1

14 days ago

exclude\_adobe\_creative\_cloud.xml

schemaversion to 4.1

14 days ago

exclude\_adobe\_flash.xml

schemaversion to 4.1

14 days ago

exclude\_adobe\_supporting\_processes.xml

schemaversion to 4.1

14 days ago

exclude\_cisco\_anyconnect.xml

schemaversion to 4.1

14 days ago

exclude\_dotnet-3-or-4.xml

schemaversion to 4.1

14 days ago

exclude\_drivers.xml

schemaversion to 4.1

14 days ago

exclude\_dropbox.xml

schemaversion to 4.1

14 days ago

exclude\_google\_chrome.xml

schemaversion to 4.1

14 days ago

exclude\_microsoft\_office\_click2run.xml

schemaversion to 4.1

14 days ago

exclude\_microsoft\_office\_services.xml

schemaversion to 4.1

14 days ago

exclude\_mozilla\_firefox.xml

schemaversion to 4.1

14 days ago

exclude\_splunk.xml

schemaversion to 4.1

14 days ago

exclude\_splunk\_universal\_forwarder.xml

schemaversion to 4.1

14 days ago

exclude\_svchost.xml

schemaversion to 4.1

14 days ago

exclude\_windows\_defender.xml

schemaversion to 4.1

14 days ago

exclude\_windows\_generic\_processes.xml

schemaversion to 4.1

14 days ago

include\_accessibility\_features.xml

MITRE names added

14 days ago

include\_appc\_shim.xml

MITRE ATT&CK annotation added

14 days ago

include\_bitsadmin.xml

MITRE ATT&CK annotation added

14 days ago

include\_bypass\_uac.xml

MITRE ATT&CK annotation added

14 days ago

include\_dosfuscation.xml

Added commandline obfuscation

13 days ago

include\_installutil.xml

MITRE ATT&CK annotation added

14 days ago

include\_living\_of\_the\_land.xml

added several ParentImages

6 days ago

include\_mavinject.xml

MITRE ATT&CK annotation added

14 days ago

include\_microsoft\_cmstp.xml

MITRE ATT&CK annotation added

14 days ago

include\_msbuild.xml

MITRE ATT&CK annotation added

14 days ago

include\_regsvcs\_regasm.xml

MITRE ATT&CK annotation added

14 days ago

include\_syncappvpublishingserver.xml

MITRE ATT&CK annotation added

14 days ago

include\_uncommon\_locations.xml

Added common masquerading locations

13 days ago

include\_windows\_control\_panel.xml

MITRE ATT&CK annotation added

14 days ago

include\_windows\_defender\_tampering.xml

Added windows defender tampering technique

13 days ago


include\_windows\_remote\_management.xml

MITRE ATT&CK annotation added

14 days ago

PS C:\..\..\creation> type exclude\_splunk\_universal\_forwarder.xml

Branch: master [sysmon-modular](#) / [1\\_process\\_creation](#) / [exclude\\_splunk\\_universal\\_forwarder.xml](#) Find file Copy path

 olafhartong schemaversion to 4.1 1f550aa 14 days ago


1 contributor

44 lines (43 sloc) 2.48 KB Raw Blame History

```
1 <Sysmon schemaversion="4.1">
2   <!-- Capture all hashes -->
3   <HashAlgorithms>*</HashAlgorithms>
4   <CheckRevocation/>
5   <EventFiltering>
6     <!-- Event ID 1 == Process Creation. -->
7     <ProcessCreate onmatch="exclude">
8       <!--SECTION: Splunk:UniversalForwarder-->
9       <Image condition="begin with">C:\Program Files\SplunkUniversalForwarder\bin\</Image> <!--Splunk:UniversalForwarder
10      <ParentImage condition="is">C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</ParentImage> <!--Splunk:Univ
11        <ParentImage condition="is">C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</ParentImage> <!--Splu
12      <Image condition="begin with">D:\Program Files\SplunkUniversalForwarder\bin\</Image> <!--Splunk:UniversalForwarder
13      <ParentImage condition="is">D:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</ParentImage> <!--Splunk:Univ
14        <ParentImage condition="is">D:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</ParentImage> <!--Splu
15      </ProcessCreate>
16    <!-- Event ID 2 == File Creation Time. -->
17    <FileCreateTime onmatch="include"/>
```

PS C:\..\..\creation> type include\_windows\_defender\_tampering.xml

Branch: master [sysmon-modular](#) / [1\\_process\\_creation](#) / [include\\_windows\\_defender\\_tampering.xml](#) Find file Copy path

 olafhartong Added windows defender tampering technique 9ec2400 13 days ago

1 contributor

41 lines (40 sloc) 2.46 KB Raw Blame History

```
1 <Sysmon schemaversion="4.1">
2   <!-- Capture all hashes -->
3   <HashAlgorithms*></HashAlgorithms>
4   <CheckRevocation/>
5   <EventFiltering>
6     <!-- Event ID 1 == Process Creation. -->
7     <ProcessCreate onmatch="include">
8       <Image name="technique_id=T1089,technique_name=Disabling Security Tools" condition="image">MpCmdRun.exe</Image><!-- Credit @viss h
9       <CommandLine name="technique_id=T1089,technique_name=Disabling Security Tools" condition="contains">Add-MpPreference</CommandLine
10      <CommandLine name="technique_id=T1089,technique_name=Disabling Security Tools" condition="contains">RemoveDefinitions</CommandLine
11      <CommandLine name="technique_id=T1089,technique_name=Disabling Security Tools" condition="contains">DisableIOAVProtection</Comman
12    </ProcessCreate>
13    <!-- Event ID 2 == File Creation Time. -->
14    <FileCreateTime onmatch="include"/>
15    <!-- Event ID 3 == Network Connection. -->
16    <NetworkConnect onmatch="include"/>
17    <!-- Event ID 5 == Process Terminated. -->
```


# PS C:\> tree

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 Items	25 Items	41 Items	21 Items	49 Items	16 Items	19 Items	15 Items	13 Items	9 Items	20 Items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessability Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	Appinit DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Appinit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Execution through API	Authentication Package	Application Shimming	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	
Execution through Module Load	Bootkit	Bypass User Account Control	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Encoding	
Exploitation for Client Execution	Browser Extensions	DLL Search Order Hijacking	Control Panel Items	Hooking	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Other Network Medium	Domain Fronting	
Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	DCShadow	Input Capture	Peripheral Device Discovery	Remote File Copy	Email Collection	Exfiltration Over Physical Medium	Fallback Channels	
Supply Chain Compromise	Component Firmware	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Kerberoasting	LLMNR/NBT-NS Poisoning	Replication Through Removable Media	Input Capture	Scheduled Transfer	Multi-hop Proxy	
Trusted Relationship	LSASS Driver	File System Permissions Weakness	Disabling Security Tools	Network Sniffing	Password Filter DLL	Process Discovery	Man in the Browser		Multi-Stage Channels	
Valid Accounts	Mshta	Hooking	DLL Search Order Hijacking	Private Keys	Replication Through Removable Media	Query Registry	Screen Capture		Multiband Communication	
	PowerShell	Image File Execution Options Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	Security Software Discovery	System Information Discovery	Video Capture		Multilayer Encryption	
	Regsvcs/Regasm	New Service	Extra Window Memory Injection	File Deletion	System Network Configuration Discovery	System Owner/User Discovery			Remote Access Tools	
	Regsvr32	Path Interception	File System Logical Offsets	Hidden Files and Directories	System Network Connections Discovery	System Service Discovery			Remote File Copy	
	Rundll32	Process Injection	Image File Execution Options Injection	Scheduled Task	System Time Discovery				Standard Application Layer Protocol	
	Scheduled Task	Scheduled Task	Indicator Blocking	Indicator Removal from Tools					Standard Cryptographic Protocol	
	Scripting	Service Registry Permissions Weakness	Indicator Removal on Host	Indirect Command Execution					Standard Non-Application Layer Protocol	
	Service Execution	SID-History Injection	Invalid Accounts	Install Root Certificate					Uncommonly Used Port	
	Signed Binary Proxy Execution	Valid Accounts	Web Shell	InstallUtil					Web Service	
	Signed Script Proxy Execution	Netsh Helper DLL		Masquerading						
	Third-party Software	Port Monitors		Modify Registry						
	Trusted Developer Utilities	Redundant Access		Mshta						
	User Execution	Registry Run Keys / Start Folder		Network Share Connection Removal						
	Windows Management Instrumentation	Scheduled Task		NTFS File Attributes						
	Windows Remote Management	Screensaver		Obfuscated Files or Information						
		Security Support Provider		Process Doppelgänger						
		Service Registry Permissions Weakness		Process Hollowing						
		Shortcut Modification		Process Injection						
		SIP and Trust Provider Hijacking		Redundant Access						
		System Firmware		Regsvcs/Regasm						
		Time Providers		Regsvr32						
		Valid Accounts		Rootkit						
		Web Shell		Rundll32						
		Windows Management Instrumentation Event Subscription		Scripting						
		Winlogon Helper DLL		Signed Binary Proxy Execution						
				Signed Script Proxy Execution						
				SIP and Trust Provider Hijacking						
				Software Packing						
				Timestamp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						

# Deployment and maintenance at scale



# PS C:\> echo "Deploy and ingest options"

	<b>Sysmon deploy and maintain app</b> <ul style="list-style-type: none"><li>• Install and/or upgrade Sysmon through my Splunk Deployment app</li></ul>	<b>SCCM or Group Policy Deployment</b> <ul style="list-style-type: none"><li>• Installation through a script pushed via SCCM or a GPO</li></ul>
	<b>Sysmon deploy and maintain app</b> <ul style="list-style-type: none"><li>• Push configuration updates via my app, updating is built in.</li></ul>	<b>Group Policy Deployment</b> <ul style="list-style-type: none"><li>• Push updates through a script pushed via a GPO</li></ul>
	<b>Splunk Universal Forwarder</b> <ul style="list-style-type: none"><li>• Shipping of Windows Event log, WMI and Sysmon logging is configured through 1 central configuration on the deployment server</li></ul>	<b>Windows Event Forwarding</b> <ul style="list-style-type: none"><li>• Subscribe to relevant logs through GPO</li><li>• Splunk Heavy Forwarder installed on the Windows Event Collector to ship to Splunk</li></ul>
	<b>Requirements</b> <ul style="list-style-type: none"><li>• Accessible Splunk Deployment Server</li><li>• Splunk Universal Forwarder installed on servers/endpoints</li></ul> <b>Pros</b> <ul style="list-style-type: none"><li>• Easy configuration</li><li>• Monitoring of system status</li><li>• No AD admin required, faster deployment</li></ul> <b>Cons</b> <ul style="list-style-type: none"><li>• Additional agent</li><li>• Splunk UF running as system (default)</li></ul>	<b>Requirements</b> <ul style="list-style-type: none"><li>• Active Directory</li><li>• Domain joined clients</li><li>• Windows Event Collector server</li></ul> <b>Pros</b> <ul style="list-style-type: none"><li>• No agent for log transport</li><li>• Thorough filtering options</li><li>• Windows native solution</li></ul> <b>Cons</b> <ul style="list-style-type: none"><li>• AD admin required for changes</li><li>• Harder configuration</li><li>• Dependence on 1 system</li></ul>

## PS C:\> Get-DiskUsage -Splunk -WeeklyAverage

Average Data Size per Host and Source			
Source ↕	Avg Host Count ↕	Avg Source Volume (MB) ↕	Avg Host Source Volume (MB) ↕
WinEventLog:Security	241.40	9991.287	41.389
WinEventLog:Microsoft-Windows-Sysmon/Operational	235.40	6142.608	26.094
WinEventLog:Application	6.00	2.200	0.367
C:\\Windows\\sysmon.log	243.20	0.021	0.000



# Threat Hunting utilizing this data



```
PS C:\> set "Threat Hunting App"
```

---

## Goal

- Create a investigative workflow approach for Threat Hunters
- Work with ML (Mandatory Learning) to get to know your environment
- There are no false positives
- Supply the user with tools to contextualize and investigate these events
- Use MITRE ATT&CK as a foundation

## Threat Hunting trigger overview

Edit

Export ▾

...

Trendline range

Last 7 days ▾

[Hide Filters](#)

Persistence

3 ↗  
-1

Privilege Escalation

No results found.

Defense Evasion

5 ↗  
3

Credential Access

9 ↗  
-1

Discovery

8 ↗  
-3

Lateral Movement

1 ↗  
1

Execution

11 ↗  
-20

Collection

No results found.

Exfiltration

No results found.

Command &amp; Control

4 ↗  
4

Top triggered techniques in the last 24h

mitre_technique_id ▾	mitre_technique ▾	mitre_category ▾	count ▾
T1059	Command-Line Interface	Execution	24
T1003	Credential Dumping	Credential_Access	17
T1047	Windows_Management_Instrumentation	Lateral_Movement	14
T1047	Windows Management Instrumentation	Execution	11
T1060	Registry Run Keys or Start Folder	Persistence	7
T1069	Permission Groups Discovery	Discovery	5
T1087	Account Discovery	Discovery	5
T1033	System Owner/User Discovery	Discovery	4
T1043	Commonly Used Port	Command_and_Control	4
T1049	System Network Connections Discovery	Discovery	4

&lt; prev 1 2 next &gt;

Top triggered host\_fqdns in the last 24h

host_fqdn ▾	count ▾
win10.windomain.local	81
dc.windomain.local	1

# Real Customer Example

Threat Hunting trigger overview

Drilldowns ▾

Hunting Indicators ▾

About this app

Search



ThreatHunting

## Threat Hunting trigger overview

Edit

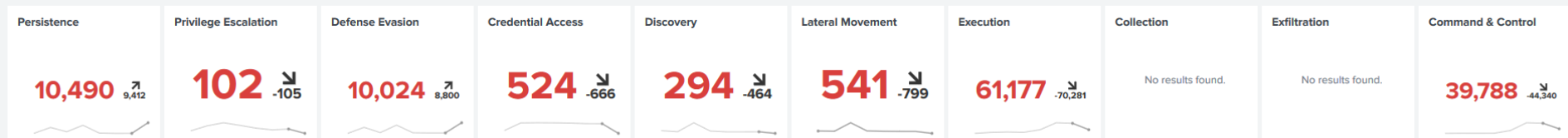
Export ▾

...

Trendline range

Last 7 days ▾

Hide Filters



Top triggered techniques in the last 24h

mitre_technique_id ▾	mitre_technique ▾	mitre_category ▾	count ▾
T1059	Command-Line Interface	Execution	129642
T1043	Commonly Used Port	Command_and_Control	85048
T1122	Component Object Model Hijacking	Persistence,Defense_Evasion	10450
T1086	PowerShell	Execution	2073
T1003	Credential Dumping	Credential_Access	1213
T1075	Pass the Hash	Lateral_Movement	1213
T1057	Process Discovery	Execution	735
T1042	Change Default File Association	Persistence	502
T1063	Security Software Discovery	Discovery	348
T1112	Modify Registry	Defense_Evasion	345

« prev 1 2 3 next »

Top triggered Computers in the last 24h

Computer ▾	count ▾
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	182270
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	26128
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	4797
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	4789
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	3517
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	1597
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	1511
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	1032
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	446
XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX	445

« prev 1 2 3 4 5 6 7 8 9 10 next »

Note; Initial deployment, un-whitelisted. After a few days these numbers are down to manageable

```
PS C:\> echo "Lessons Learned"
```

---

## DO

Plan your app, no really

Design the user workflows

Think ahead of future capabilities and design accordingly

Strive towards uniformity as much as possible

Test regularly, preferably with simulated as well as real world data

Create use cases from the scenarios that generate low noise events. This will enable you to respond quicker or even automatically

## DID

Rebuilt the app 4 times due to new insights

Created whitelisting capabilities 3 times, it is now generic and user friendly

Adopted a data model to the 4<sup>th</sup> rebuild to facilitate universal dashboards

Test runs at customers and various labs provided valuable details

Invented a form of Agile ;)

Note: I'm not a developer

# Roadmap



Optimizations to the app  
Add drilldown dashboards, additional  
contextual enrichment (workflows)



Windows, Powershell transcript and WMI logging  
Threat hunting triggers on these logs



Linux coverage  
OSQuery configuration and build Threat  
hunting triggers on these logs



Other sources  
Bro, Firewalls, Anti Virus, EDR and other sources

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

# PS C:\ echo thank you && exit

---

## My contact details

[@olafhartong](#)

[ohartong@deloitte.nl](mailto:ohartong@deloitte.nl)

## My GitHub repositories

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

<https://github.com/olafhartong/TA-Sysmon-deploy>

<https://github.com/olafhartong/SA-Threat-Hunting>



## Link summary

<https://attack.mitre.org>  
<https://mitre.github.io/attack-navigator/>  
<https://github.com/SwiftOnSecurity/sysmon-config>  
<https://github.com/Cyb3rWard0g/ThreatHunter-Playbook>  
<https://github.com/MHaggis/sysmon-dfir>  
<https://github.com/endgameinc/rta>  
<https://github.com/redcanaryco/atomic-red-team>  
<https://github.com/Neo23x0/APTSimulator>  
<https://github.com/mitre/caldera>  
<https://github.com/uber-common/metta>

## Twitter mentions

[@MITREattack](#)  
[@SwiftOnSecurity](#)  
[@Cyb3rWard0g](#)  
[@Mhaag](#)  
[@subTee](#)  
[@cyb3rops](#)  
[@\\_devonkerr](#)  
[@carnal0wnage](#)  
[@DavidJBianco](#)



# QUESTIONS?







# Thank you

Olaf Hartong, Blue Team Specialist Leader, Deloitte  
[ohartong@deloitte.nl](mailto:ohartong@deloitte.nl)  
[@olafhartong](https://twitter.com/olafhartong)



# LAS VEGAS 2018

ISF 29<sup>TH</sup> ANNUAL WORLD CONGRESS