



Endpoint Detection Superpowers with Sysmon + Splunk

Olaf Hartong
Specialist Leader Blue Team | Deloitte

Who am I?



Olaf Hartong

Blue Team Specialist Leader

Currently having fun @ Deloitte

13+ years in Info Security

Consulted at banks, educational institutions and governmental organizations

- Built and/or led Security Operations Centers
- Threat hunting, IR and Compromise assessments
- SOC Maturity transformations

Former documentary photographer

Father of 2 boys

 @olafhartong

 github.com/olafhartong

 ohartong@deloitte.nl

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Why am I here?

-  The Endpoint is a frequently 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

Agenda

- ▶ MITRE ATT&CK
- ▶ Sysmon
 - What is it
 - Why use it
 - Configuration, mapped to ATT&CK
- ▶ ThreatHunting application
 - The goal
 - My challenges
 - Demonstration



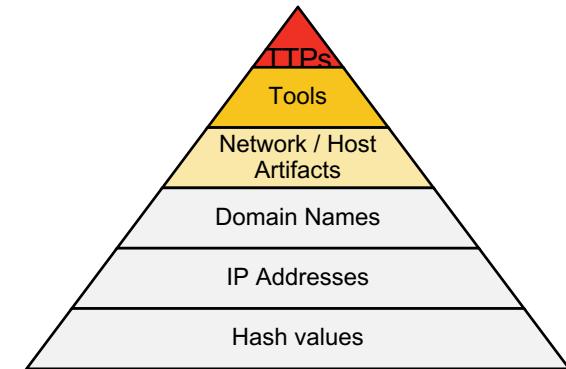
This is not a magic bullet.
It will require tuning and real
investigative work to be truly
effective in your environment

DISCLAIMER

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)



ATT&CK™
Adversarial Tactics, Techniques
& Common Knowledge

<https://attack.mitre.org>

<https://mitre.github.io/attack-navigator/>

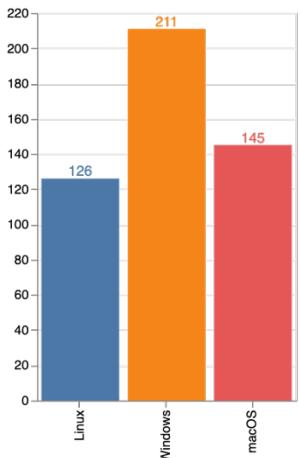
@MITREattack

ATT&CK's Structure

245 Techniques!

Covering:

- 211 Windows
- 126 Linux
- 145 MacOS



| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And Control | Exfiltration | Impact |
|-------------------------------------|-----------------------------------|------------------------------------|---|-------------------------------------|--|--|---|--|---|-------------------------------|----------|
| 11 items | 33 items | 68 items | 28 items | 67 items | 19 items | 22 items | 17 items | 13 items | 22 items | 9 items | 14 items |
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated | Data Destruction | |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Binary Padding | Bash History | Application Window Discovery | Application Deployment Software | Communication Through Removable Media | Data Compressed | Data Encrypted for Impact | | |
| External Remote Services | Command-Line Interface | Account Manipulation | Accessibility Features | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Connection Proxy | Data Encrypted | Data Transfer Size Limits | Defacement | |
| Hardware Additions | Compiled HTML File | AppCert DLLs | AppCert DLLs | Credential Dumping | Domain Trust Discovery | Data from Information Repositories | Custom Command and Control Protocol | Data Transfer Size Limits | Disk Content Wipe | Disk Structure Wipe | |
| Replication Through Removable Media | Dynamic Data Exchange | Application Shimming | Application Shimming | Credentials in Files | File and Directory Discovery | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol | Endpoint Denial of Service | Firmware Corruption | |
| Spearphishing Attachment | Execution through API | Authentication Package Control | Bypass User Account Control | Code Signing | Exploitation for Credential Access | Exploitation for Network Share Discovery | Exploitation of Remote Services | Exfiltration Over Shared Drive | Exfiltration Over Command and Control Channel | Inhibit System Recovery | |
| Spearphishing Link | Execution through Module Load | BITS Jobs | DLL Search Order Hijacking | Compiled HTML File | Forced Authentication | Network Sniffing | File from Removable Media | Data Encoding | Data Obfuscation | Network Denial of Service | |
| Spearphishing via Service | Exploitation for Client Execution | Browser Extensions | Dylib Hijacking | Component Firmware | Hacking | Peripheral Device Discovery | Domain Fronting | Domain Generation Algorithms | Exfiltration Over Other Network Medium | Transmitted Data Manipulation | |
| Supply Chain Compromise | Graphical User Interface | Change Default File Association | Exfiltration for Component Object Model | Input Capture | Permission Groups Discovery | Remote Desktop Protocol | Email Collection | Exfiltration Over Physical Medium | Exfiltration Over Multi-hop Proxy | Resource Hijacking | |
| Trusted Relationship | InstallUtil | Component Firmware Association | Privilege Escalation | Input Prompt | Process Discovery | Remote File Copy | Fallback Channels | Man in the Browser | Multi-Stage Channels | Runtime Data Manipulation | |
| Valid Accounts | Launchctl | Component Firmware Injection | Kerberoasting | Query Registry | Remote System Discovery | Replication Through Removable Media | Multi-band Communication | Screen Capture | Multi-hop Proxy | Service Stop | |
| | Local Job Scheduling | Component Object Model Hijacking | Keychain | Remote Services | Security Software Discovery | Shared Webroot | Multilayer Encryption | Video Capture | Multi-Stage Channels | Stored Data Manipulation | |
| | LSASS Driver | Create Account | Rebootfuscate/Decode Files or Information | Replication Through Removable Media | SSH Hijacking | SSH Hijacking | Port Knocking | | | Transmitted Data Manipulation | |
| | Mshta | DLL Search Order Hijacking | Weakness | Security Software Discovery | System Configuration Discovery | System Network Configuration Discovery | Remote Access Tools | | | | |
| | PowerShell | Hacking | Disabling Security Tools | System Information Discovery | System Network Configuration Discovery | System Network Connections Discovery | Remote File Copy | | | | |
| | Regsvcs/Regasm | Dylib Hijacking | Image File Execution Options Injection | DLL Search Order Hijacking | Password Filter DLL | Taint Shared Content | Standard Application Layer Protocol | | | | |
| | Regsvr32 | External Remote Services | Launch Daemon | DLL Side-Loading | Private Keys | Third-party Software Discovery | Standard Cryptographic Protocol | | | | |
| | Rundll32 | File System Permissions Weakness | New Service | Private Guards | Security Memory | Windows Admin Shares | Standard Non-Application Layer Protocol | | | | |
| | Scheduled Task | Hidden Files and Directories | Path Interception | Plist Modification | Two-Factor Authentication Interception | System Owner/User Discovery | Windows Remote Management | | | | |
| | Scripting | Service Execution | Port Monitors | Extra Window Memory Injection | System Service Discovery | System Time Discovery | | | | | |
| | | Hacking | File Deletion | | Virtualization/Sandbox Evasion | | | | | | |
| | | Signed Binary Proxy Execution | Process Injection | | | | | | | | |
| | | Signed Script Proxy Execution | Scheduled Task | | | | | | | | |
| | | Source | Service Registry Permissions Weakness | | | | | | | | |
| | | Space after Filename | Setuid and Setgid | | | | | | | | |
| | | Third-party Software | SID-History Injection | | | | | | | | |
| | | Trap | Startup Items | | | | | | | | |
| | | Trusted Developer Utilities | LC_LOAD_DYLIB Addition | | | | | | | | |
| | | User Execution | Local Job Scheduling | | | | | | | | |
| | | Windows Management Instrumentation | MSI Cache | | | | | | | | |
| | | Windows Remote Management | Logon Item | | | | | | | | |
| | | XSL Script Processing | Logon Scripts | | | | | | | | |
| | | | LSASS Driver | | | | | | | | |
| | | | Modify Existing Service | | | | | | | | |
| | | | Ntsh Helper DLL | | | | | | | | |
| | | | New Service | | | | | | | | |
| | | | Office Application Startup | | | | | | | | |
| | | | Path Interception | | | | | | | | |
| | | | Plist Modification | | | | | | | | |
| | | | Port Knocking | | | | | | | | |
| | | | Port Monitors | | | | | | | | |
| | | | Re.common | | | | | | | | |
| | | | Re-opened Applications | | | | | | | | |
| | | | Redundant Access | | | | | | | | |
| | | | Registry Run Keys / Startup Folder | | | | | | | | |
| | | | Scheduled Task | | | | | | | | |
| | | | Screensaver | | | | | | | | |
| | | | Security Support Provider | | | | | | | | |
| | | | Service Registry Permissions Weakness | | | | | | | | |
| | | | Setuid and Setgid | | | | | | | | |
| | | | Shortcut Modification | | | | | | | | |
| | | | SIP and Trust Provider Hijacking | | | | | | | | |
| | | | Startup Items | | | | | | | | |
| | | | System Firmware | | | | | | | | |
| | | | System Service | | | | | | | | |
| | | | Time Providers | | | | | | | | |
| | | | Trap | | | | | | | | |
| | | | Valid Accounts | | | | | | | | |
| | | | Web Shell | | | | | | | | |
| | | | Windows Management Instrumentation Event Subscription | | | | | | | | |
| | | | Winlogon Helper DLL | | | | | | | | |
| | | | XSL Script Processing | | | | | | | | |

Technique structure

[TITLE] Credential Dumping

[DESCRIPTION] Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

ID: T1003

Tactic: Credential Access

Platform: Windows, Linux, macOS

Permissions Required: Administrator, SYSTEM, root

Data Sources: API monitoring, Process monitoring, PowerShell logs, Process command-line parameters

CAPEC ID: CAPEC-567

Contributors: Vincent Le Toux, Ed Williams, Trustwave, SpiderLabs

Version: 1.0

Examples

| Name | Description |
|----------|---|
| APT28 | APT28 regularly deploys both publicly available and custom password retrieval tools on victims. ^{[18][19]} |
| Mimikatz | Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from the LSA, SAM table, credential vault, DCSync/NetSync, and DPAPI. ^{[52][15][53]} |

Mitigation

Detection

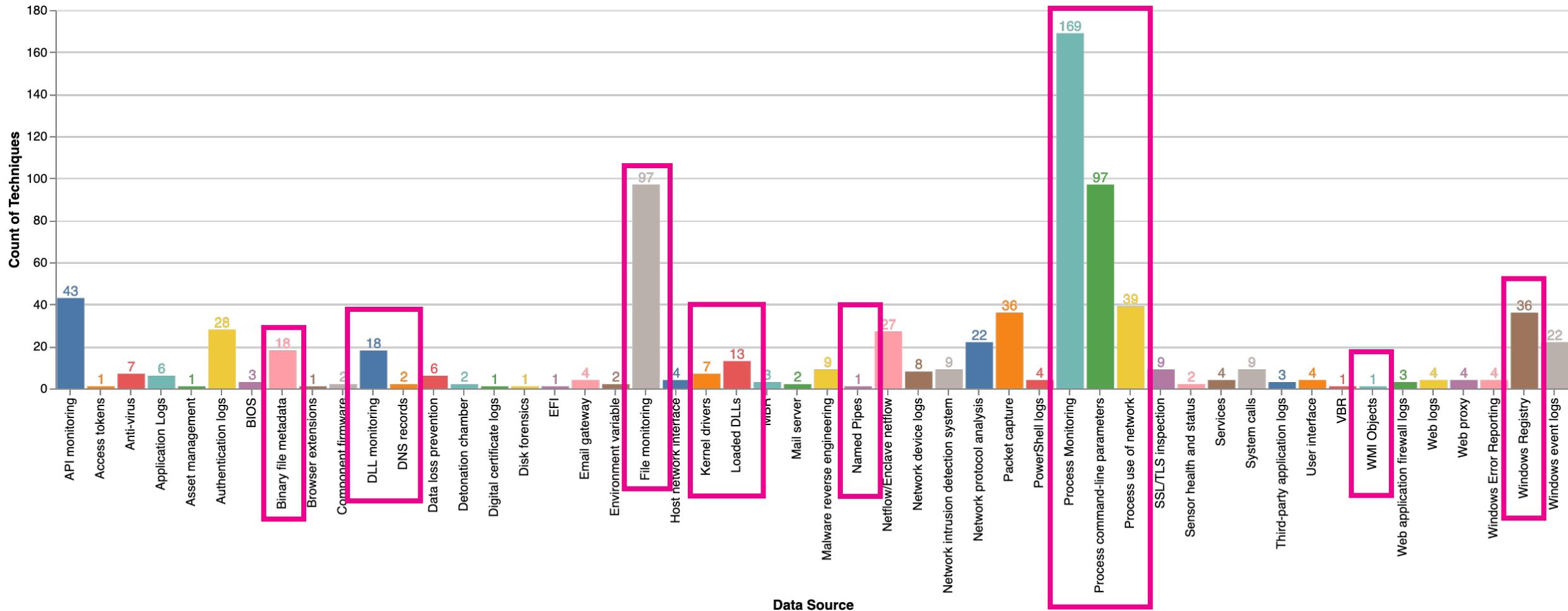
References

<https://attack.mitre.org>

splunk> .conf19

Data dispersion

The MITRE ATT&CK mentions per data source



What is Sysmon?

This is where the subtitle goes

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

<https://live.sysinternals.com>

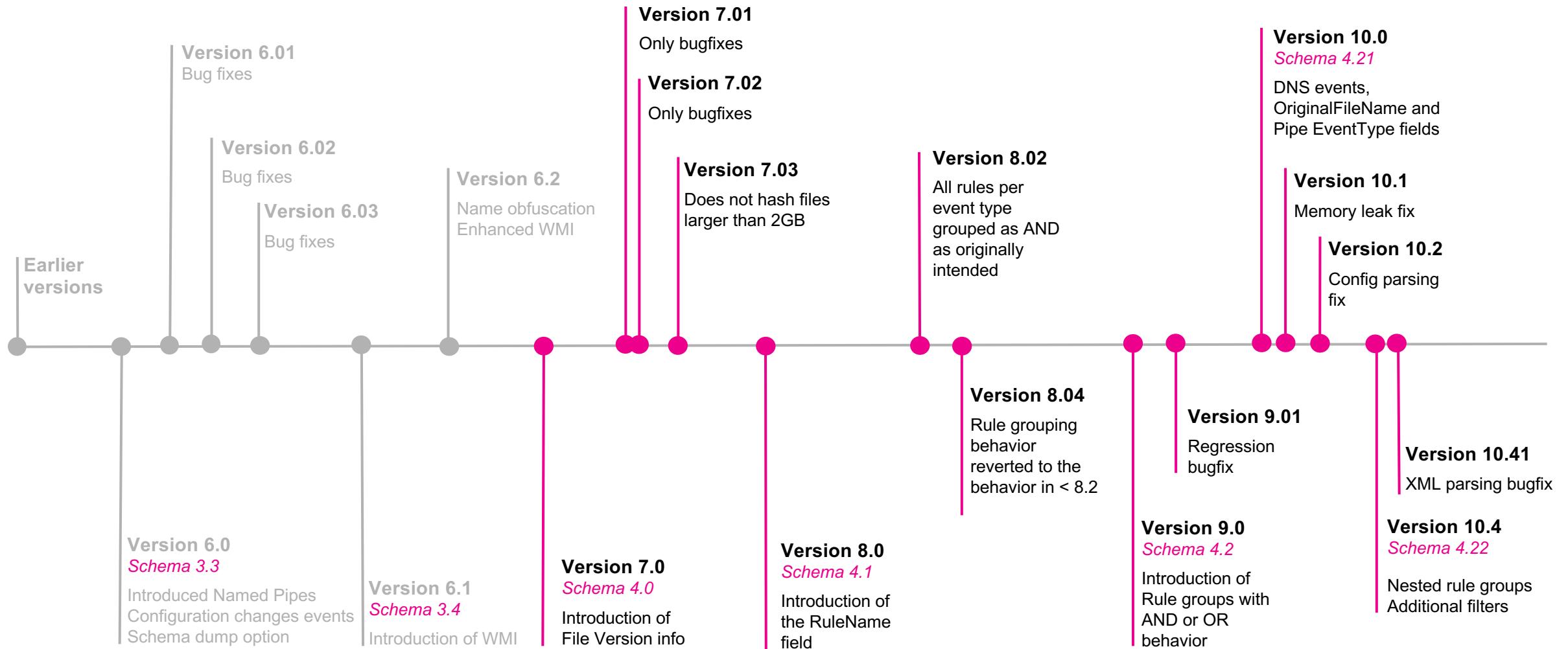
<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

What is Sysmon?

The event types it can write to the event log

- ▶ Process creation
- ▶ 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
- ▶ DNS

The evolution of Sysmon



Why use Sysmon ?

MITRE Data source perspective:

A little over **68%** of all techniques can (partially) be detected with process monitoring, **40%** with process command-line parameters

MITRE Threat group perspective:

Almost **65%** of known attacker groups prefer to use the command-line interface, standard application layer protocols and often start their attack with System information discovery

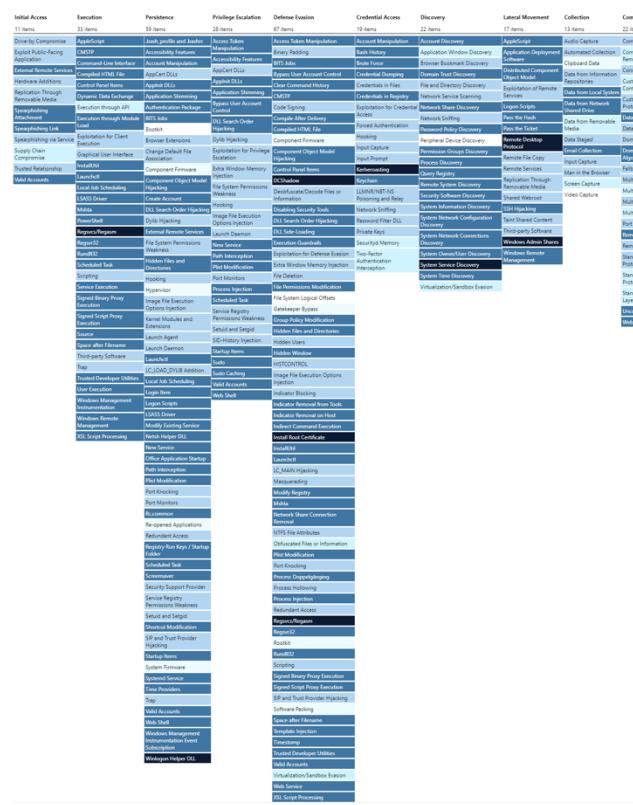
MITRE ATT&CK applicability

The likelihood of achieving full technique coverage per activity

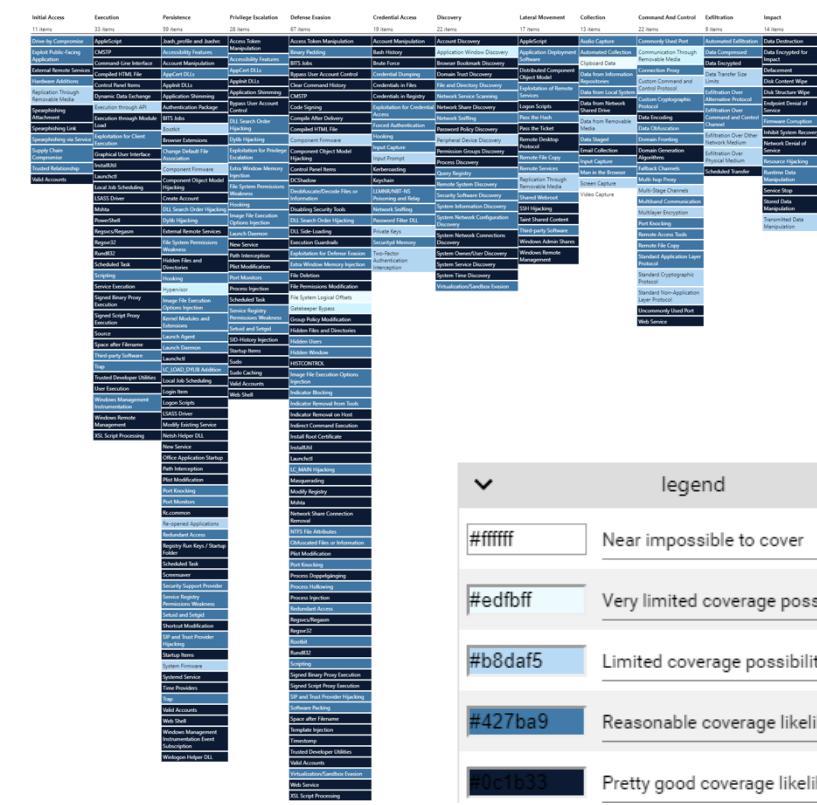
Alerting



Hunting



Forensics



legend

Near impossible to cover

Very limited coverage possible

Limited coverage possibility

• 11 • 11

Why use Sysmon ?

Event Properties - Event 1, Sysmon

General **Details**

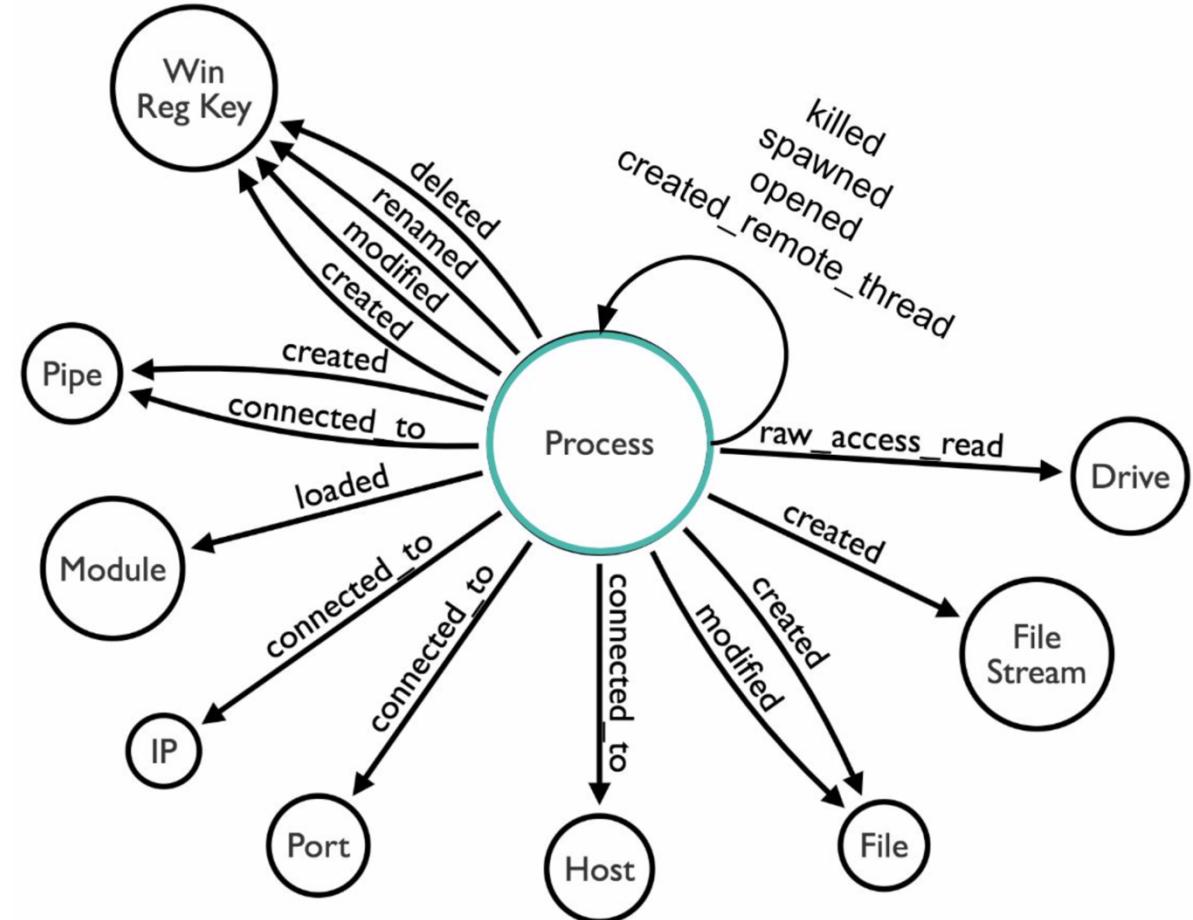
```

Process Create:
RuleName: technique_id=T1057,technique_name=Process Discovery
UtcTime: 2019-08-27 13:53:28.170
ProcessGuid: {4357c82a-35d8-5d65-0000-0010ae6acf00}
ProcessId: 9180
Image: C:\ProgramData\chocolatey\bin\pslist.exe
FileVersion: 1.4.0.0
Description: Process information lister - shim
Product: Sysinternals pslist
Company: Sysinternals - www.sysinternals.com
OriginalFileName: pslist.exe
CommandLine: "C:\ProgramData\chocolatey\bin\pslist.exe"
CurrentDirectory: C:\Users\homerus\
User: HOMERUS-10\homerus
LogonGuid: {4357c82a-3884-5d28-0000-0020e6350500}
LogonId: 0x535E6
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=6D86F4D3FFE0C27CE3ADFCB49D73D6C7BAD5502B,MD5=79B2D127664C84935D5AFA6C2E74CB5C,SHA256=790B4A0517EAB8C88A81EA1D61200AA9CB419F252E2CE13EDFA5B965748C6180,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
ParentProcessGuid: {4357c82a-3571-5d65-0000-00103da7c300}
ParentProcessId: 6820
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
More Information: Event Log Online Help

```

Copy Close



Sysmon

Some configuration examples

<https://github.com/SwiftOnSecurity/sysmon-config>

@SwiftOnSecurity

This screenshot shows the GitHub repository for SwiftOnSecurity/sysmon-config. It includes sections for Code, Issues (12), Pull requests (9), Projects (0), and Insights. The repository has 1,158 stars, 203 watches, and 282 forks. A note at the top states: "Sysmon configuration file template with default high-quality event tracing". Below this are tags: sysmon, threatintel, threat-hunting, sysinternals, windows, netsec, monitoring, logging. The repository has 114 commits, 1 branch, 0 releases, and 8 contributors. A .gitignore file was updated on Jan 31. The README.md file was last updated a year ago. A sysmonconfig-export.xml file was added on Jan 31. A section titled "sysmon-config | A Sysmon configuration file for everybody to fork" contains a note: "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." A link to the repository is provided at the bottom.

<https://github.com/Cyb3rWard0g/ThreatHunter-Playbook>

@Cyb3rWard0g

This screenshot shows the GitHub repository for Cyb3rWard0g/ThreatHunter-Playbook. It includes sections for Code, Issues (2), Pull requests (0), Projects (0), and Insights. The repository has 841 stars, 167 watches, and 190 forks. A note at the top states: "A Threat hunter's playbook to aid the development of techniques and hypothesis for hunting campaigns.". Below this are tags: threat-hunting, sysmon, hunting-campaigns, hypothesis, hunting, dfir, hunter, mitre-attack-db, mitre. The repository has 156 commits, 2 branches, 0 releases, and 6 contributors. A .gitignore file was updated on Feb 6. The README.md file was last updated a year ago. A section titled "README.md" contains a note: "This branch is 343 commits ahead, 47 commits behind SwiftOnSecurity:master." A link to the repository is provided at the bottom.

<https://github.com/ion-storm/sysmon-config>

@ionstorm

This screenshot shows the GitHub repository for ion-storm/sysmon-config. It includes sections for Code, Issues (0), Pull requests (0), Projects (0), and Insights. The repository was forked from SwiftOnSecurity/sysmon-config. It has 376 stars, 71 watches, and 453 forks. A note at the top states: "Advanced Sysmon configuration, Installer & Auto Updater with high-quality event tracing". Below this are tags: threat-analysis, mitre-attack. The repository has 410 commits, 4 branches, 0 releases, and 7 contributors. A .gitignore file was updated on Jan 25. The README.md file was last updated 2 months ago. A section titled "README.md" contains a note: "This branch is 343 commits ahead, 47 commits behind SwiftOnSecurity:master." A link to the repository is provided at the bottom.

Great work by many others, a few examples;
@Neo23x0, @c_APT_ure, @hexacorn, @darkoperator, @mattifestation, @Sbousseaden, @mhaag, @markrussinovich, @analyze_v

Introducing 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

 github.com/olafhartong/Sysmon-modular

Configuration Structure

All available event types

Merge script

Complete generated configuration

olafhartong / sysmon-modular

Code Issues 1 Pull requests 1 Projects 0 Wiki Security Insights Settings

A repository of sysmon configuration modules

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

229 commits 5 branches 0 releases 1 contributor MIT

Branch: v10.4 View #22 Create new file Upload files Find File Clone or download

This branch is 26 commits ahead of master. #22 Compare

olafhartong update to add Merge-AllSysmonXml Latest commit 7a22031 34 seconds ago

| Commit | Description | Time Ago |
|--------------------------------|--|----------------|
| 10_process_access | Airplane session, lots of additions | 3 days ago |
| 11_file_create | Airplane session, lots of additions | 3 days ago |
| 12_13_14_registry_event | added rule groups with OR | 10 days ago |
| 15_file_create_stream_hash | added rule groups with OR | 10 days ago |
| 17_18_pipe_event | Airplane session, lots of additions | 3 days ago |
| 19_20_21_wmi_event | added rule groups with OR | 10 days ago |
| 1_process_creation | typo fixes | 2 days ago |
| 22_dns_query | added dns events thanks to SwiftOnSecurity | 2 days ago |
| 2_file_create_time | added rule groups with OR | 10 days ago |
| 3_network_connection_initiated | additional lolbins | 9 days ago |
| 5_process_ended | added rule groups with OR | 10 days ago |
| 6_driver_loaded_into_kernel | added rule groups with OR | 10 days ago |
| 7_image_load | typo fixes | 2 days ago |
| 8_create_remote_thread | Airplane session, lots of additions | 3 days ago |
| 9_raw_access_read | added rule groups with OR | 10 days ago |
| attack_matrix | minor change | 5 months ago |
| .gitignore | revocation check added | last year |
| Merge-SysmonXml.ps1 | Add Merge-SysmonXml.ps1 | 2 days ago |
| README.md | update to add Merge-AllSysmonXml | 34 seconds ago |
| license.md | Create license.md | last year |
| sysmonconfig.xml | Generated 09062019 | 2 minutes ago |

Configuration Structure

For process creation events

Included processes

Excluded processes

This branch is 10 commits ahead of master.

olafhartong update to v10 features

Latest commit 8a321c6 5 hours ago

..

Excluded processes

- exclude_adobe_acrobat.xml
- exclude_adobe_creative_cloud.xml
- exclude_adobe_flash.xml
- exclude_adobe_supporting_processes.xml
- exclude_cisco_anycconnect.xml
- exclude_dotnet_3-or-4.xml
- exclude_drivers.xml
- exclude_dropbox.xml
- exclude_eset.xml
- exclude_google_chrome.xml
- exclude_ivanti_res.xml
- exclude_malwarebytes.xml
- exclude_microsoft_office_click2run.xml
- exclude_microsoft_office_services.xml
- exclude_mozilla_firefox.xml
- exclude_sophos.xml
- exclude_splunk.xml
- exclude_splunk_universal_forwarder.xml
- exclude_svhost.xml
- exclude_trend_micro.xml
- exclude_windows_defender.xml
- exclude_windows_generic_processes.xml
- include_accessibility_features.xml
- include_appe_shim.xml
- include_bitsadmin.xml
- include_bypass_uac.xml
- include_dosfuscation.xml
- include_ftmxml.xml
- include_installutil.xml
- include_living_of_the_land.xml
- include_mavinject.xml
- include_microsoft_crnsp.xml
- include_msbuild.xml
- include_regsvcs_regasxml.xml
- include_syncappvublishingserver.xml
- include_sysinternals.xml
- include_uncommon_locations.xml
- include_windows_control_panel.xml
- include_windows_defender_tampering.xml
- include_windows_remote_management.xml

Included processes

Configuration Example

Exclude Splunk

Branch: master ▾ sysmon-modular / 1_process_creation / exclude_splunk.xml Find file Copy path

olafhartong major overhaul, removing all template overhead c0c5333 on 16 Apr

1 contributor

10 lines (10 sloc) | 563 Bytes Raw Blame History

```
1 <Sysmon schemaversion="4.1">
2   <EventFiltering>
3     <ProcessCreate onmatch="exclude">
4       <Image condition="begin with">C:\Program Files\Splunk\bin\</Image> <!--Splunk child processes-->
5       <ParentImage condition="is">C:\Program Files\Splunk\bin\splunkd.exe</ParentImage> <!--Splunk:Daemon-->
6       <Image condition="begin with">D:\Program Files\Splunk\bin\</Image> <!--Splunk child processes-->
7       <ParentImage condition="is">D:\Program Files\Splunk\bin\splunkd.exe</ParentImage> <!--Splunk:Daemon-->
8     </ProcessCreate>
9   </EventFiltering>
10  </Sysmon>
```



olafhartong upgraded to v10 features

9b1db90 6 hours ago

1 contributor

33 lines (32 sloc) | 3.7 KB

[Raw](#) [Blame](#) [History](#)

```
1 <OriginalFileName<Sysmon schemaversion="4.22">
2   <EventFiltering>
3     <RuleGroup name="" groupRelation="or">
4       <ProcessCreate onmatch="include">
5         <!--Note: Not all Sysinternals listed here, only the ones I know/suspect to be used for malicious activity -->
6         <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PsList.exe</OriginalFileName>
7         <OriginalFileName name="technique_id=T1007,technique_name=System Service Discovery" condition="is">PsService.exe</OriginalFileName>
8         <OriginalFileName name="technique_id=T1035,technique_name=Service Execution" condition="is">PsExec.exe</OriginalFileName>
9         <OriginalFileName name="technique_id=T1035,technique_name=Service Execution" condition="is">PsExec.c</OriginalFileName>
10        <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">PsGetSID.exe</OriginalFileName>
11        <OriginalFileName name="technique_id=T1089,technique_name=Disabling Security Tools" condition="is">PsKill.exe</OriginalFileName>
12        <OriginalFileName name="technique_id=T1089,technique_name=Disabling Security Tools" condition="is">PKill.exe</OriginalFileName>
13        <OriginalFileName name="technique_id=T1003,technique_name=Credential Dumping" condition="contains">ProcDump</OriginalFileName>
14        <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">PsLoggedOn.exe</OriginalFileName>
15        <OriginalFileName name="technique_id=T1105,technique_name=Remote File Copy" condition="image">PsFile.exe</OriginalFileName>
16        <OriginalFileName name="technique_id=T1088,technique_name=Bypass User Account Control" condition="contains">ShellRunas</OriginalFileName>
17        <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PipeList.exe</OriginalFileName>
18        <OriginalFileName name="technique_id=T1083,technique_name=File and Directory Discovery" condition="is">AccessChk.exe</OriginalFileName>
19        <OriginalFileName name="technique_id=T1083,technique_name=File and Directory Discovery" condition="is">AccessEnum.exe</OriginalFileName>
20        <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">LogonSessions.exe</OriginalFileName>
21        <OriginalFileName name="technique_id=T1005,technique_name>Data from Local System" condition="is">PsLogList.exe</OriginalFileName>
22        <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PsInfo.exe</OriginalFileName>
23        <OriginalFileName name="technique_id=T1007,technique_name=System Service Discovery" condition="contains">LoadOrd</OriginalFileName>
24        <OriginalFileName name="technique_id=T1098,technique_name=Account Manipulation" condition="is">PsPasswd.exe</OriginalFileName>
25        <OriginalFileName name="technique_id=T1012,technique_name=Query Registry" condition="is">ru.exe</OriginalFileName>
26        <OriginalFileName name="technique_id=T1012,technique_name=Query Registry" condition="contains">Regsize</OriginalFileName>
27        <OriginalFileName name="technique_id=T1003,technique_name=Credential Dumping" condition="is">ProcDump</OriginalFileName>
28        <CommandLine name="technique_id=T1003,technique_name=Credential Dumping" condition="is">-ma lsass.exe</CommandLine>
29      </ProcessCreate>
30    </RuleGroup>
31  </EventFiltering>
32 </Sysmon>
```

Configuration Example

Include Sysinternals tools mapped to ATT&CK techniques

Latest features:

- OriginalFileName field
- DNS Events
- Additional filters;
contains any, contains all
- Nested rule grouping (yeah!)



```
<Sysmon schemaversion="4.22">
  <EventFiltering>
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="include">
        <Rule name="Eventviewer Bypass UAC" groupRelation="and">
          <ParentImage name="technique_id=T1088,technique_name=Bypass User Account Control" condition="image">eventvwr.exe</ParentImage>
          <Image condition="is not">c:\windows\system32\mmc.exe</Image>
        </Rule>
      </ProcessCreate>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```

ATT&CK coverage

Approximate, the configuration will also generate events for techniques otherwise tagged

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command And Control |
|-------------------------------------|------------------------------------|---|---|--|--|------------------------------|------------------------------------|------------------------------------|---|---|
| 10 items | 27 items | 42 items | 21 items | 53 items | 15 items | 20 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 | Account Manipulation | Accessibility Features | Binary Padding | Brute Force | Application Window Discovery | Distributed Component Object Model | Automated Collection | Data Compressed | Communication Through Removable Media |
| Hardware Additions | Compiled HTML File | AppCert DLLs | AppCert DLLs | BITs Jobs | Credential Dumping | Browser Bookmark Discovery | Clipboard Data | Data Encrypted | Data Transfer Size Limits | Connection Proxy |
| Replication Through Removable Media | Control Panel Items | Applnit DLLs | Applnit DLLs | Bypass User Account Control | Credentials in Files | Credentials in Registry | Exploitation of Remote Services | Data from Information Repositories | Data Transfer Over Alternative Protocol | Custom Command and Control Protocol |
| Spearphishing Attachment | Execution through API | Authentication Package | Bypass User Account Control | Code Signing | Exploitation for Credential Access | File and Directory Discovery | File from Local System | Data from Network Shared Drive | Data from Network Shared Drive | Custom Cryptographic Protocol |
| Spearphishing Link | Execution through Module Load | BITS Jobs | DLL Search Order Hijacking | Component Firmware | Forced Authentication | Network Share Discovery | Network Sniffing | Pass the Hash | Exfiltration Over Command and Control Channel | Exfiltration Over Other Network Medium |
| Spearphishing via Service | Exploitation for Client Execution | Browser Extensions | Exploitation for Privilege Escalation | Component Object Model Hijacking | Hooking | Network Sniffing | Pass the Ticket | Pass the Ticket | Data from Removable Media | Data Encoding |
| Supply Chain Compromise | Graphical User Interface | Change Default File Association | Extra Window Memory Injection | Input Capture | Peripheral Device Discovery | Passport Policy Discovery | Remote Desktop Protocol | Remote File Copy | Exfiltration Over Physical Medium | Domain Fronting |
| Trusted Relationship | InstallUtil | Component Firmware | DCShadow | Kerberoasting | Permission Groups Discovery | Remote Services | Remote Services | Data Staged | Fallback Channels | Scheduled Transfer |
| Valid Accounts | LSASS Driver | Component Object Model Hijacking | File System Permissions Weakness | LLMNR/NBT-NS Poisoning | Replication Through Removable Media | Windows Admin Shares | Windows Remote Management | Input Capture | Multi-hop Proxy | Multi-Stage Channels |
| | Mshta | Hooking | Deobfuscate/Decode Files or Information | Network Sniffing | Man in the Browser | | | | | Multiband Communication |
| | PowerShell | Create Account | Image File Execution Options Injection | Password Filter DLL | Shared Webroot | | | | | Multilayer Encryption |
| | Regsvcs/Regasm | DLL Search Order Hijacking | DLL Search Order Hijacking | Private Keys | System Information Discovery | | | | | Remote Access Tools |
| | Regsvr32 | External Remote Services | New Service | Two-Factor Authentication Interception | System Network Configuration Discovery | | | | | Remote File Copy |
| | Rundll32 | File System Permissions Weakness | DLL Side-Loading | System Network Connections Discovery | | | | | | Standard Application Layer Protocol |
| | Scheduled Task | Hidden Files and Directories | Path Interception | Exploitation for Defense Evasion | System Owner/User Discovery | | | | | Standard Cryptographic Protocol |
| | Scripting | Hooking | Port Monitors | Extra Window Memory Injection | System Service Discovery | | | | | Standard Non-Application Layer Protocol |
| | Service Execution | Hypervisor | Process Injection | File Deletion | System Time Discovery | | | | | Uncommonly Used Port |
| | Signed Binary Proxy Execution | Image File Execution Options Injection | Service Registry Permissions Weakness | File System Logical Offsets | | | | | | Web Service |
| | Signed Script Proxy Execution | Logon Scripts | SID-History Injection | Hidden Files and Directories | | | | | | |
| | Third-party Software | LSASS Driver | Valid Accounts | Image File Execution Options Injection | | | | | | |
| | Trusted Developer Utilities | Modify Existing Service | Web Shell | Indicator Blocking | | | | | | |
| | User Execution | Netsh Helper DLL | | Indicator Removal from Tools | | | | | | |
| | Windows Management Instrumentation | New Service | | Indicator Removal on Host | | | | | | |
| | Windows Remote Management | Office Application Startup | | Indirect Command Execution | | | | | | |
| | XSL Script Processing | Path Interception | | Install Root Certificate | | | | | | |
| | | Port Monitors | | InstallUtil | | | | | | |
| | | Redundant Access | | Masquerading | | | | | | |
| | | Registry Run Keys / Startup Folder | | Modify Registry | | | | | | |
| | | Scheduled Task | | Mshta | | | | | | |
| | | Screen saver | | Network Share Connection Removal | | | | | | |
| | | Security Support Provider | | NTFS File Attributes | | | | | | |
| | | Service Registry Permissions Weakness | | Obfuscated Files or Information | | | | | | |
| | | Shortcut Modification | | Process Doppelgänging | | | | | | |
| | | SIP and Trust Provider Hijacking | | Process Hollowing | | | | | | |
| | | System Firmware | | Process Injection | | | | | | |
| | | Time Providers | | Redundant Access | | | | | | |
| | | Valid Accounts | | Regsvcs/Regasm | | | | | | |
| | | Web Shell | | Regsvr32 | | | | | | |
| | | Windows Management Instrumentation Event Subscription | | Rootkit | | | | | | |
| | | Winlogon Helper DLL | | Rundll32 | | | | | | |
| | | | | Scripting | | | | | | |
| | | | | Signed Binary Proxy Execution | | | | | | |
| | | | | Signed Script Proxy Execution | | | | | | |
| | | | | SIP and Trust Provider Hijacking | | | | | | |
| | | | | Software Packing | | | | | | |
| | | | | Template Injection | | | | | | |
| | | | | Timestamp | | | | | | |
| | | | | Trusted Developer Utilities | | | | | | |
| | | | | Valid Accounts | | | | | | |
| | | | | Web Service | | | | | | |
| | | | | XSL Script Processing | | | | | | |

Data volume

Average per 7 days, on servers. Workstations will generate less

Average Data Size per Host and Source

| Source | Avg Host Count | Avg Source Volume (MB) | Avg Host Source Volume (MB) |
|--|----------------|------------------------|-----------------------------|
| WinEventLog:Security | 232.14 | 11682.962 | 50.327 |
| WinEventLog:Microsoft-Windows-Sysmon/Operational | 218.14 | 5528.664 | 25.345 |
| WinEventLog:Microsoft-Windows-WMI-Activity/Operational | 152.57 | 122.911 | 0.806 |
| WinEventLog:Microsoft-Windows-PowerShell/Operational | 38.29 | 21.885 | 0.572 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | 1.00 | 0.104 | 0.104 |
| WinEventLog:Application | 6.00 | 0.325 | 0.054 |
| C:\\Windows\\sysmon.log | 222.43 | 0.021 | 0.000 |

Introducing the ThreatHunting app

Goal

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



github.com/olafhartong/ThreatHunting



splunkbase.splunk.com/app/4305

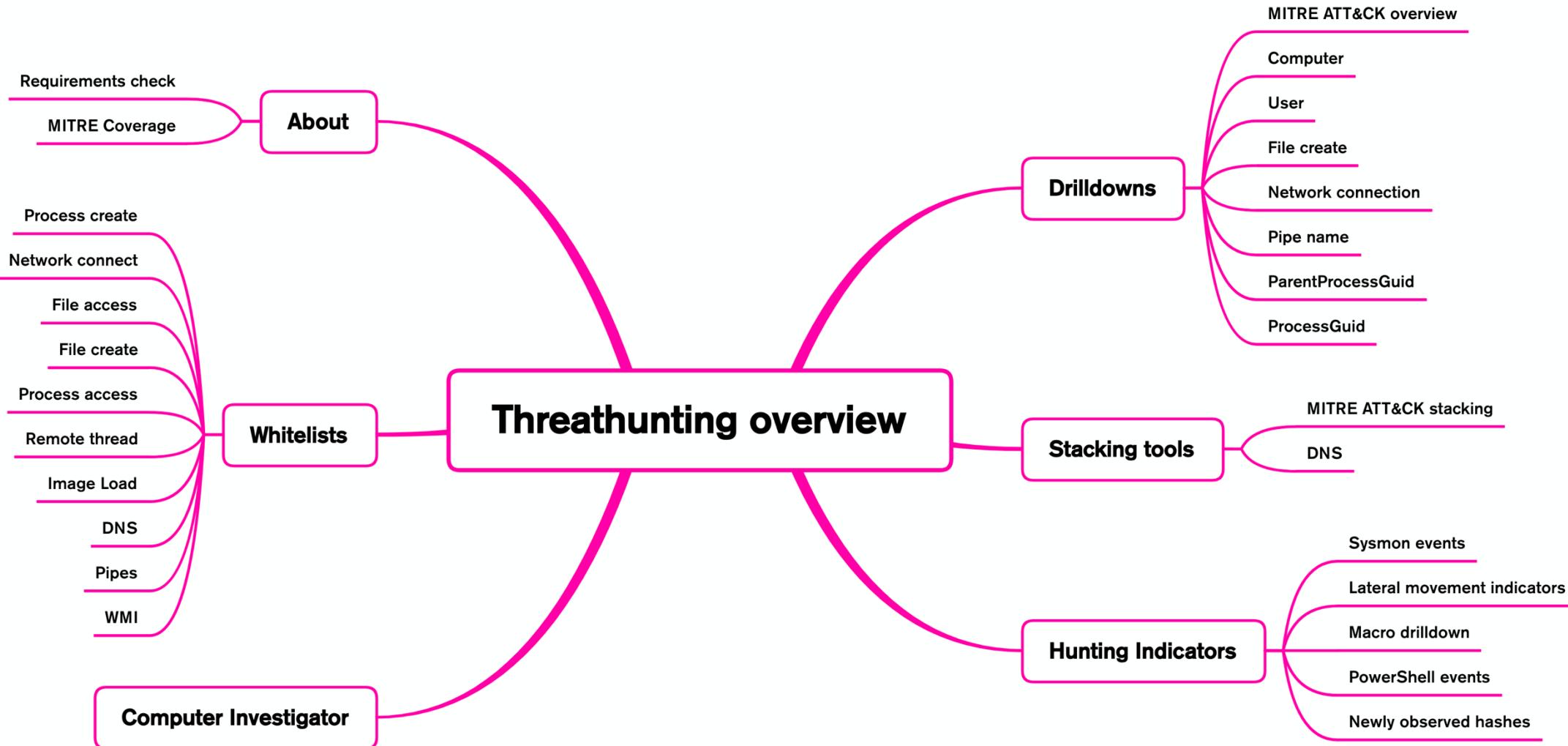
Introducing the ThreatHunting app

Challenges

- No data model I liked, created one based on OSSEM
- Inventing a whitelist capability on 150+ searches
- I'm not a great coder
- Rebuilt the app over 4 times to address hindsight, let's call this Agile
- Keeping the app performing swiftly
- Still some technical limitations



Introducing the ThreatHunting app



ATT&CK coverage

144 Reports!

and several live dashboards

Generating triggers for over 130 Techniques*

* triggers are not intended to cover the full technique

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And Control | Exfiltration | Impact |
|-------------------------------------|-----------------------------------|------------------------------------|---|---|--|--|------------------------------------|-------------------------------------|--|---|-------------------------------|
| 11 items | 27 items | 42 items | 21 items | 57 items | 16 items | 22 items | 15 items | 13 items | 21 items | 9 items | 14 items |
| Drive-by Compromise | CMSTP | Accessibility Features | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | Application Deployment Software | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| Exploit Public-Facing Application | Command-Line Interface | Account Manipulation | Accessibility Features | Binary Padding | Brute Force | Application Window Discovery | Distributed Component Object Model | Automated Collection | Communication Through Removable Media | Data Encrypted for Impact | Data Encrypted for Impact |
| External Remote Services | Compiled HTML File | AppCert DLLs | BITS Jobs | Credential Dumping | Browser Bookmark Discovery | Domain Trust Discovery | Data from Information Repositories | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| Hardware Additions | Control Panel Items | AppInit DLLs | Bypass User Account Control | Credentials in Files | File and Directory Discovery | File Exploitation | Data from Local System | Custom Command and Control Protocol | Data Transfer Size Limits | Disk Content Wipe | Disk Structure Wipe |
| Replication Through Removable Media | Dynamic Data Exchange | Application Shimming | CMSTP | Credentials in Registry | Network Service Scanning | Network Share Discovery | Logon Scripts | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol | Endpoint Denial of Service | Firmware Corruption |
| Spearphishing Attachment | Execution through API | Authentication Package | Code Signing | Exploitation for Credential Access | Forced Authentication | Network Sniffing | Pass the Hash | Data from Network Shared Drive | Data Encoding | Exfiltration Over Command and Control Channel | Inhibit System Recovery |
| Spearphishing Link | Execution through Module | BITS Jobs | Compile After Delivery | Hooking | Passport Policy Discovery | Pass the Ticket | Remote Desktop Protocol | Data from Removable Media | Data Obfuscation | Domain Fronting | Network Denial of Service |
| Spearphishing via Service | Load | Bootkit | DLL Search Order Hijacking | Component Firmware | Peripheral Device Discovery | Remote File Copy | Domain Staged | Domain Generation Algorithms | Exfiltration Over Other Network Medium | Exfiltration Over Physical Medium | Resource Hijacking |
| Supply Chain Compromise | Exploitation for Client Execution | Browser Extensions | Change Default File Association | Component Object Model Hijacking | Input Capture | Email Collection | Fallback Channels | Domain Generation Algorithms | Exfiltration Over Physical Medium | Exfiltration Over Physical Medium | Runtime Data Manipulation |
| Trusted Relationship | Graphical User Interface | InstallUtil | Extra Window Memory Injection | Kerberoasting | Input Prompt | Input Capture | Man in the Browser | Multi-hop Proxy | Multi-band Communication | Multi-stage Channels | Scheduled Transfer |
| Valid Accounts | LSASS Driver | Component Object Model Hijacking | DCShadow | LLMNR/NBT-NS Poisoning and Relay | Network Sniffing | Network System Discovery | Shared Webroot | Multi-layer Encryption | Multi-layer Encryption | Standard Application Layer Protocol | Service Stop |
| | PowerShell | Create Account | File System Permissions Weakness | Deobfuscate/Decode Files or Information | Network Sniffing | Security Software Discovery | Taint Shared Content | Windows Admin Shares | Windows Remote Management | Standard Cryptographic Protocol | Stored Data Manipulation |
| | Regsvcs/Regasm | DLL Search Order Hijacking | Hijacking | Disabling Security Tools | Network Sniffing | System Information Discovery | Third-party Software | Windows Admin Shares | Windows Remote Management | Standard Non-application Layer Protocol | Transmitted Data Manipulation |
| | Regsvr32 | External Remote Services | Image File Execution Options Injection | DLL Search Order Hijacking | Private Keys | System Network Configuration Discovery | | | | Uncommonly Used Port | Web Service |
| | Rundll32 | New Service | Path Interception | DLL Side-Loading | Two-Factor Authentication Interception | System Network Connections Discovery | | | | | |
| | Scheduled Task | File System Permissions Weakness | Port Monitors | Execution Guardrails | | System Owner/User Discovery | | | | | |
| | Scripting | Hidden Files and Directories | Process Injection | Exploitation for Defense Evasion | | System Service Discovery | | | | | |
| | Service Execution | Signed Binary Proxy Execution | Hooking | Extra Window Memory Injection | | System Time Discovery | | | | | |
| | | Signed Script Proxy Execution | Hypervisor | Scheduled Task | | Virtualization/Sandbox Evasion | | | | | |
| | | Third-party Software | Image File Execution Options Injection | File Deletion | | | | | | | |
| | | Trusted Developer Utilities | Logon Scripts | File Permissions Modification | | | | | | | |
| | | User Execution | LSASS Driver | File System Logical Offsets | | | | | | | |
| | | Windows Management Instrumentation | Modify Existing Service | Group Policy Modification | | | | | | | |
| | | Windows Remote Management | Netshell Helper DLL | Hidden Files and Directories | | | | | | | |
| | | XSL Script Processing | New Service | Image File Execution Options Injection | | | | | | | |
| | | | Office Application Startup | Indicator Blocking | | | | | | | |
| | | | Path Interception | Indicator Removal from Tools | | | | | | | |
| | | | Port Monitors | Indicator Removal on Host | | | | | | | |
| | | | Redundant Access | Indirect Command Execution | | | | | | | |
| | | | Registry Run Keys / Startup Folder | Install Root Certificate | | | | | | | |
| | | | Scheduled Task | InstallUtil | | | | | | | |
| | | | Screensaver | Masquerading | | | | | | | |
| | | | Security Support Provider | Modify Registry | | | | | | | |
| | | | Service Registry Permissions Weakness | Mshta | | | | | | | |
| | | | Shortcut Modification | Network Share Connection Removal | | | | | | | |
| | | | SIP and Trust Provider Hijacking | NTFS File Attributes | | | | | | | |
| | | | System Firmware | Obfuscated Files or Information | | | | | | | |
| | | | Time Providers | Process Doppelgänging | | | | | | | |
| | | | Valid Accounts | Process Hollowing | | | | | | | |
| | | | Web Shell | Process Injection | | | | | | | |
| | | | Windows Management Instrumentation Event Subscription | Redundant Access | | | | | | | |
| | | | Winlogon Helper DLL | Regsvcs/Regasm | | | | | | | |
| | | | | Regsvr32 | | | | | | | |
| | | | | Rootkit | | | | | | | |
| | | | | Rundll32 | | | | | | | |
| | | | | Scripting | | | | | | | |
| | | | | Signed Binary Proxy Execution | | | | | | | |
| | | | | Signed Script Proxy Execution | | | | | | | |
| | | | | SIP and Trust Provider Hijacking | | | | | | | |
| | | | | Software Packing | | | | | | | |
| | | | | Template Injection | | | | | | | |
| | | | | Timestamp | | | | | | | |
| | | | | Trusted Developer Utilities | | | | | | | |
| | | | | Valid Accounts | | | | | | | |
| | | | | Virtualization/Sandbox Evasion | | | | | | | |
| | | | | Web Service | | | | | | | |
| | | | | XSL Script Processing | | | | | | | |

DEMO

One of my oopsies

Threat Hunting trigger overview

Drilldowns ▾ Stacking Tools ▾ Hunting Indicators ▾ Computer Investigator Whitelist ▾ About this app Search

THREAT HUNTING 

Threat Hunting trigger overview

Time range Exclude Technique Exclude host Hide Filters

Last 7 days None X None X

Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection Exfiltration Command & Control

0 3,010,003 -6,716,523 807,835 -1,885,282 131,196 -589,442 3,016,733 -6,878,561 95,104 -436,131 876,844 -2,359,350 302,528 -257,915 95,104 -436,122 0 29 -3,971

Top triggered techniques in the selected timeframe

| mitre_technique_id | mitre_technique | mitre_category | count |
|--------------------|------------------------------------|----------------------------------|----------|
| T1047 | Windows Management Instrumentation | Execution | 10510290 |
| T1197 | BITS Jobs | Persistence,Defense_Evasion | 10258530 |
| T1170 | MSHTA | Defense_Evasion,Execution | 10216079 |
| T0000 | Remotely Query Login Sessions | Discovery | 10154993 |
| T1117 | Regsvr32 | Defense_Evasion,Execution | 9045099 |
| T1218 | Signed Binary Proxy Execution | Defense_Evasion,Execution | 8936177 |
| T1076 | Remote Desktop Protocol | Lateral_Movement | 4879063 |
| T1138 | Application Shimming | Persistence,Privilege_Escalation | 1181254 |
| T1191 | CMSTP | Defense_Evasion,Execution | 1179265 |
| T1115 | Clipboard Data | Collection | 1178035 |

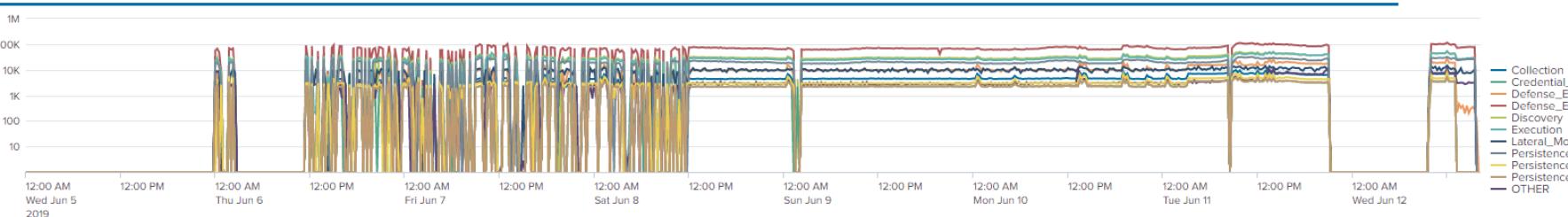
« Prev 1 2 3 4 5 6 Next »

Top triggered host_fqdns in the selected timeframe

| host_fqdn | count |
|---------------|----------|
| 192.168.1.100 | 15416637 |
| 192.168.1.101 | 13405503 |
| 192.168.1.102 | 11590275 |
| 192.168.1.103 | 10122483 |
| 192.168.1.104 | 8996219 |
| 192.168.1.105 | 3778348 |
| 192.168.1.106 | 3355315 |
| 192.168.1.107 | 3025412 |
| 192.168.1.108 | 2721990 |
| 192.168.1.109 | 1856635 |

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Activity by time per day

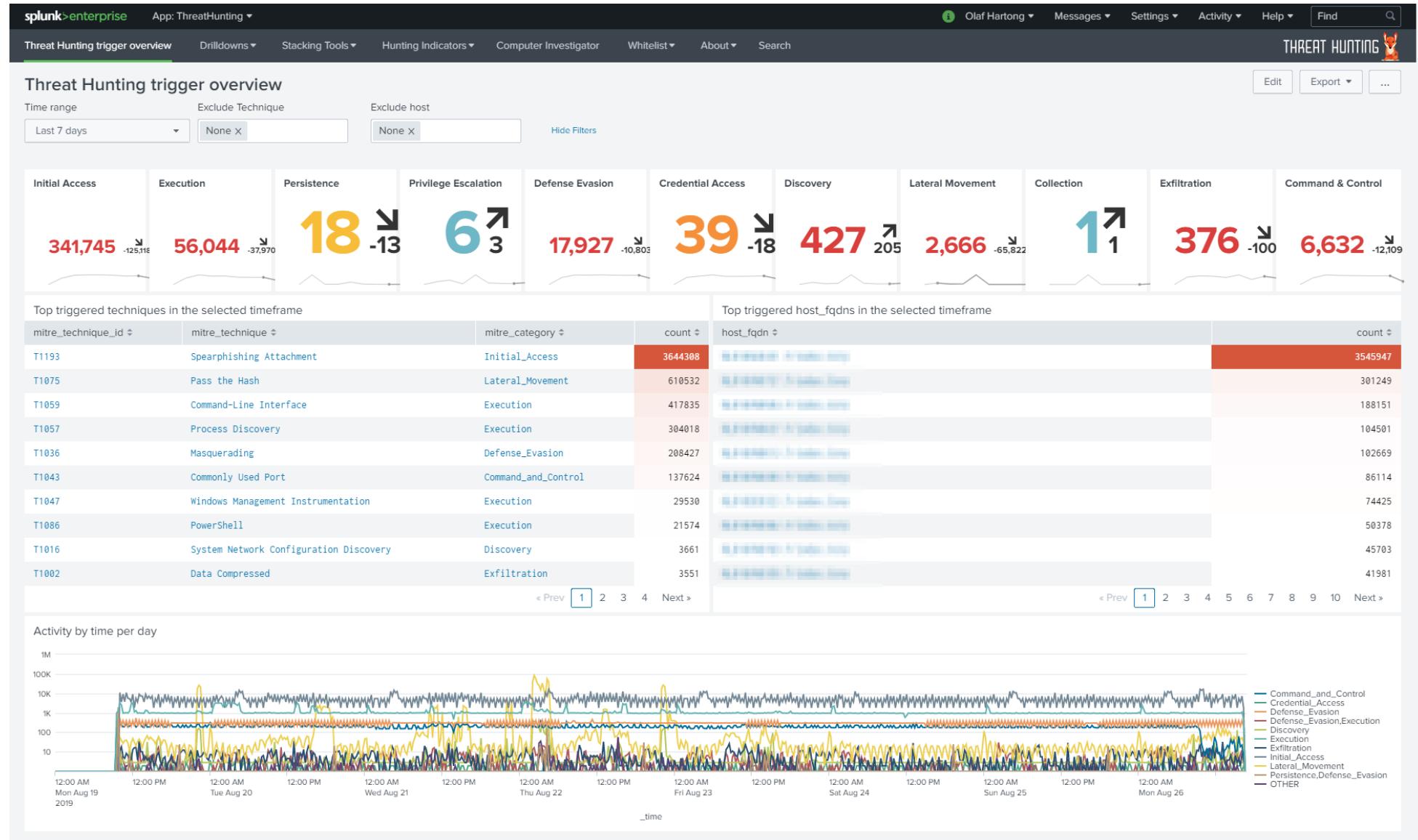


Legend:

- Collection
- Credential_Access,Discovery
- Defense_Evasion
- Defense_Evasion,Execution
- Discovery
- Execution
- Lateral_Movement
- Persistence,Defense_Evasion
- Persistence,Privilege_Escalation
- Persistence,Privilege_Escalation,Credential_Access
- OTHER

Real customer example

Initial deployment, un-whitelisted. After a few days these numbers are manageable



Try it yourself



DETECTIONLAB



github.com/clong/DetectionLab

A lab environment complete with security tooling and logging best practices, containing;

- Windows DC
- Windows WEF server
- Windows 10
- Logger machine, containing Splunk, Bro, Suricata, Kolide and much more

Roadmap

Things on my backlog



Optimizations to the app, add drilldown dashboards
 Additional contextual enrichment (workflows)
 Check new hashes daily against VT



Windows, PowerShell (transcript) and WMI logging
 Threat hunting triggers and dashboards on these logs



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



Other log sources and triggers for;
 Bro/Zeek , Firewalls, Antivirus, EDRs and more

Pull requests are welcome!

| 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 | | |

Available now!

Any questions ?

 github.com/olafhartong/threathunting

 splunkbase.splunk.com/app/4305

 github.com/olafhartong/Sysmon-modular

.conf19[®]

splunk[®]>

Thank
You!