

THM Challenge: Summit
Difficulty: Easy
Ron

Summit

Q1: What is the first flag you receive after successfully detecting sample1.exe?

Let's examine the info that has been sent to us.

General Info - sample1.exe

File Name	sample1.exe
File Size	202.50 KB
File Type	PE32+ executable (GUI) x86-64, for MS Windows
Analysis Date	September 5, 2023
OS	Windows 10x64 v1803
Tags	Trojan.Metasploit.A
MIME	application/x-dosexec
MDS	cbda8ae808aa0cbe7c8b982bae896c2a
SHA1	83d2791ca93e5868598485aa62597cbebbf7618
SHA256	9c558591a25c6228cb7d74d97bd133d75c961f7ed2ef7180144859cc09efca8c

Behaviour Analysis

MALICIOUS

METASPLOIT was detected
• sample1.exe (PID: 2492)

SUSPICIOUS

Connects to unusual port
• sample1.exe (PID: 2492)

INFO

Reads the machine GUID from the registry
• sample1.exe (PID: 2492)
The process checks LSA protection
• sample1.exe (PID: 2492)
Reads the computer name
• sample1.exe (PID: 2492)
Checks supported languages
• sample1.exe (PID: 2492)

Starting from the lowest level of the pyramid of pain, we can start from trying to block the SHA256 hash that belongs to the malicious file by navigating to "Manage Hashes".

The choice to block the SHA256 over other hash types in this task was made because it is harder for the attacker to tweak the same file with a different hash of this type and avoid the hash block.

Manage Hashes

Home / IOC Management / Manage Hashes

Q Detect Hashes

Manually add a hash to the blocklist

If you've discovered a hash value related to a malicious file or executable, you can submit it here. Submitted hashes will automatically update PicoSecure's EDR detection signatures and improve its ability to detect and block similar threats.

Hash Algorithm:

☐ MDS

☐ SHA1

☒ SHA256

Hash Value:

8cb7d74d97bd133d75c961f7ed2ef7180144859cc09efca8c

Submit Hash

Hash Blocklist

Nice work! You prevented sample1.exe from executing by detecting its unique hash value. Check your inbox for the next steps.

Algorithm	Value	Actions
SHA256	9c558591a25c6228cb7d74d97bd133d75c961f7ed2ef7180144859cc09efca8c	<input checked="" type="checkbox"/> <input type="checkbox"/>
MDS	c5a20611630c69f8f1ca53f000e17	<input checked="" type="checkbox"/> <input type="checkbox"/>
MDS	f0540bd025ebab9c05571000b2c5002	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA1	350930418162092027ab53c99001f00829d41d	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA256	ed347ad7305214db08974a0086746b78c03b1f6b73c8baf979e40f8e15580	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA256	b0657d328bbae59176613e794ae1bf99c7c2e52905876fdeb17b06448f	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA256	cd3c59eedabaa12e1e8508db0876b23597aaaf08f069c7616af96c2e90aa00f	<input checked="" type="checkbox"/> <input type="checkbox"/>

Great, it worked and we got our first flag!

Update: You Blocked Me!

📧 Sphinx <sphinx@pentesting.thm>

👤 To: You

📧 📧 📧 ...
9/5/2023 10:14 AM

Hey again,

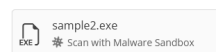
Good work. That detection you added blocked my malware from executing. Since file hashes and digests are unique to each file, they are, by far, the *highest confidence* indicators out there. You can be sure it's my malware sample the next time you see that hash.

However, by design, that is also one of the significant downfalls of simply relying on hashes for detection mechanisms. Since they are so susceptible to change, I only need to alter a single bit of the file, and the detection rule you added will fail.

In fact, all I did this time was recompile the malware, and I generated a new file hash and executed it without issue. See if you can come up with a new way to detect sample2.exe!

🚩 Here's your flag: **THM{f3cbf08151a11a6a331db9c6cf5f4fe4}**

-Sphinx



ANSWER: THM{f3cbf08151a11a6a331db9c6cf5f4fe4}

THM Challenge: Summit
Difficulty: Easy
Ron

Q2: What is the second flag you receive after successfully detecting sample2.exe?

After analyzing the info of this sample file, we can see that this time the malware initiates network activity. The malware opens two connections to an IP address associated with “Microsoft Corporation” but there is also a third connection to an IP address - 154[.]35[.]10[.]113 associated with “Intrabuzz Hosting Limited” and it seems like the malware sends an HTTP GET request to that suspicious IP, via port 4444, which is a default port for many malicious applications, often remote access tools(RATs). This correlates with the “Trojan.Metasploit.A” tag we see in the General Info section, as Metasploit Framework often uses this port for its reverse shells and payloads.

General Info - sample2.exe

File Name sample2.exe
File Size 202.73 KB
File Type PE32+ executable (GUI) x86-64, for MS Windows
Analysis Date September 5, 2023
OS Windows 10x64 v1803
Tags Trojan.Metasploit.A
MIME application/x-dosexec
MD5 486613f685d89b15915a533b572a6bd
SHA1 6878976974c27c8547cf5acc98f628ad2f9e975
SHA256 d576245e85e6b752b2f6ff643abae61b2c1383556b0169f684934d6c6c1cd9f

Behaviour Analysis

MALICIOUS
METASPLOIT was detected
• sample2.exe (PID: 1927)

SUSPICIOUS
Connects to unusual IP address
• sample2.exe (PID: 1927)
Connects to unusual port
• sample2.exe (PID: 1927)

INFO
Reads the machine GUID from the registry
• sample2.exe (PID: 1927)
The process checks LSA protection
• sample2.exe (PID: 1927)
Reads the computer name
• sample2.exe (PID: 1927)
Checks supported languages
• sample2.exe (PID: 1927)

Network Activity

HTTP(S) requests: 1
TCP/UDP connections: 3
DNS requests: 0
Threats: 0

HTTP requests

PID	Process	Method	IP	URL
1927	sample2.exe	GET	154.35.10.113:4444	http://154.35.10.113:4444/ui/L8Yf32

Connections

PID	Process	IP	Domain	ASN
1927	sample2.exe	154.35.10.113:4444	-	Intrabuzz Hosting Limited
1927	sample2.exe	40.97.128.3:443	-	Microsoft Corporation
1927	sample2.exe	40.97.128.4:443	-	Microsoft Corporation

Let's use our Firewall Rule Manager to block the outbound connections to this IP address by creating an *Egress*(outbound) rule, where *Any*(all) devices on our network will be denied to communicate with the suspicious destination IP that we found earlier.

Firewall Rule Manager
Home / IOC Management / Firewall Rule Manager

Create Firewall Rule

Type:
Source IP:
Destination IP:
Action:

Active Rules

Nice work! The firewall rule prevented sample2.exe from connecting to the tester's command-and-control server. Check your inbox for the next steps.

Enabled	Type	Source	Destination	Action	Settings
Yes	Egress	Any	154.35.10.113	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Egress	10.10.23.45	142.56.78.90	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Ingress	88.90.123.45	Any	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Ingress	203.56.78.90	Any	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Egress	Any	203.78.90.12	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Ingress	121.111.13.14	Any	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Ingress	187.123.45.67	10.10.23.45	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Ingress	154.67.89.23	10.10.56.78	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Egress	Any	95.123.45.67	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Yes	Egress	10.10.45.67	180.23.45.67	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>

THM Challenge: Summit
Difficulty: Easy
Ron

It worked, we got our second flag!

Stumped again... for now!

Sphinx <sphinx@pentesting.thm>

To: You

9/5/2023 10:58 AM

Huh.

It seems like you stopped me again. You must have found the IP address to which my malware sample connected. Clever!

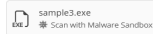
This method isn't bulletproof, though, as it's trivial for a motivated adversary to get around it using a new public IP address. I just signed up for a cloud service provider and now have access to many more public IPs!

This time, you'll need to detect `sample3.exe` another way. I already have my server running from a new IP address and have plenty more backups to fallow in case they get blocked!

Good luck. 🍀

Here's your flag: `THM{2ff48a3421a938b388418be273f4806d}`

-Sphinx



ANSWER: `THM{2ff48a3421a938b388418be273f4806d}`

Q3: What is the third flag you receive after successfully detecting sample3.exe?

This malware initiates a download of another presumably malicious file “backdoor.exe” by reaching the following domain - “emudyn[.]bresonicz[.]info”. As blocking only the IP address will make it easy for the attacker to come back with a different one, let's make it a little more “painful” and use the “DNS Rule Manager” to block the domain being used for downloading the file.

General Info - sample3.exe

File Name sample3.exe
File Size 207.12 KB
File Type PE32+ executable (GUI) x86-64, for MS Windows
Analysis Date September 5, 2023
OS Windows 10x64 v1903
Tags Trojan/Malicious.A
MIME application/x-dosexec
MD5 e11f96a19210b0a070ba9a7c0a0b0e
SHA1 af320a0a33a346209f7a8271a7f73131305a79
SHA256 a3308c208108a40f7f7308a4c3093131305a7944c131305a7944c131305a7944c1

Behaviour Analysis

MALICIOUS
MICAPLDR.dll was detected
• sample3.exe (PID: 1021)
Downloaded executable file from the Internet
• backdoor.exe (PID: 2712)

SUSPICIOUS
Connects to unusual IP address
• sample3.exe (PID: 1021)
Connects to unusual port
• sample3.exe (PID: 1021)

RPO
Reads the machine GUID from the registry
• sample3.exe (PID: 1021)
The process checks LSA protection
• sample3.exe (PID: 1021)
Reads the computer name
• sample3.exe (PID: 1021)
Checks supported languages
• sample3.exe (PID: 1021)

Network Activity

HTTP(S) requests: 2
TCP/UDP connections: 4
DNS requests: 2
Threats: 0

HTTP requests

PID	Process	Method	IP	URL
1021	sample3.exe	GET	62.123.140.9:1337	http://emudyn.bresonicz.info/1337/tan203a
1021	sample3.exe	GET	62.123.140.9:80	http://emudyn.bresonicz.info/backdoor.exe

Connections

PID	Process	IP	Domain	ASN
1021	sample3.exe	40.97.128.4:443	services.microsoft.com	Microsoft Corporation
1021	sample3.exe	62.123.140.9:1337	emudyn.bresonicz.info	Xpionta Cloud Services
1021	sample3.exe	62.123.140.9:80	emudyn.bresonicz.info	Xpionta Cloud Services
2712	backdoor.exe	62.123.140.9:80	emudyn.bresonicz.info	Xpionta Cloud Services

DNS requests

Domain	IP
services.microsoft.com	40.97.128.4
emudyn.bresonicz.info	62.123.140.9

Let's choose a rule name that describes what we are about to block, choose *Malware* as the category, provide the domain name, and finally select *Deny* as the action.

The reason for blocking the domain “bresonicz[.]info” rather than the whole url including the subdomain is to avoid the case where the attacker would only have to change the subdomain if they intend to repeat the attack. This way, we make them acquire a new domain, which might be more expensive and time consuming.

RE: Stumped again... for now!

 Sphinx <sphinx@pentesting.thm>

 To: You

9/5/2023 11:32 AM

It looks like you were able to block my domain this time because every new IP address I try gets detected. You're causing me a bit of trouble now because I have to purchase and register some new domain names and modify DNS records. Some attackers might get mildly annoyed by this and find a new target, but I'm motivated to continue like many.

Moving up our Pyramid of Pain, we encounter a behavior that tempers with our registry to evade our anti-virus

General Info - sample4.exe

Q5: What is the fifth flag you receive after successfully detecting sample5.exe?

This time we are being provided with an outgoing traffic log.

Viewing attachment: [outgoing_connections.log](#)

2023-08-15 09:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 09:23:45	Source: 10.10.15.12	Destination: 43.10.65.115	Port: 443	Size: 21541 bytes
2023-08-15 09:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 10:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 10:14:21	Source: 10.10.15.12	Destination: 87.32.56.124	Port: 80	Size: 1204 bytes
2023-08-15 10:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 11:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 11:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 11:45:09	Source: 10.10.15.12	Destination: 145.78.90.33	Port: 443	Size: 805 bytes
2023-08-15 12:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 12:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 13:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 13:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 13:32:17	Source: 10.10.15.12	Destination: 72.15.61.98	Port: 443	Size: 26084 bytes
2023-08-15 14:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 14:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 14:55:33	Source: 10.10.15.12	Destination: 208.45.72.16	Port: 443	Size: 45091 bytes
2023-08-15 15:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 15:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 15:40:10	Source: 10.10.15.12	Destination: 101.55.20.79	Port: 443	Size: 95021 bytes
2023-08-15 16:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 16:18:55	Source: 10.10.15.12	Destination: 194.92.18.10	Port: 80	Size: 8004 bytes
2023-08-15 16:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 17:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 17:09:30	Source: 10.10.15.12	Destination: 77.23.66.214	Port: 443	Size: 9584 bytes
2023-08-15 17:27:42	Source: 10.10.15.12	Destination: 156.29.88.77	Port: 443	Size: 10293 bytes
2023-08-15 17:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 18:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 18:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 19:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 19:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 20:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 20:30:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes
2023-08-15 21:00:00	Source: 10.10.15.12	Destination: 51.102.10.19	Port: 443	Size: 97 bytes

Examining the log file for anomalies, we spot a regular, periodic and encrypted communication from the victim machine to the IP address - 51[.]102[.]10[.]19 via port 443. It repeats every 30 minutes, sending a packet with a size of exactly 97kb each time. Analyzing our findings, we may assume that this behavior indicates a C2 communication taking place. Let's confirm this by navigating to MITRE website, and follow up with creating a rule to block this behaviour.

MITRE | ATT&CK

ATT&CKicon 6.0 is coming October 14-15 in McLean, VA and live online. To potentially join us on stage, submit to our CFP by July 9th

TACTICS

Enterprise

Reconnaissance

Resource Development

Initial Access

Execution

Home > Tactics > Enterprise > Command and Control

Command and Control

The adversary is trying to communicate with compromised systems to control them.

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

ID: TA0011

Created: 17 October 2018

Last Modified: 25 April 2025

Time to take action! Let's navigate through - "Create Sigma Rule" → "Sysmon Event Logs" → "Network Connections", and use all previously gathered information to create the best rule we can. Starting with the "Remote IP" and "Remote Port", we want to keep these on *Any* to prevent the attacker from simply changing them to avoid our new rule, as we are trying to make it more "painful" for them to return in the future by denying them the ability to reuse the same tools. Therefore, we will use more specific information to block this one out. We know the exact size of the packet that is being sent(97kb) and the frequency with which it happens(30 minutes\1800 seconds), and the ATT&CK ID that is being used(TA0011). Let's click on "Validate Rule".

THM Challenge: Summit

Difficulty: Easy

Ron

Create Sigma Rule

Step 1: I want to create a rule that focuses on:

- ☒ **Sysmon Event Logs**
Sysmon is a Windows system service that monitors and logs various system activities. It provides detailed information about command-line activity, process creations, network connections, file creation, and more.
- ☐ **Web Server Logs**
Logs from web servers like Apache or Nginx can provide information about incoming requests, user agents, URLs accessed, and more.
- ☐ **VPN Logs**
Logs from virtual private network (VPN) services can show connections and disconnections, user activities, and potential unauthorized access.
- ☐ **Application Logs**
Logs generated by various applications can provide insights into their behavior, including errors, authentication attempts, and unusual activities.

Step 2: Sysmon Event Logs

I want to target the Sysmon event:

- ☐ **Process Creation**
Detect specific processes being created.
- ☐ **File Creation and Modification**
Detect files being created or modified, changes to critical system files, or creation of executables or scripts.
- ☒ **Network Connections**
Detect outgoing network connections, network traffic patterns, or connections made by specific processes.
- ☐ **Registry Modifications**
Detect changes in registry keys or values such as system settings, security policies, automn entries, or access control configurations.

Step 3: Network Connections

Set the rule conditions and options:

This rule will detect network connections made from a host machine with specific conditions, such as remote IP, port, size of the connection, and how often it occurs (frequency).

Remote IP:

Remote Port:

Size bytes:

Frequency (seconds):

ATTACK ID:

Sigma Rule Validation

```
title: Alert on Suspicious Remote Network Connections
id: network_connection_suspicious_sysmon
description: |
  Detects network connections with specific criteria in Sysmon logs: remote IP, remote port, size, and frequency.

references:
  - https://artforhackers.com/articles/THM/

tags:
  - attack.t0001
  - sysmon

detection:
  selection:
    RemoteIP: '*'
    RemotePort: '*'
    Size: 0
    Frequency: 1800 seconds
  condition: selection

falsepositives:
  - Legitimate network traffic may match this criteria.

level: high
```

Great, we made the attacker spend more time and resources on finding a new tool with a different behaviour if they intend to continue attacking us.

RE: New Approach

Sphinx <sphinx@pentesting.thm>

To: You

8/5/2023 1:02 PM

Hello again,

You managed to detect `sample.exe`! I'm very impressed. But also very annoyed! Because now, I need to go back to the drawing board and create a brand new tool to do what I need to do. If I can't find another one quickly, this will be another significant investment. Also, I will need to train myself all over again on how to use it!

I can keep this up one or two times, but there's no way I can continue after this. The reward no longer outweighs the cost, and I would instead find an easier target with detection capabilities much lower on the pyramid.

For my last trick, I have `sample.exe`. This time, you will need more than artifacts or tool detection to help you. You'll need to focus on something extremely hard for me to change subconsciously - my techniques and procedures.

I've attached the recorded command logs from all my previous samples to understand better what actions I tend to perform on my victims to extract info once I have remote access. Good luck!

Here's your flag: `THM{46b21c4410e47dc5729ceadef0fc722e}`

-Very Annoyed Sphinx

commands.log

Open in the Attachment Viewer

ANSWER: `THM{46b21c4410e47dc5729ceadef0fc722e}`

Q6: What is the final flag you receive from Sphinx?

Finally, we reached our last step following the "Pyramid of Pain". This time we look at a log file that contains a list of commands that are being executed. Let's take a look.

Viewing attachment: `commands.log`

```
dir c:\ >> %temp%\exfiltr8.log
dir "c:\Documents and Settings\" >> %temp%\exfiltr8.log
dir "c:\Program Files\" >> %temp%\exfiltr8.log
dir d:\ >> %temp%\exfiltr8.log
net localgroup administrator >> %temp%\exfiltr8.log
ver >> %temp%\exfiltr8.log
systeminfo >> %temp%\exfiltr8.log
ipconfig /all >> %temp%\exfiltr8.log
netstat -ano >> %temp%\exfiltr8.log
net start >> %temp%\exfiltr8.log
```

THM Challenge: Summit

Difficulty: Easy

Ron

We see that the commands being executed are writing different data to a certain “exfiltr8.log” file in our victim’s %temp% folder, trying to exfiltrate information about our host and network. Before we proceed, we can check if it corresponds with MITRE description regarding exfiltration tactics.

MITRE ATT&CK

ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. To potentially join us on stage, submit to our CFP by July 9th

Tactics

Enterprise

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Home > Tactics > Enterprise > Exfiltration

Exfiltration

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

ID: TA0010

Created: 17 October 2018

Last Modified: 25 April 2025

Version Permalink

Let's take action to prevent that .log file from being created in the first place. Navigating through “Create Sigma Rule” → “Sysmon Event Logs” → “File Creation and Modification”, we may now fill the blanks to create our rule. The “File Path” would be the %temp% folder as we saw in our logs, which is essentially a shortcut for - “C:\Users\username\AppData\Local\Temp”. The filename of the file that the data is being written to is - “exfiltr8.log”, and the ATT&CK ID is - TA0010.

Sigma Rule Builder

Home > Sigma Rule Builder

Step 1: Create Sigma Rule

I want to create a rule that focuses on:

System Event Logs

System is a Windows system device that monitors and logs various system activities. It provides detailed information about command line activity, process creation, network connections, file creation, and more.

Web Server Logs

Logs from web servers like Apache or Nginx can provide information about incoming requests, user agents, URLs accessed, and more.

VPN Logs

Logs from virtual private network (VPN) services can show connections and disconnections, user activities, and potential unauthorized access.

Application Logs

Logs generated by various applications can provide insights into their behavior, including errors, authentication attempts, and unusual activities.

Step 2: System Event Logs

I want to target this system event:

Process Creation

Detect specific processes being created.

File Creation and Modification

Detect files being created or modified, changes to critical system files, or creation of executables or scripts.

Network Connections

Detect outgoing network connections, network traffic patterns, or connections made by specific processes.

Registry Modifications

Detect changes to registry keys or values such as system settings, security policies, autounattend, or access control configurations.

Step 3: File Creation and Modification

Set the rule conditions and options:

File Path*

Example

File Name*

exfiltr8.log

ATT&CK ID*

Exfiltration (TA0010)

At PulseSecure we require that all Sigma detection rules map to the MITRE ATT&CK framework. We recommend that you verify that the chosen conditions and options match the intended attack and response.

Cancel Validate Rule

Sigma Rule Validation

Compare an existing Sigma Rule. Check your rules for the final flag

YAML

title: Alert on Insecure Exfiltration through File Creation or Modification

id: system_file_creation_modification_log

description: |

Detects File Creation or Modification events with specific criteria: File path and File name.

references: |

- https://attack.mitre.org/techniques/T1059/

tags: |

- attack:osint

- attack:exfiltration

- attack:file_creation

- attack:file_modification

- system

detection: |

selection: |

- eventid: 1

- filename: "****.log"

- filename: "****.tmp"

condition: selection

falsepositives: |

- legitimate use of file creation and modification in a user's temp folder.

level: high

Clicking on the “Validate Rule” button, we see that our rule worked and we made the attacker give up after we successfully defended our systems from everything they had in their adversary arsenal against us.

I'm Giving Up

Sphinx <sphinx@pentesting.thm>

To: You

9/5/2023 2:42 PM

Well, that's it. I have officially given up.

Throughout the engagement, you managed to chase me to the very top of the Pyramid of Pain, and I have to say, it's not fun up here!

You detected my samples file hashes, IPs, domains, host artifacts, tools, and now my own behavioural techniques! To continue, I have no choice but to completely retrain myself and conduct extensive research to figure out how you're catching me. And with that, I don't think you'll ever see me again. Enjoy the final flag: you've earned it!

Here's your flag: THM{c8951b2ad24bbcbac60c16cf2c83d92c}

-A significantly defeated Sphinx!

ANSWER: THM{c8951b2ad24bbcbac60c16cf2c83d92c}

8