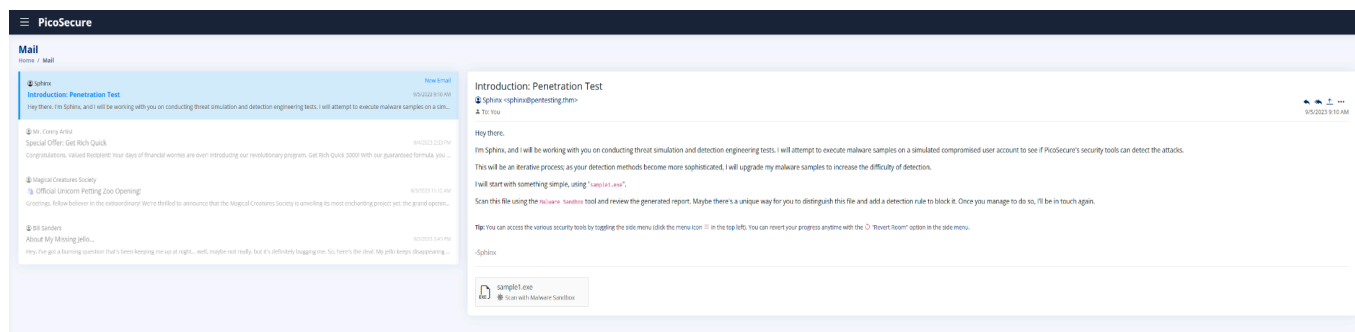


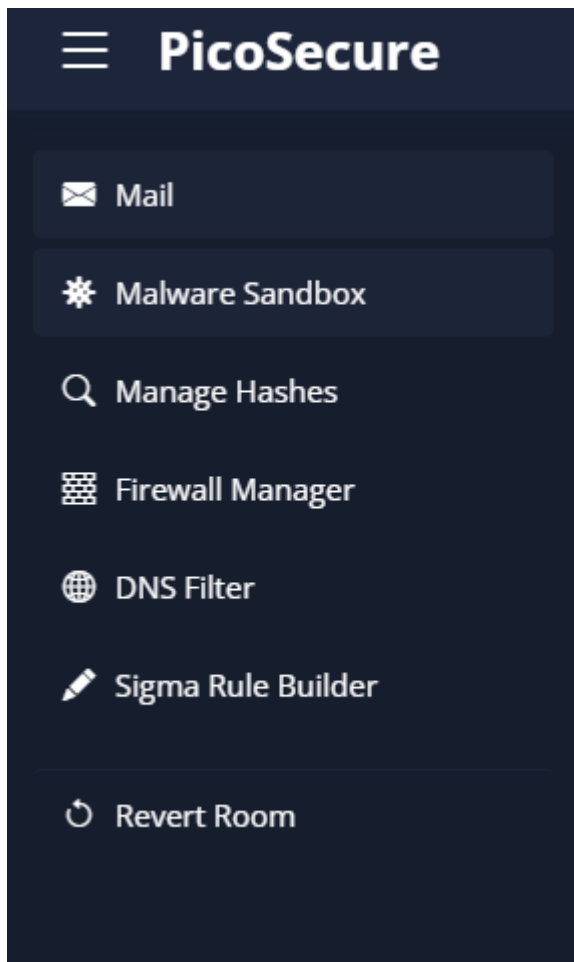
TryHackMe: Summit Write Up

We start with the emulated environment, in here we have an inbox with alerts, we are only interested on the “sample” attachments.

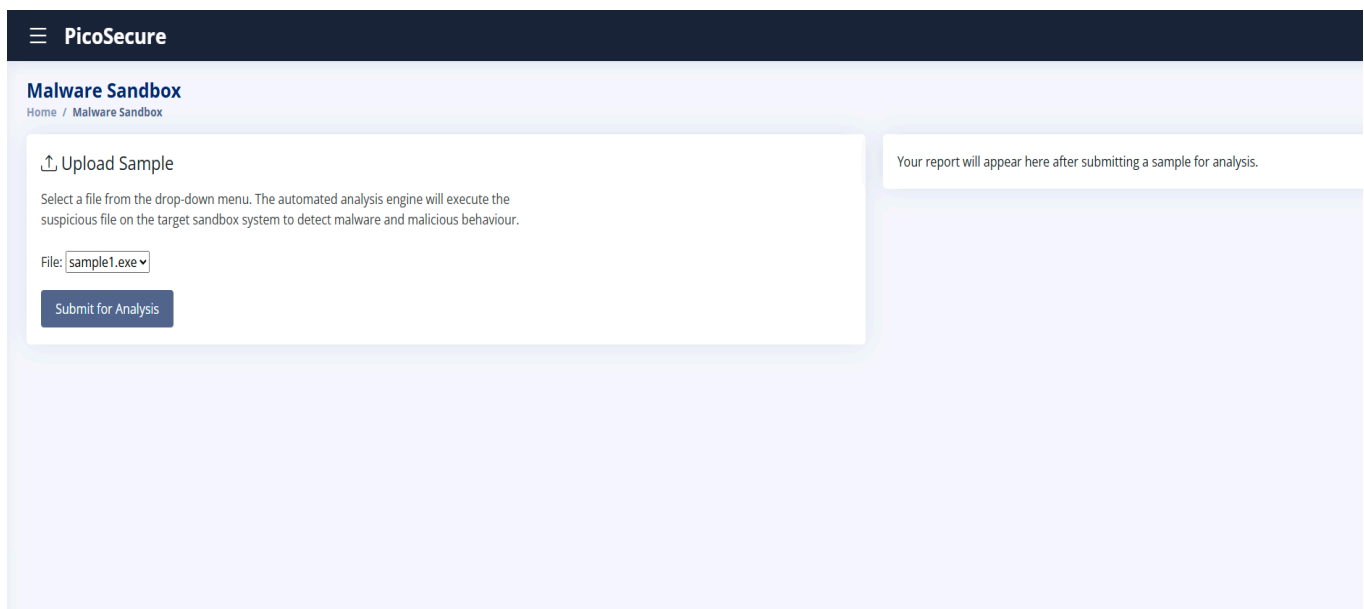
We have `sample1.exe` that we need to analyze.



In this sandbox we have different tools, let's start with the “Malware Sandbox” tool.



We attempt to analyze the sample1.exe file to get a report



After analysis we get a report with a wealth of information and we see the different types of hashes

Menu icon

PicoSecure

Malware Sandbox

Home / Malware Sandbox

Upload Sample

Select a file from the drop-down menu. The automated analysis engine will execute the suspicious file on the target sandbox system to detect malware and malicious behaviour.

File: sample1.exe

Submit for Analysis

General Info - sample1.exe

File Name	sample1.exe
File Size	202,50 KB
File Type	PC32 - executable (GUI) x86-64, for MS Windows
Analysis Date	September 5, 2023
OS	Windows 10/64 v1803
Tags	Trojan.Metasploit.A
MIME	application/x-dosexec
MD5	c8da5ae99b9a7376184922ae99f6c2a
SHA1	83d2791ca93a3868839483aee21073d9d89763d8
SHA256	5c39831a3c4223b357474457068133a7c1983f9e3d9f73386144853dc09f9c4b6

Behaviour Analysis

MALICIOUS

METASPLOIT was detected

sample1.exe (PID: 2450)

SUSPICIOUS

Connects to unusual port

sample1.exe (PID: 2450)

INFO

Reads the machine GUID from the registry

sample1.exe (PID: 2450)

The process checks LSA protection

sample1.exe (PID: 2450)

Reads the computer name

sample1.exe (PID: 2450)

Checks supported languages

sample1.exe (PID: 2450)

We discovered the hashes of sample1.exe, we can use these to block the malware using our EDR.

PicoSecure

Manage Hashes

Home / SOC Management / Manage Hashes

Q Detect Hashes

Manually add a hash to the blacklist

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**

Submit Hash

Hash Blacklist

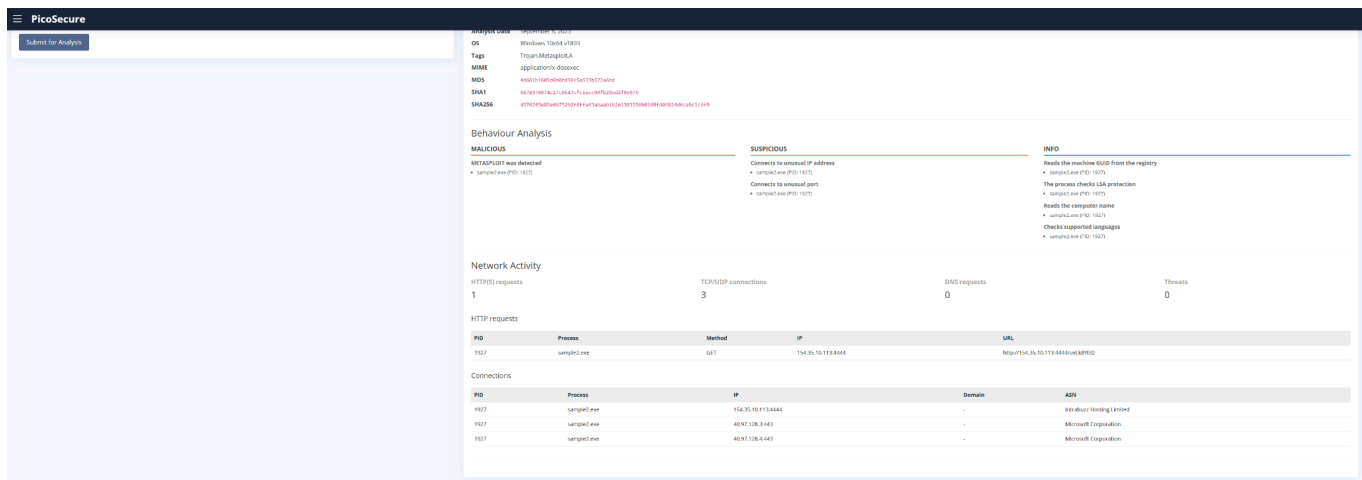
New world! You prevented [some bot.exe](#) from executing by detecting its unique hash value. Check your [inbox](#) for the next steps.

Algorithm	Value	Actions
SHA256	9c0999f1a2e5d28b3c5518f158f153af761bf8dc2cf789f5d33cc9ef9a6e	<div><div></div><div></div><div></div></div>
MDS	c2a094763da5bd8ff3ca585ba9e17	<div><div></div><div></div><div></div></div>
MDS	85481ed0f9a4a9c5c537f100b2e15010	<div><div></div><div></div><div></div></div>
SHA1	359835ac181c1e20278c5c9903100827ee4fb	<div><div></div><div></div><div></div></div>
SHA256	e434fa77555214ab887aa08674ae76a6c0391faeb753ba4f77ea0bb0a1f550a	<div><div></div><div></div><div></div></div>
SHA256	d9857d2380ad0e439f761632f79a418f89c762a52295870f80817705448f	<div><div></div><div></div><div></div></div>
SHA256	e8f337eedabaf12a168308b0a876a23807aaa08036c7616391c2403eabdf	<div><div></div><div></div><div></div></div>

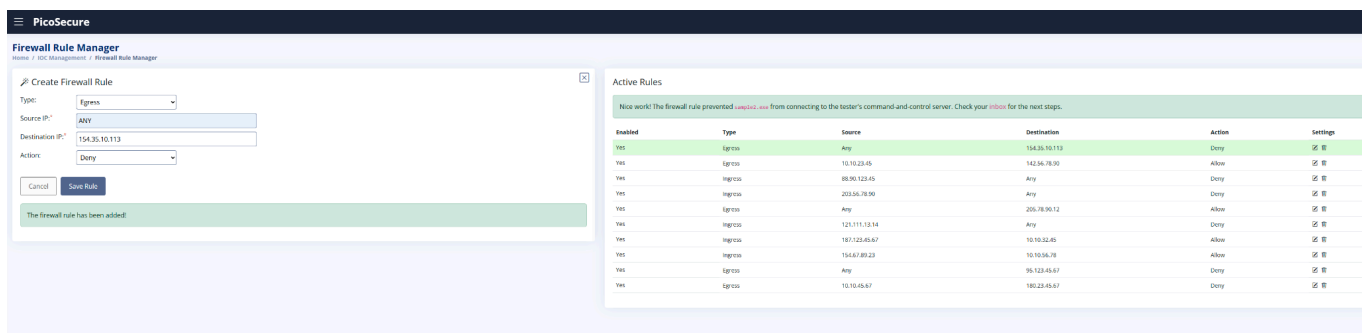
We submitted the sha256 hash to block using our EDR, and continue on to our next alert in the inbox

[illegible]

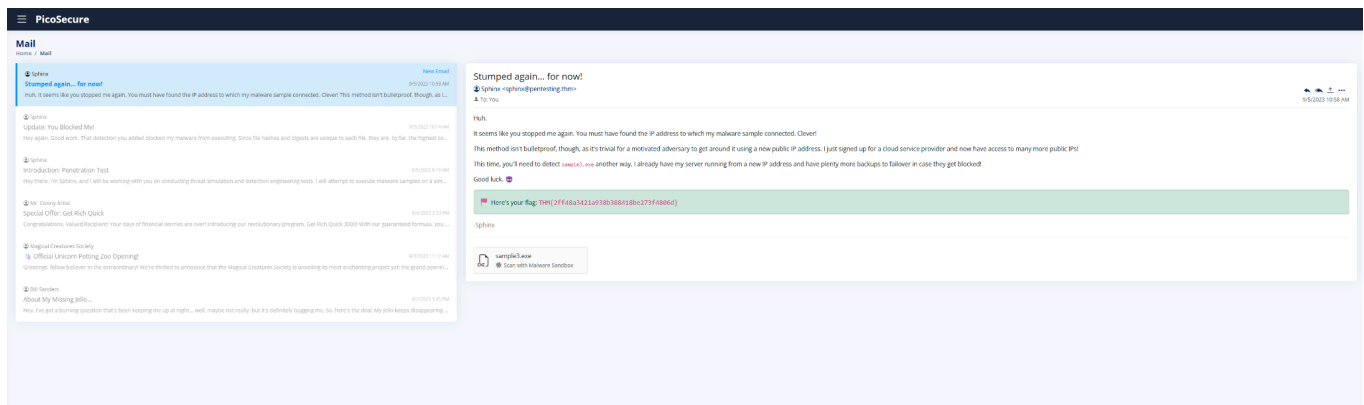
In the inbox we get sample2.exe and the flag, let analyze sample2



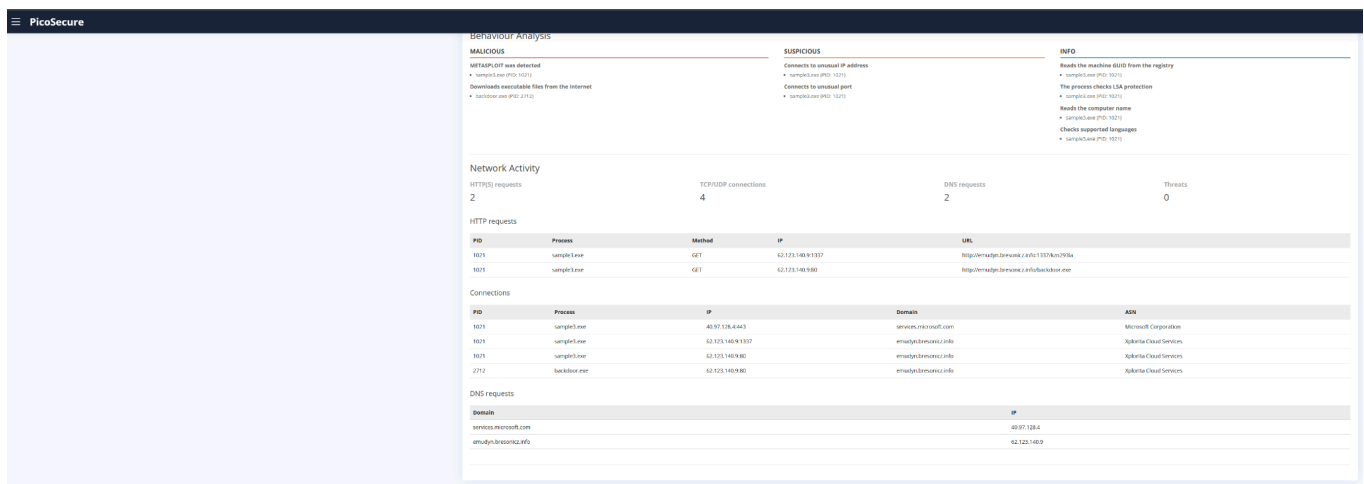
For sample2 we are getting network connections from “unusual ip” and “unusual port”. We can use a firewall to block these connections. On the HTTP request, sample2.exe attempted to get a webpage or connection from ip:port 154.35.10.113:4444, so let’s block the ip 154.35.10.113 using our firewall.



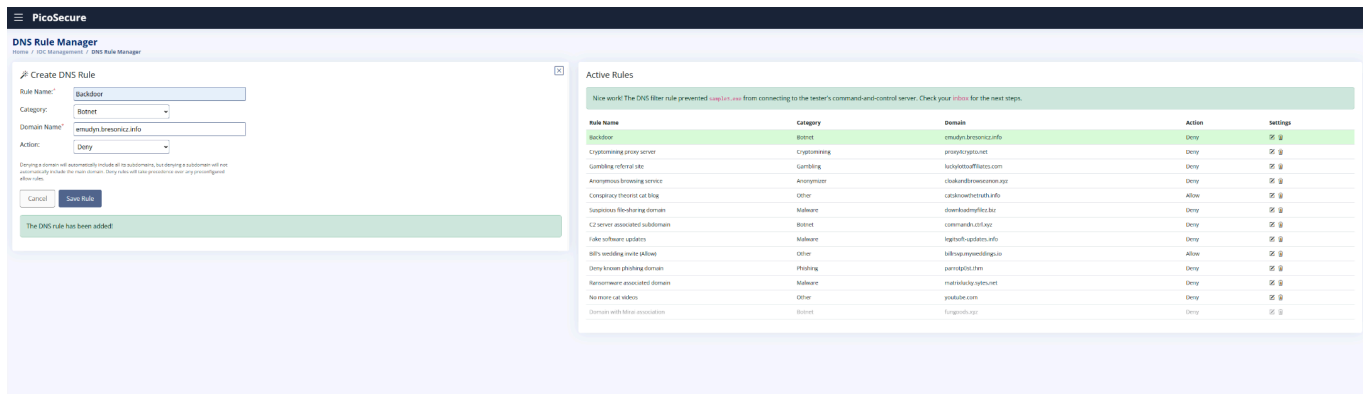
Since the malware is trying to connect externally, we setup the rule to “egress” meaning outside, the source ip to “ANY” since it could come from any of our endpoints within the network, the destination ip to 154.35.10.113 since thats the ip we got from the report communicating externally and we deny any packages for this rule.



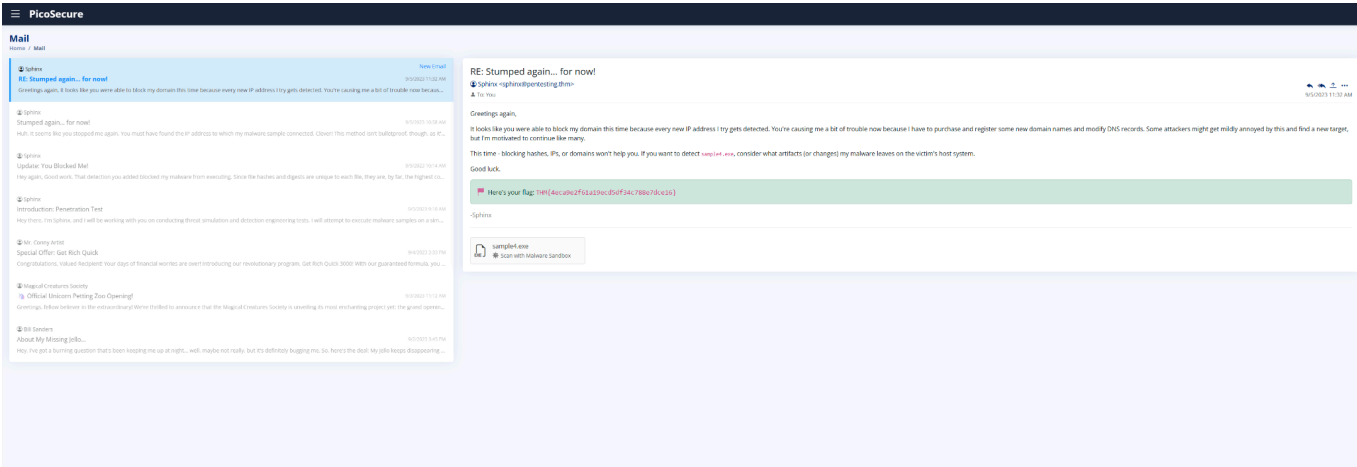
We get the flag and a new sample to dissect, lets run the malware analysis on it.



Based on the analysis for sample3, this seems to be a backdoor trying to install more tools over the internet, and is using DNS to accomplish this. We can block communications coming from **emudyn.bresonicz.info** using dns filtering.



We setup a DNS rule with the name backdoor, blocking the domain above.



We get the flag and the next sample, sample4. Let’s run some analysis on it.

Registry Activity			
Total events	Read events	Write events	Delete events
3	1	2	0
Modification events			
(PID) Process: (3806) sample4.exe		Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection	
Operation: write		Name: DisableRealTimeMonitoring	
Value: 1			
(PID) Process: (1928) explorer.exe		Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	
Operation: write		Name: EnableBalloonTips	
Value: 1			
(PID) Process: (9876) notepad.exe		Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt	
Operation: read		Name: ProgId	
Value: txtfile			

We are getting some registry activity this time. We can use the Sigma rule builder, similar to Yara rules on other systems.

PicoSecure

Sigma Rule Builder

Home / IOC Management / Sigma Rule Builder

✦ 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.

Lets select sysmon

Step 2: Sysmon Event Logs

I want to target this 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 to registry keys or values such as system settings, security policies, autorun entries, or access control configurations.

Since it is modifying the registry on windows, lets select registry modifications

☒ **Registry Modifications**

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

Step 3: Registry Modifications

Set the rule conditions and options:

Registry Key:*	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows De
Registry Name:*	disablerealtimemonitoring
Value:*	1
ATT&CK ID:*	Defense Evasion (TA0005) ▼

At PicoSecure, we require that all Sysmon detection rules map to the [MITRE ATT&CK framework](#). This ensures that our SOC team has the context to facilitate a more effective threat detection, analysis, and response.

Cancel

Validate Rule

And fill in the registry key is being modified, in this case is trying to disable real time monitoring to evade detection as part of the MITRE ATT&CK TA0005

Sigma Rule Validation

```
title: Modification of Windows Defender Real-Time Protection
id: windows_registry_defender_disable_realtime
description: |
  Detects modifications or creations of the Windows Defender Real-Time Protection DisableRealtimeMonitoring registry value.

references:
  - https://attack.mitre.org/tactics/TA0005/

tags:
  - attack.ta0005
  - sysmon

detection:
  selection:
    EventID: 4663
    ObjectType: Key
    ObjectName: 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection'
    NewValue: 'DisableRealtimeMonitoring=1'

  condition: selection

falsepositives:
  - Legitimate changes to Windows Defender settings.

level: high
```

Rule is created.

PicoSecure

Attachment Viewer

Home / Mail / Attachment Viewer

New Approach

Sphinx <sphinx@pentesting.thm>

To: You

9/5/2023 12:23 PM

Hey,

I'm not sure what you managed to do this time, but you seriously threw a wrench into my malware sample! I spent ages trying to reconfigure my attack tools and methodologies to get around your detection - SUPER ANNOYING!

Having my team develop new techniques used in my adversary tools was a time-consuming effort and a significant cost. It's good that we have a substantial budget for this engagement, but many threat actors would have given up and found a new victim by now.

I finally have `sample5.exe` for you to detect. Different approach this time. In this sample, all of the "heavy lifting" and instruction occurs on my back-end server, so I can easily change the types of protocols I use and the artifacts I leave on the host. You'll have to find something unique or abnormal about the behaviour of my tool to detect it.

I attached the logs of the outgoing network connections from the last 12 hours on the victim machine. That may help you correlate something.

I don't know what to do if you can stop me at this level.

Here's your flag: `THM{c956f455fc076aea829799c0876ee399}`

-Annoyed Sphinx

outgoing_connections.log

Open in the Attachment Viewer

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: 72.15.61.88	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: 100.55.20.79	Port: 443	Size: 9021 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: 150.29.88.77	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

We get the flag and a new log for outgoing connections, after opening it we get a list of ips. This seems to be a C2 based on the smaller bits of communications.

Since the attacker is changing protocols, we cannot use the usual tools to block this attack. However, we can use the sigma rules to create a rule based on pattern, this seems to match a c2

✳️ 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 this 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.

We select sysmon then network connections

📶 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, autorun 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:*	<input type="text" value="ANY"/>
Remote Port:*	<input type="text" value="ANY"/>
Size (bytes):*	<input type="text" value="97"/>
Frequency (seconds):*	<input type="text" value="1800"/>
ATT&CK ID:*	<input type="text" value="Command and Control (TA0011)"/>

At PicoSecure, we require that all Sysmon detection rules map to the [MITRE ATT&CK framework](#). This ensures that our SOC team has the context to facilitate a more effective threat detection, analysis, and response.

Cancel

Validate Rule

Since we know the attacker is using multiple ports and ip, we go by patterns, we see that the attacker is sending beaconing signals of 97 bits every 1800 seconds or 30 mins, just making sure the bot is alive, and this is a common c2 tactic

Sigma Rule Validation

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

references:
  - https://attack.mitre.org/tactics/TA0011/

tags:
  - attack.ta0011
  - sysmon

detection:
  selection:
    EventID: 3
    RemoteIP: '*'
    RemotePort: '*'
    Size: 97
    Frequency: 1800 seconds

  condition: selection

falsepositives:
  - Legitimate network traffic may match this criteria.

level: high
```

Here is the sigma rule validation

PicoSecure

Home / Mail /

RE: New Approach

Sphinx <sphinx@pentesting.thm>

To: You

9/5/2023 1:02 PM

Hello again,

You managed to detect `sample5.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 `sample6.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{46b21c4410e47dc5729ceade0fc722e}`

-Very Annoyed Sphinx! 😡

`commands.log`
Open in the Attachment Viewer

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
```

For the final tactic the attacker is getting desperate and is trying to exfiltrate all data from our endpoint into a log in the temp folder. We can block that with a sigma rule builder.

Step 2: Sysmon Event Logs

I want to target this 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 to registry keys or values such as system settings, security policies, autorun entries, or access control configurations.

This time we use file creation and modification from sysmon events.

Set the rule conditions and options:

exfiltr8.log

Exfiltration (TA0010)

Cancel Validate Rule

We get the final flag.

