Summit (Blue Team)

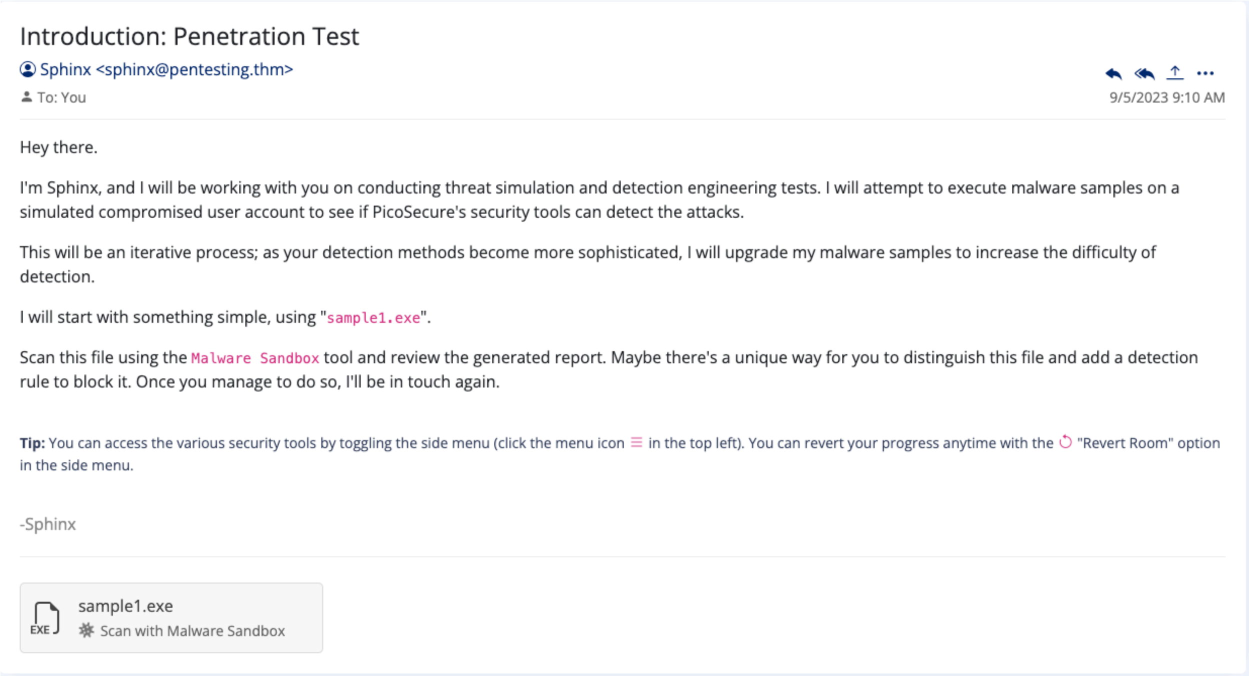
Created by	Kaio
Created time	@August 6, 2025 1:39 PM
Last edited by	Kaio
Last updated time	@August 18, 2025 11:41 PM

Objective

⇒ Follow **Pyramid of Pain**

Action

Read the email carefully



Introduction: Penetration Test

Sphinx <sphinx@pentesting.thm>

To: You

9/5/2023 9:10 AM

Hey there.

I'm Sphinx, and I will be working with you on conducting threat simulation and detection engineering tests. I will attempt to execute malware samples on a simulated compromised user account to see if PicoSecure's security tools can detect the attacks.

This will be an iterative process; as your detection methods become more sophisticated, I will upgrade my malware samples to increase the difficulty of detection.

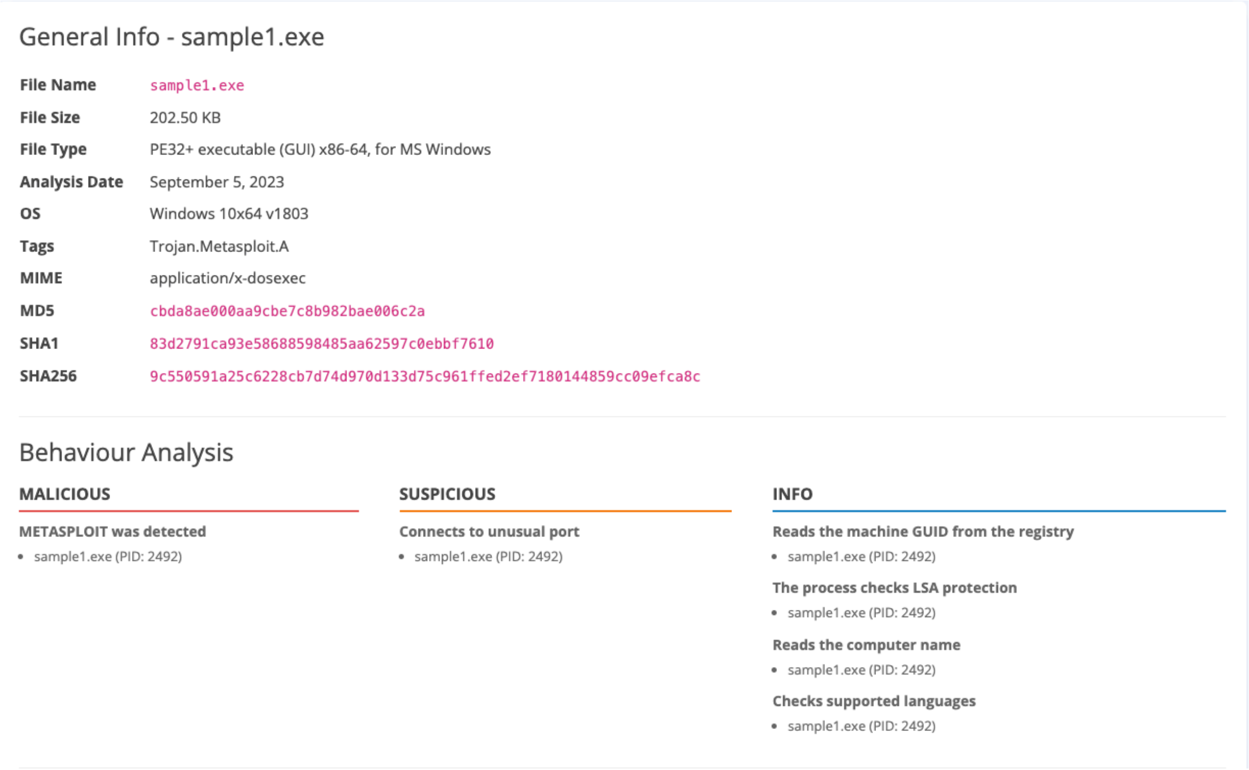
I will start with something simple, using "`sample1.exe`".

Scan this file using the `Malware Sandbox` tool and review the generated report. Maybe there's a unique way for you to distinguish this file and add a detection rule to block it. Once you manage to do so, I'll be in touch again.

Tip: You can access the various security tools by toggling the side menu (click the menu icon ☰ in the top left). You can revert your progress anytime with the ⭯ "Revert Room" option in the side menu.

-Sphinx

⇒ Our task is to analyzing the `sample1.exe` using the tool called `Malware Sandbox`



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
MD5	`cbda8ae000aa9cbe7c8b982bae006c2a`
SHA1	`83d2791ca93e58688598485aa62597c0ebbf7610`
SHA256	`9c550591a25c6228cb7d74d970d133d75c961ffed2ef7180144859cc09efca8c`

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)

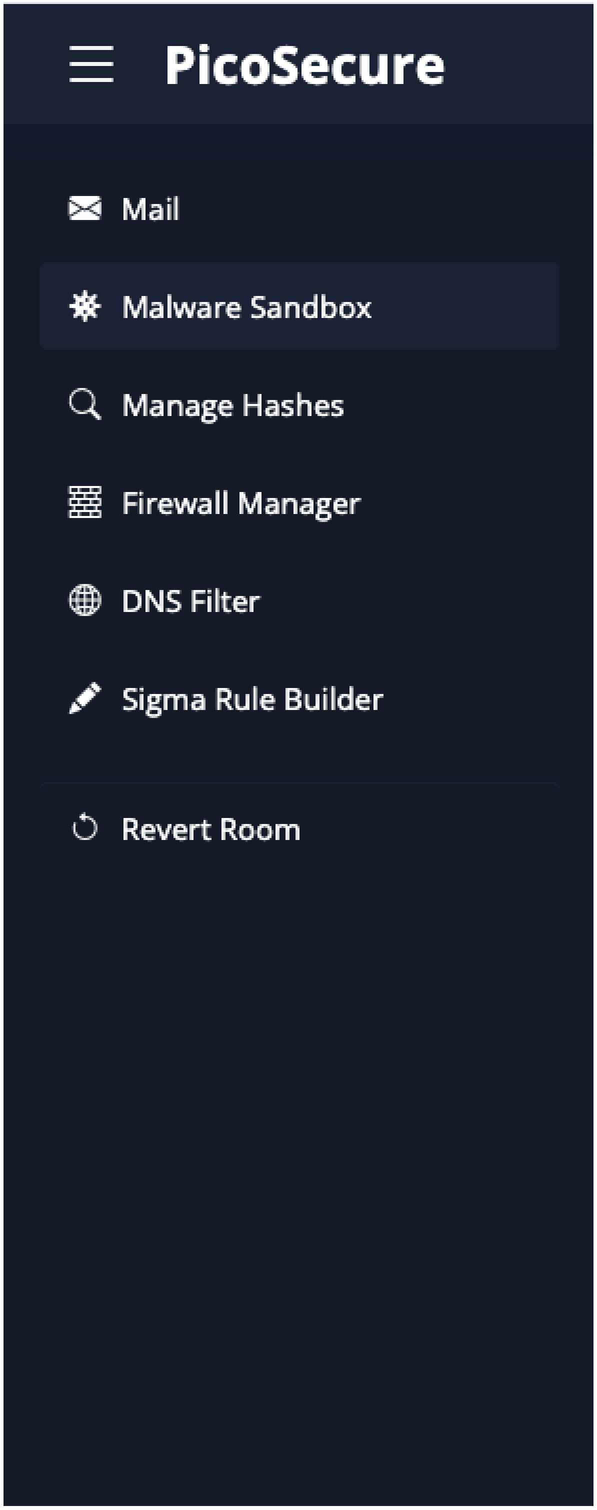
Reads the computer name

- sample1.exe (PID: 2492)

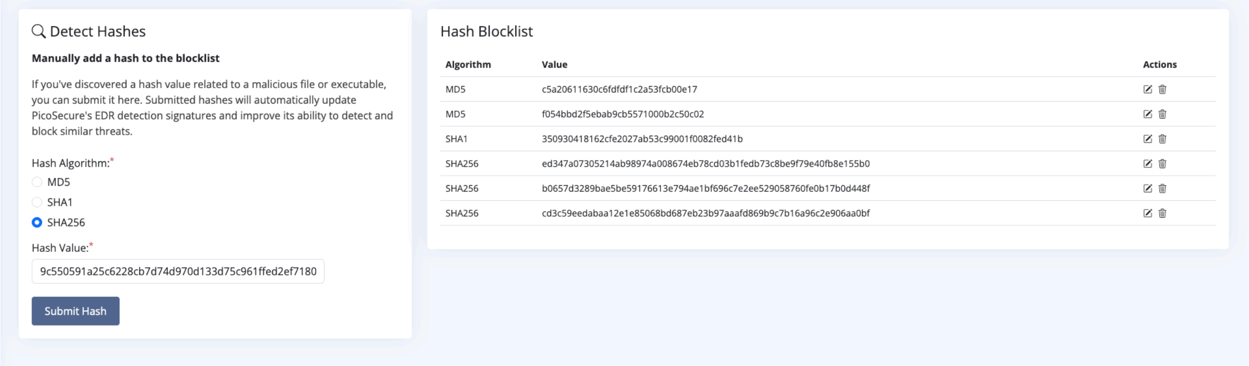
Checks supported languages

- sample1.exe (PID: 2492)

After analyzing it I notice that this file has hash values like MD5, SHA1, SHA256. ⇒ Add those hash values to the `Manage Hashes` ⇒ easily detect the attacks.



I entered the SHA256 to the Hash Blocklist



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:*

○ MD5

○ SHA1

● SHA256

Hash Value:*

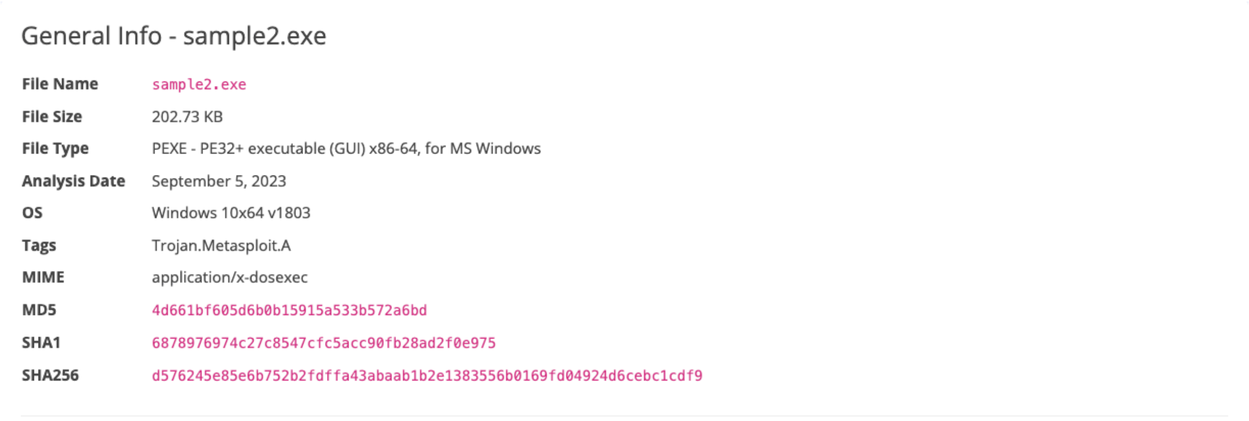
9c550591a25c6228cb7d74d970d133d75c961ffed2ef7180

Hash Blocklist

Algorithm	Value	Actions
MD5	c5a20611630c6fdfdf1c2a53fcb00e17	
MD5	f054bbd2f5ebab9cb5571000b2c50c02	
SHA1	350930418162cfe2027ab53c99001f0082fed41b	
SHA256	ed347a07305214ab98974a008674eb78cd03b1fedb73c8be9f79e40fb8e155b0	
SHA256	b0657d3289bae5be59176613e794ae1bf696c7e2ee529058760fe0b17b0d448f	
SHA256	cd3c59eedabaa12e1e85068bd687eb23b97aaafd869b9c7b16a96c2e906aa0bf	

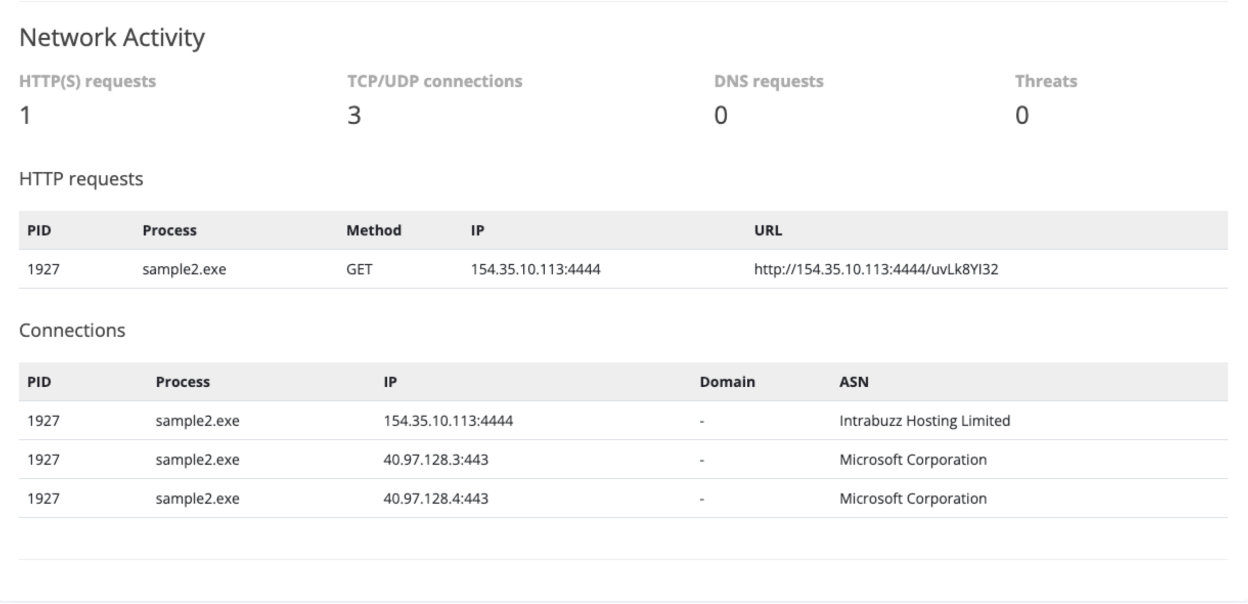
Then moving to the next question

→ Analysing `sample2.exe`



General Info - sample2.exe

File Name	sample2.exe
File Size	202.73 KB
File Type	PEXE - 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	4d661bf605d6b0b15915a533b572a6bd
SHA1	6878976974c27c8547cfc5acc90fb28ad2f0e975
SHA256	d576245e85e6b752b2fdffa43abaab1b2e1383556b0169fd04924d6cebc1cdf9



Network Activity

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

HTTP requests

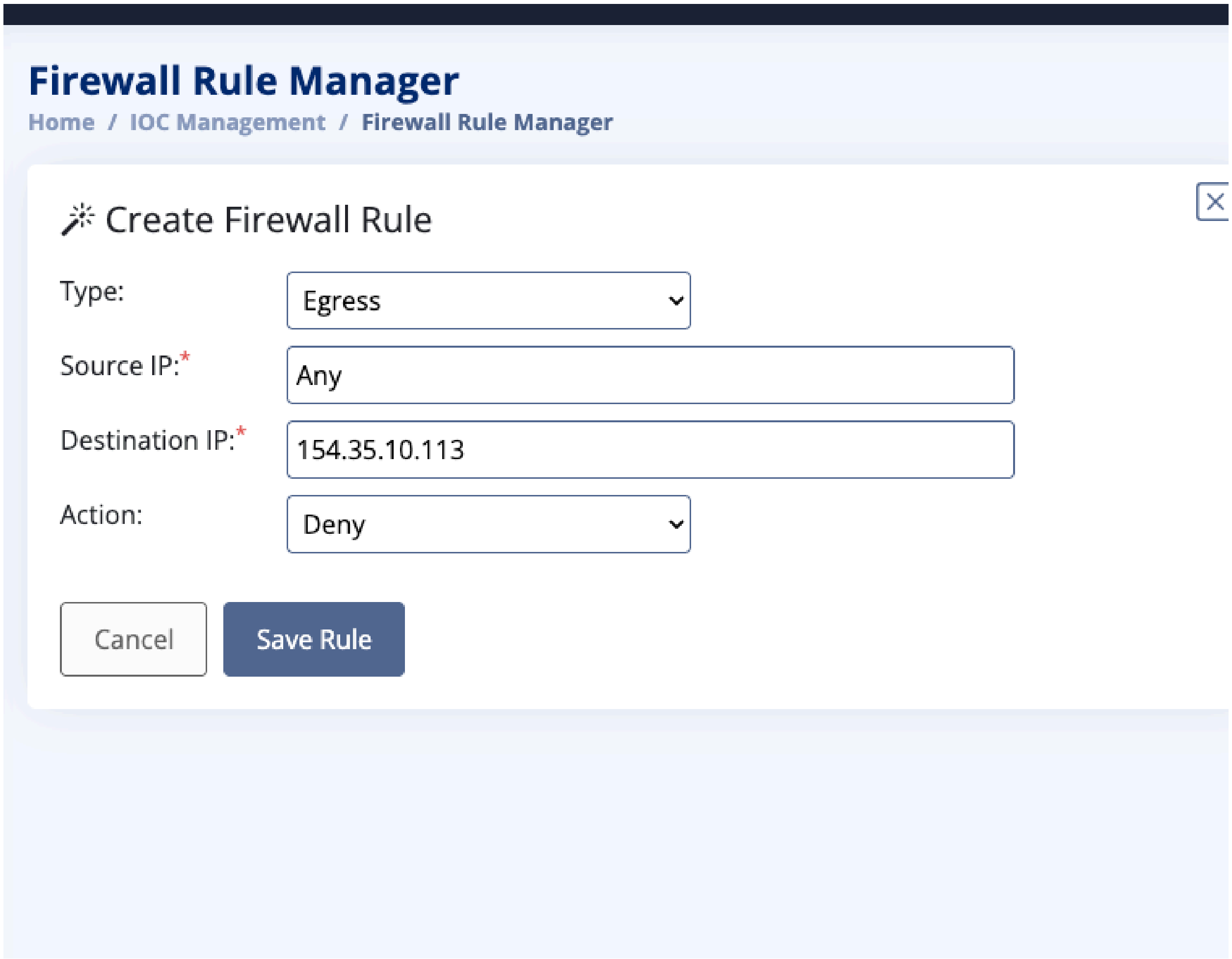
PID	Process	Method	IP	URL
1927	sample2.exe	GET	154.35.10.113:4444	http://154.35.10.113:4444/uvLk8YI32

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

this malware could try to get something from the URL `http://154.35.10.113:4444/uvLk8YI32`

⇒ block it ⇒ using firewall



Firewall Rule Manager

Create Firewall Rule

Type: Egress

Source IP:* Any

Destination IP:* 154.35.10.113

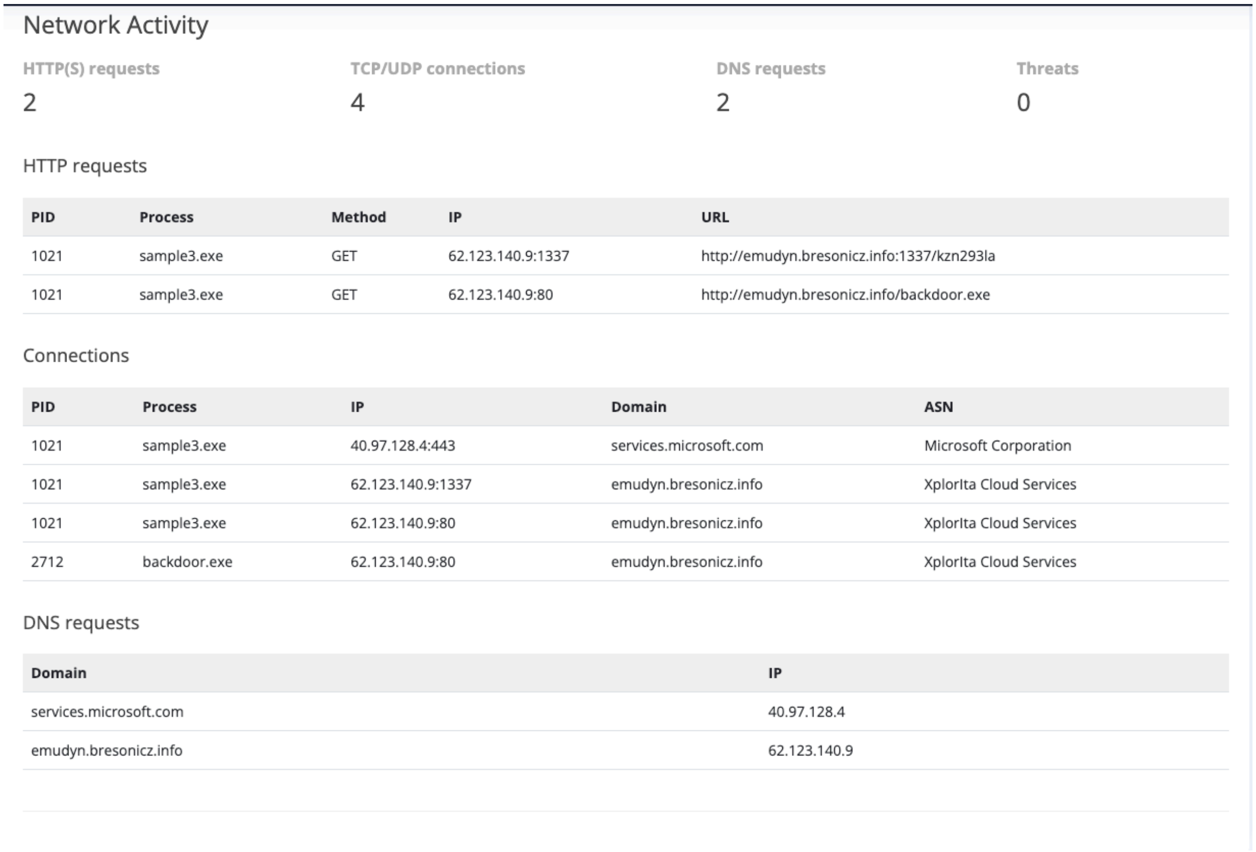
Action: Deny

egress : outgoing traffic = people leaving the network

ingress : incoming traffic = people entering the network

- In this case I used egress because systems will send a request to that IP (egress) and receive response (ingress)

Mving to the next 3rd



Network Activity

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

HTTP requests

PID	Process	Method	IP	URL
1021	sample3.exe	GET	62.123.140.9:1337	http://emudyn.bresonicz.info:1337/kzn293la
1021	sample3.exe	GET	62.123.140.9:80	http://emudyn.bresonicz.info/backdoor.exe

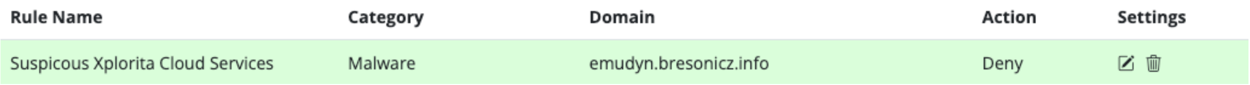
Connections

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	Xplorlta Cloud Services
1021	sample3.exe	62.123.140.9:80	emudyn.bresonicz.info	Xplorlta Cloud Services
2712	backdoor.exe	62.123.140.9:80	emudyn.bresonicz.info	Xplorlta Cloud Services

DNS requests

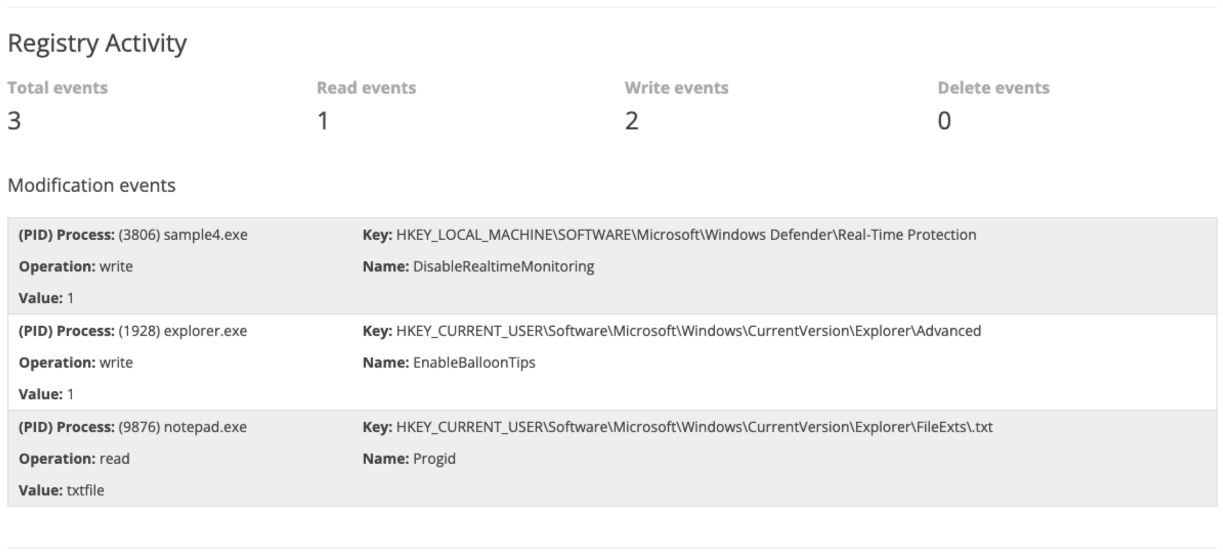
Domain	IP
services.microsoft.com	40.97.128.4
emudyn.bresonicz.info	62.123.140.9

→ After analysing I found that this malware connects to a specific domain in order to install a backdoor → Add that domain into the block list with `DNS Filter`



Rule Name	Category	Domain	Action	Settings
Suspicous Xplorita Cloud Services	Malware	emudyn.bresonicz.info	Deny	✎ 🗑

4th



Registry Activity

Total events	Read events	Write events	Delete events
3	1	2	0

Modification events

(PID) Process: (3806) sample4.exe **Operation:** write **Value:** 1	**Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection **Name:** DisableRealtimeMonitoring
(PID) Process: (1928) explorer.exe **Operation:** write **Value:** 1	**Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced **Name:** EnableBalloonTips
(PID) Process: (9876) notepad.exe **Operation:** read **Value:** txtfile	**Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt **Name:** Progid

Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection

---

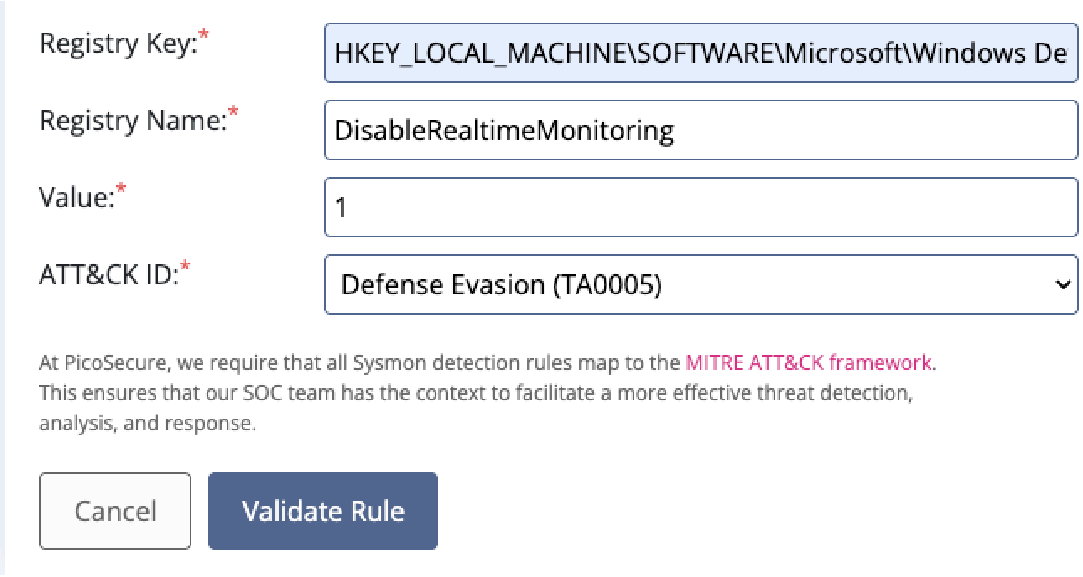
Name:

DisableRealtimeMonitoring

Looking at the PID of sample4.exe

When I have enough information, I move to `Sigma Rule Builder` tool

Sysmon Event Logs → Registry modifications



Registry Key:* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows De

Registry Name:* DisableRealtimeMonitoring

Value:* 1

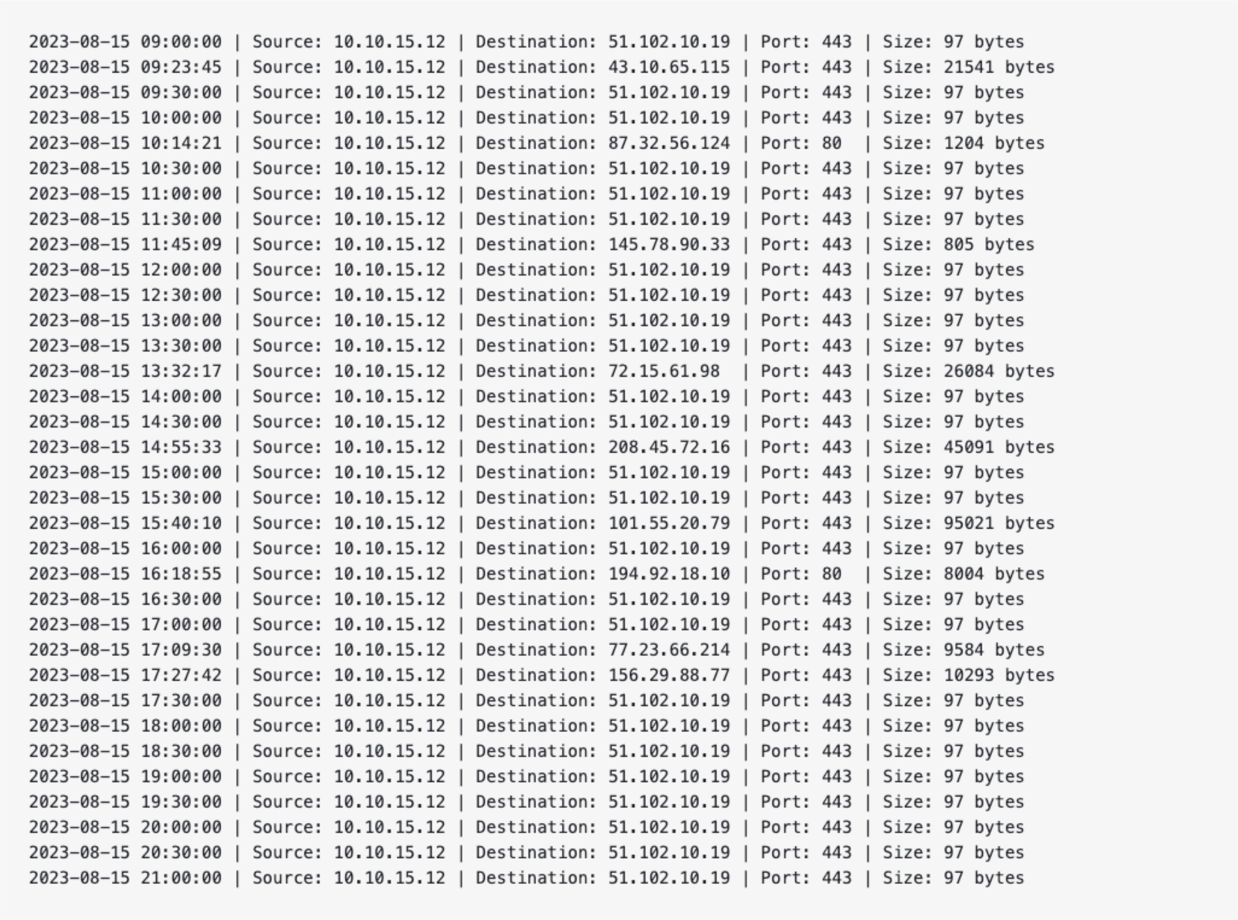
ATT&CK ID:* Defense Evasion (TA0005)

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.

5th

I viewed the log and found out that at some point the port changed from 443 → 80 (not secure).

⇒My approach is to use the firewall to block that



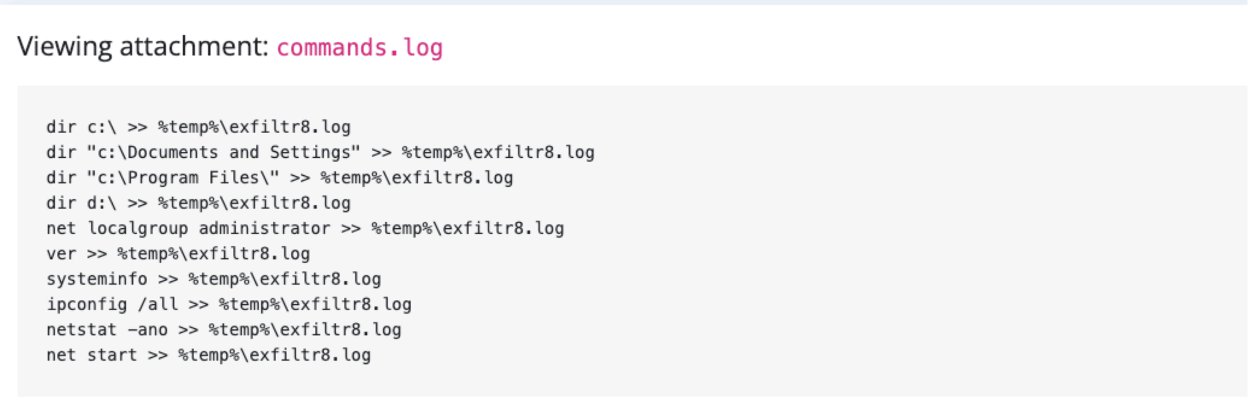
```
2023-08-15 09:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 09:23:45 | Source: 10.10.15.12 | Destination: 43.10.65.115 | Port: 443 | Size: 21541 bytes
2023-08-15 09:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
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
```

Go to Sigma tool again

`Sysmon Event Logs` → `Network Connections`

Notice that 51.102.10.19 appears more frequently than other IPs with a fixed size bytes 97

Last one



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
```

all the commands are kind of gathering information and append those infos into a file ⇒ Exfiltration