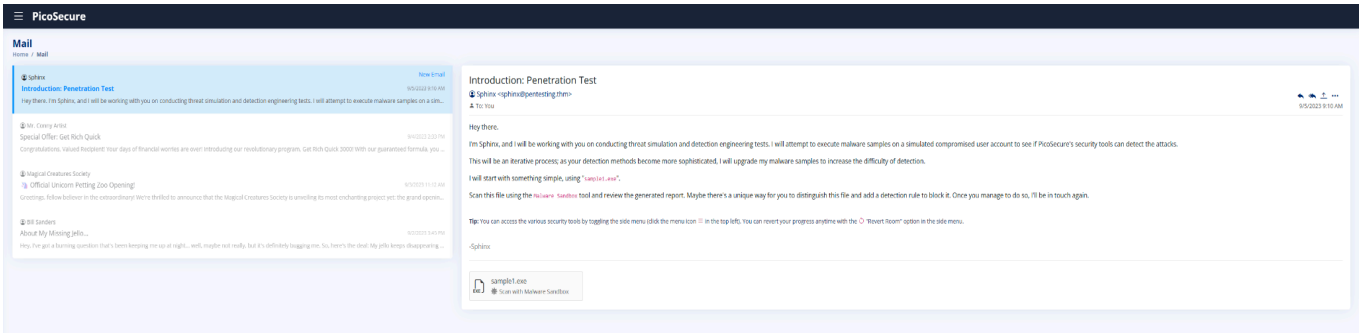
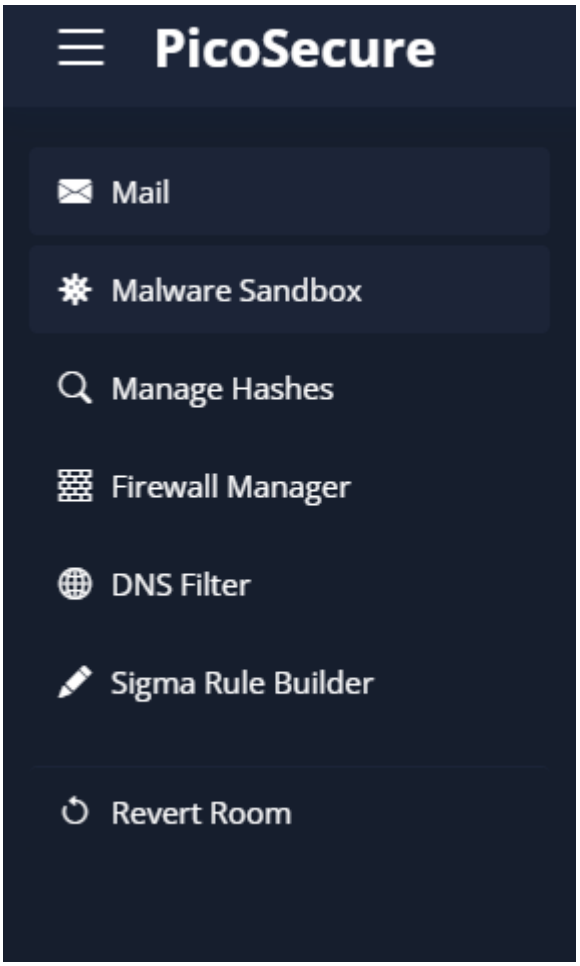
TryHackMe: Summit Write Up

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

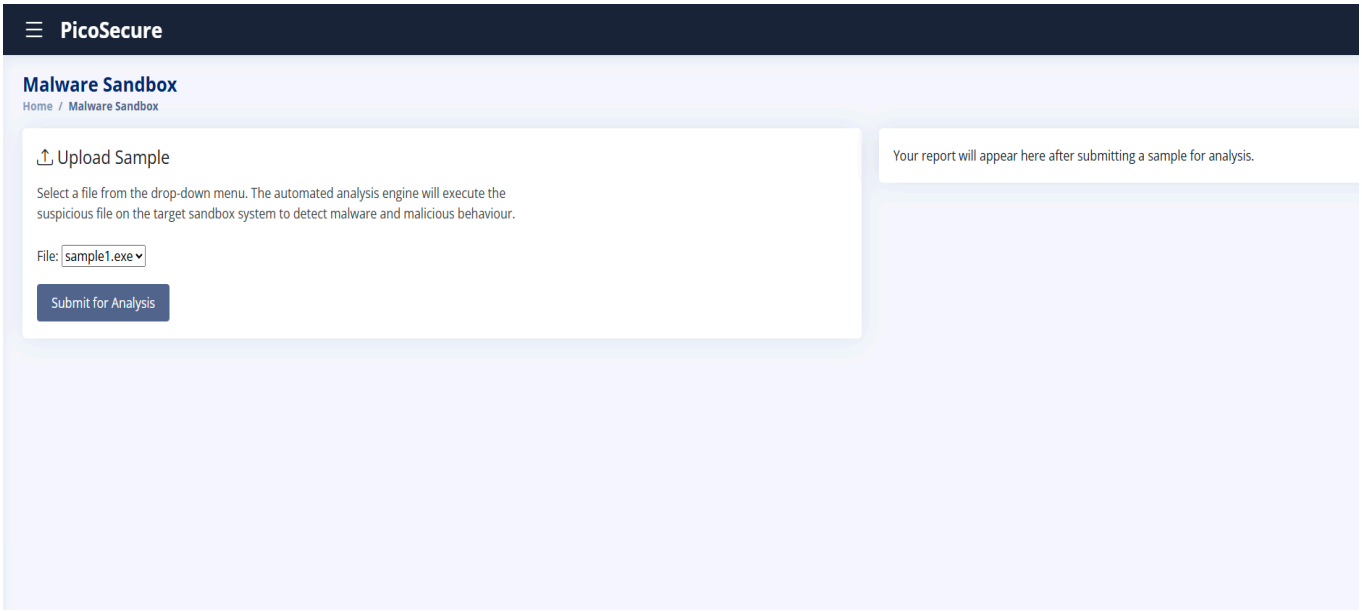
We have `sample1.exe` that we need to analyze.



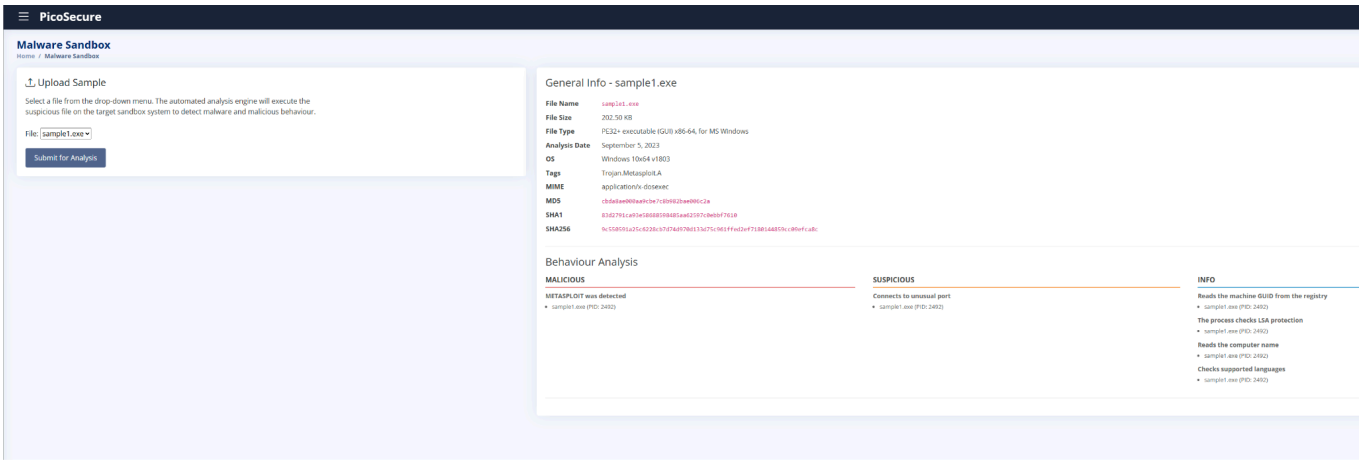
In this sandbox we have different tools, let's start with the “**Malware Sandbox**” tool.



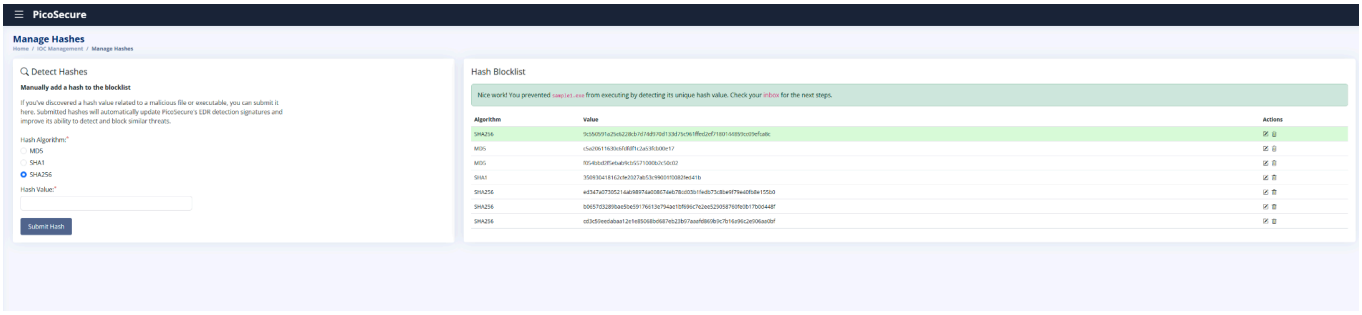
We attempt to analyze the sample1.exe file to get a report



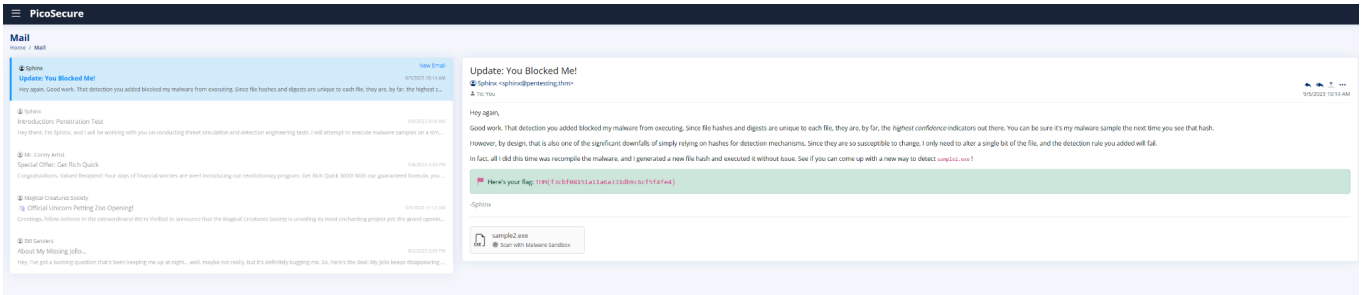
After analysis we get a report with a wealth of information and we see the different types of hashes



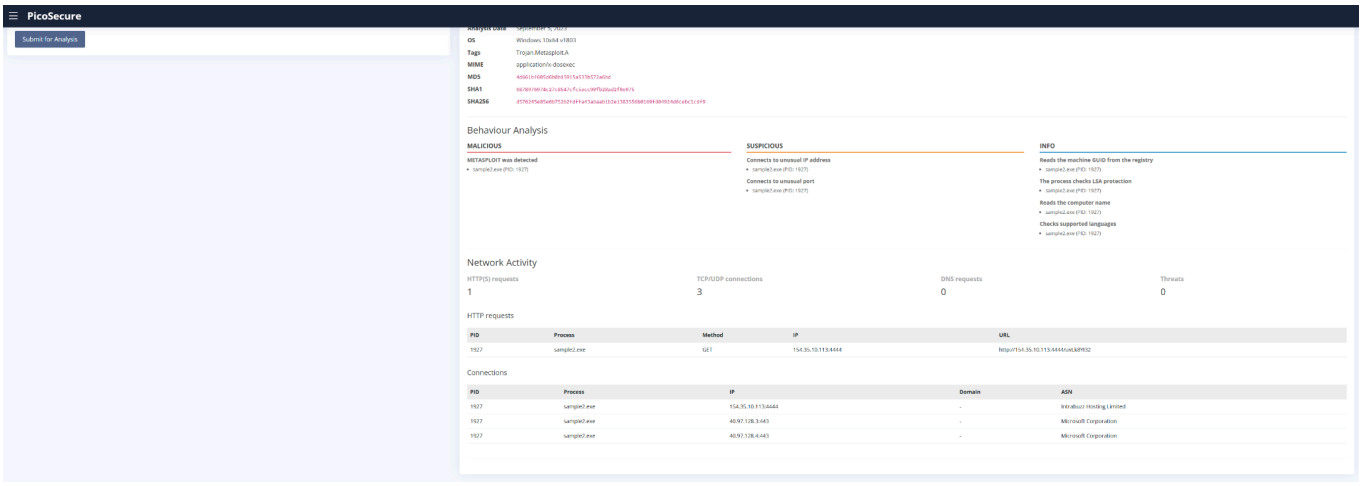
We discovered the hashes of sample1.exe, we can use these to block the malware using our EDR.



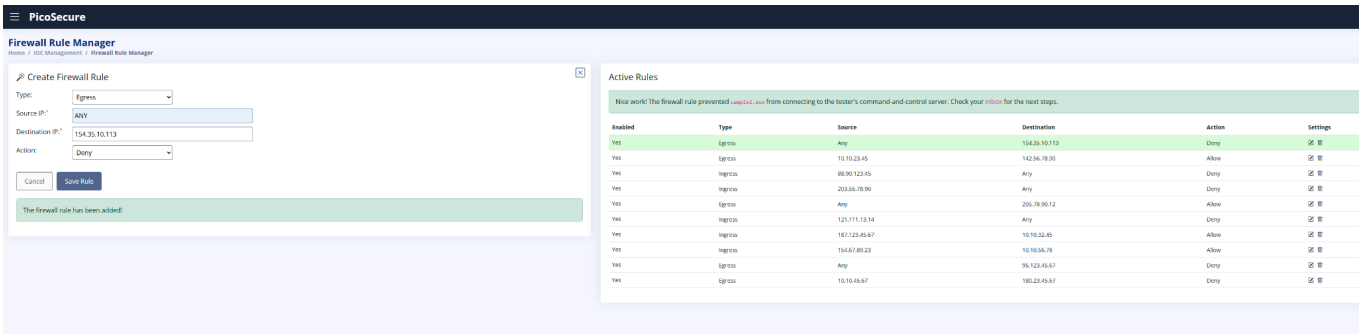
We submitted the sha256 hash to block using our EDR, and continue on to our next alert in the inbox



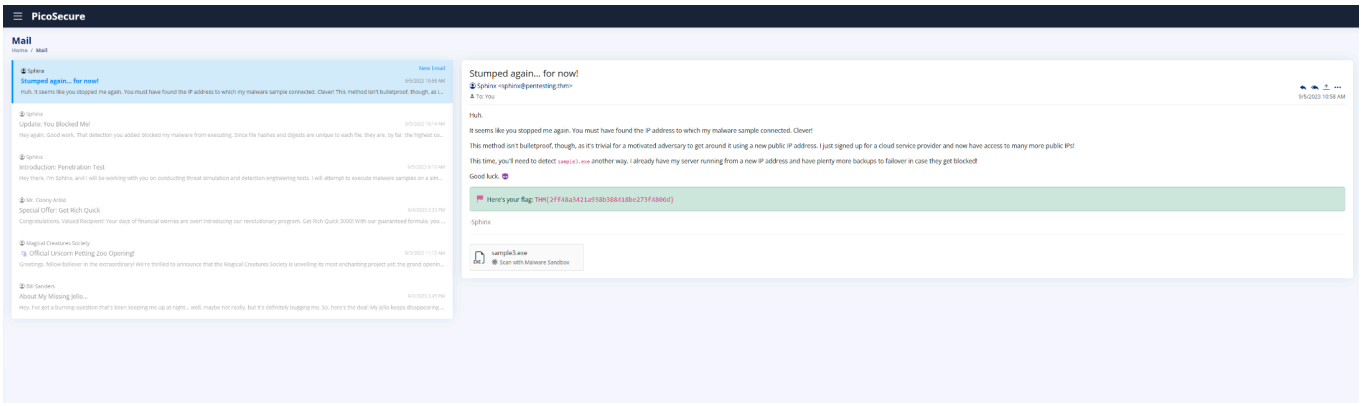
In the inbox we get sample2.exe and the flag, let analyze sample2



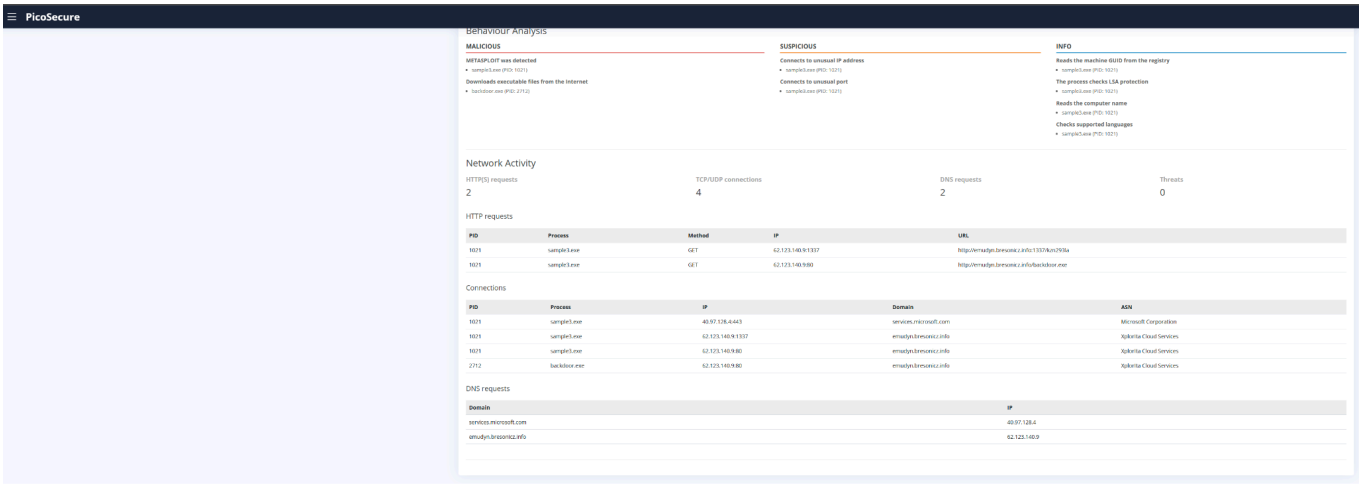
For sample2 we are getting network connections from “unusual ip” and “unusual port”. We can use a firewall to block these connections. On the HTTP request, sample2.exe attempted to get a webpage or connection from ip:port `154.35.10.113:4444`, so let’s block the ip `154.35.10.113` using our firewall.



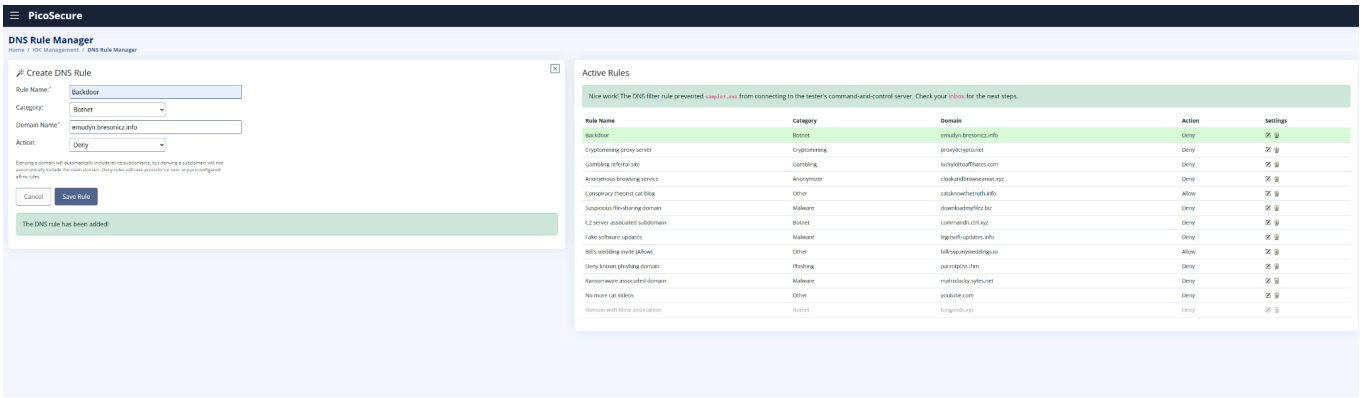
Since the malware is trying to connect externally, we setup the rule to “egress” meaning outside, the source ip to “ANY” since it could come from any of our endpoints within the network, the destination ip to `154.35.10.113` since thats the ip we got from the report communicating externally and we deny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



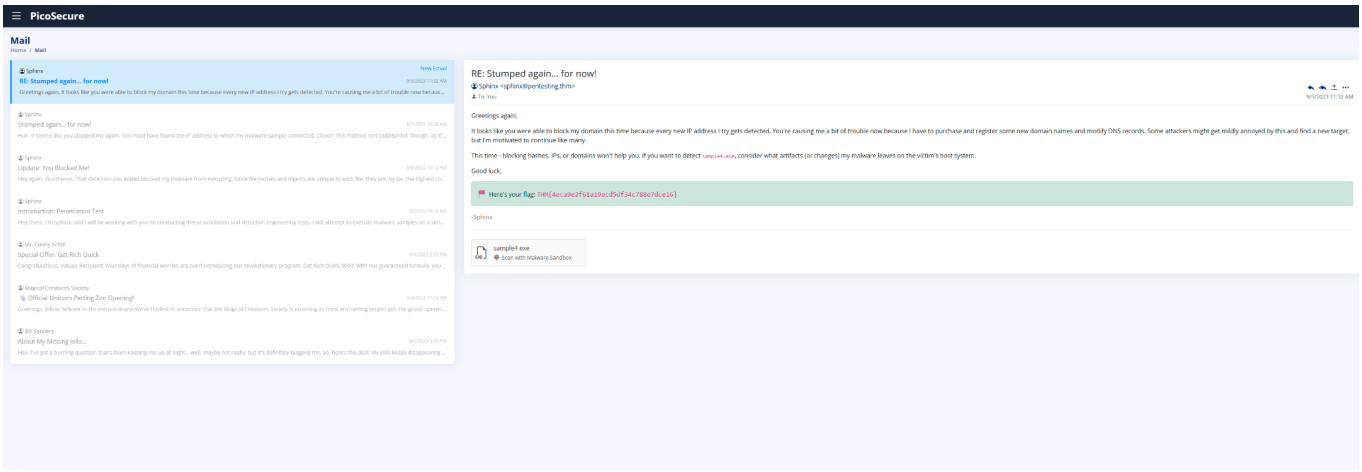
We get the flag and a new sample to dissect, lets run the malware analysis on it.



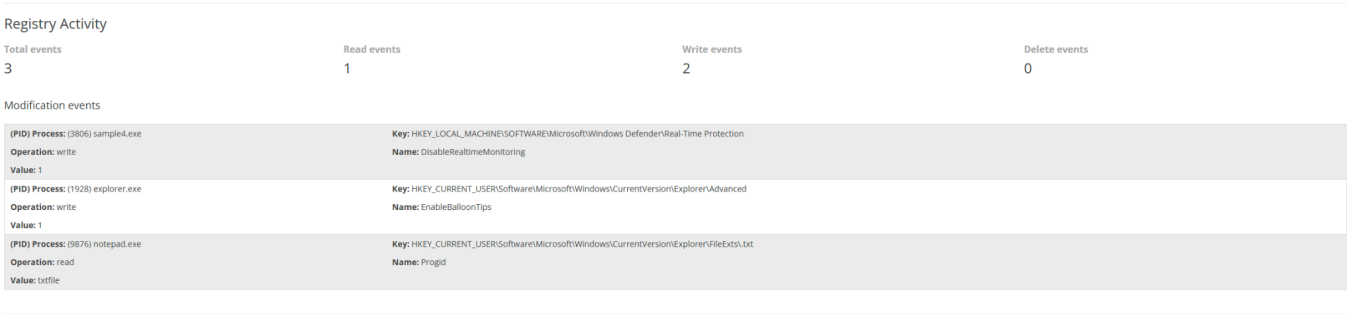
Based on the analysis for sample3, this seems to be a backdoor trying to install more tools over the internet, and is using DNS to accomplish this. We can block communications coming from `emudyn.bresonicz.info` using dns filtering.



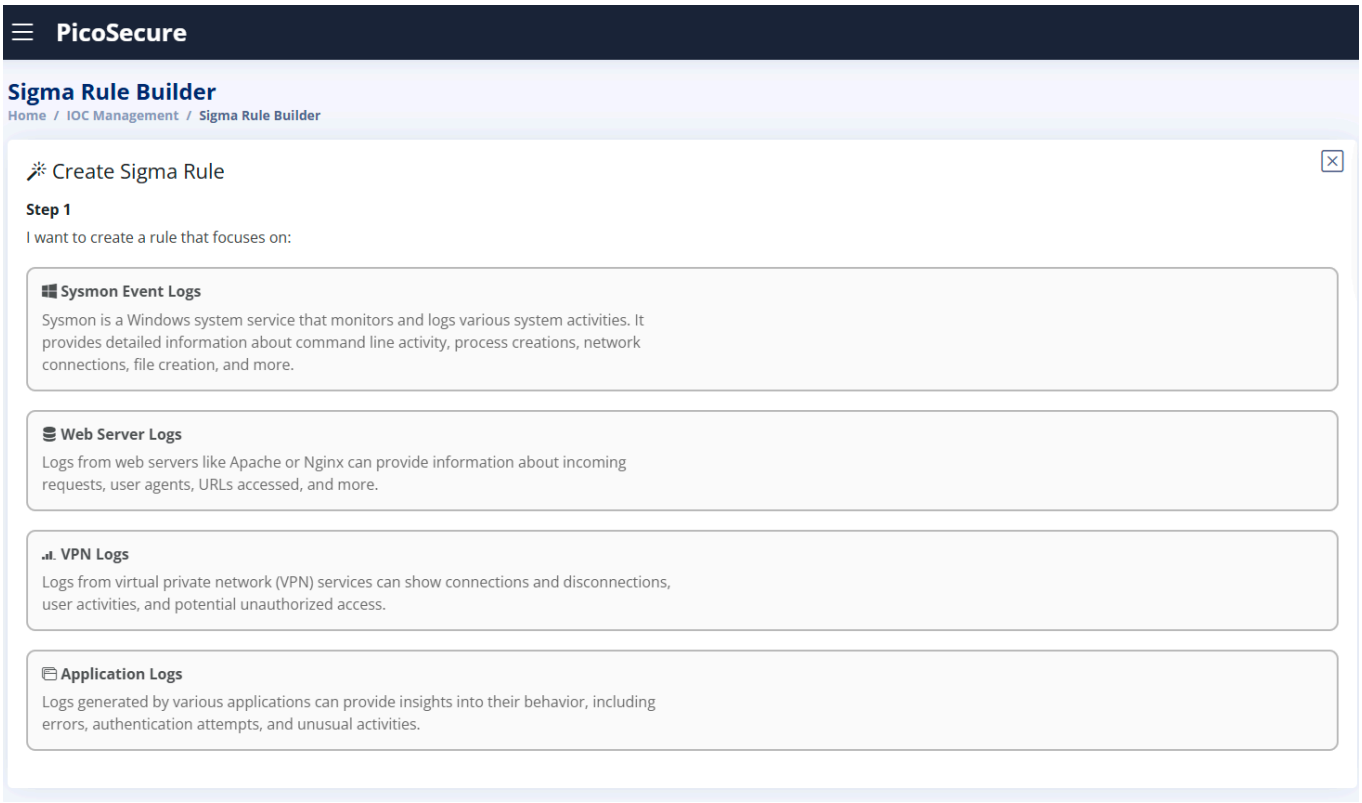
We setup a DNS rule with the name backdoor, blocking the domain above.



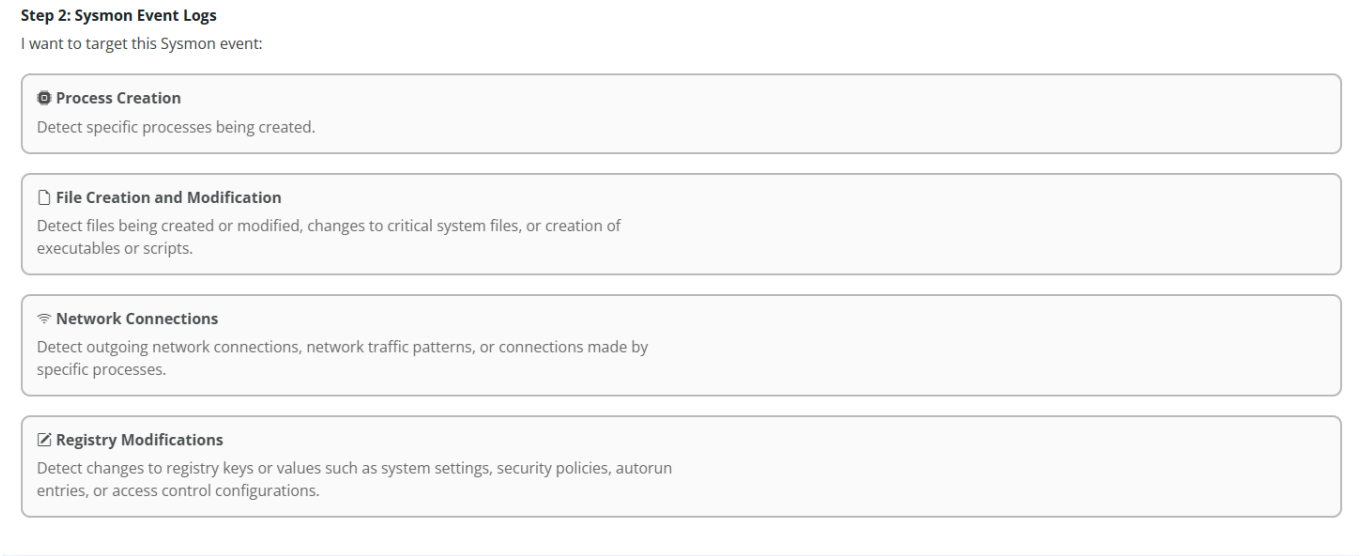
We get the flag and the next sample, sample4. Let's run some analysis on it.



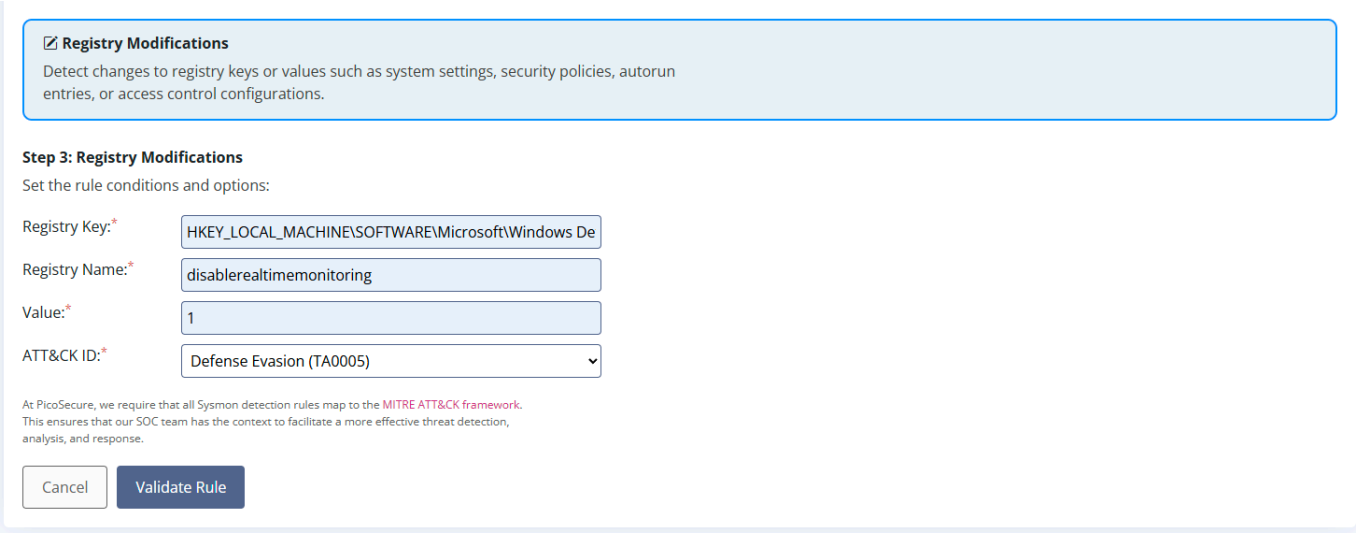
We are getting some registry activity this time. We can use the Sigma rule builder, similar to Yara rules on other systems.



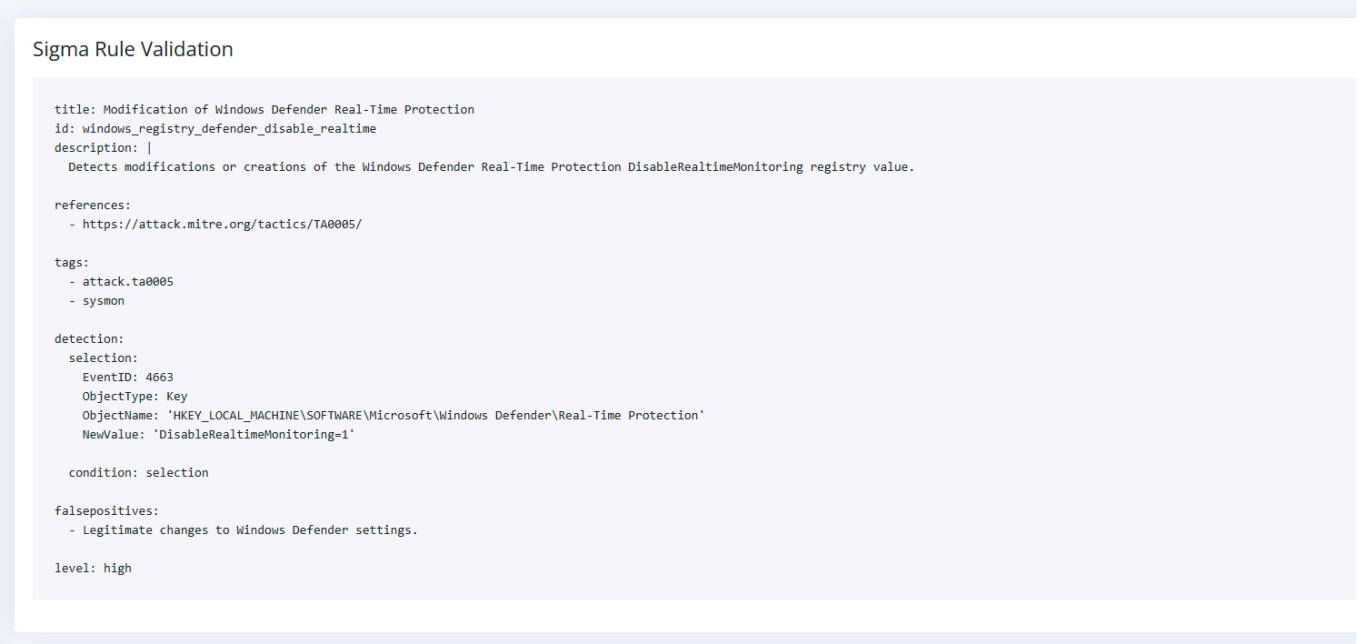
Lets select sysmon



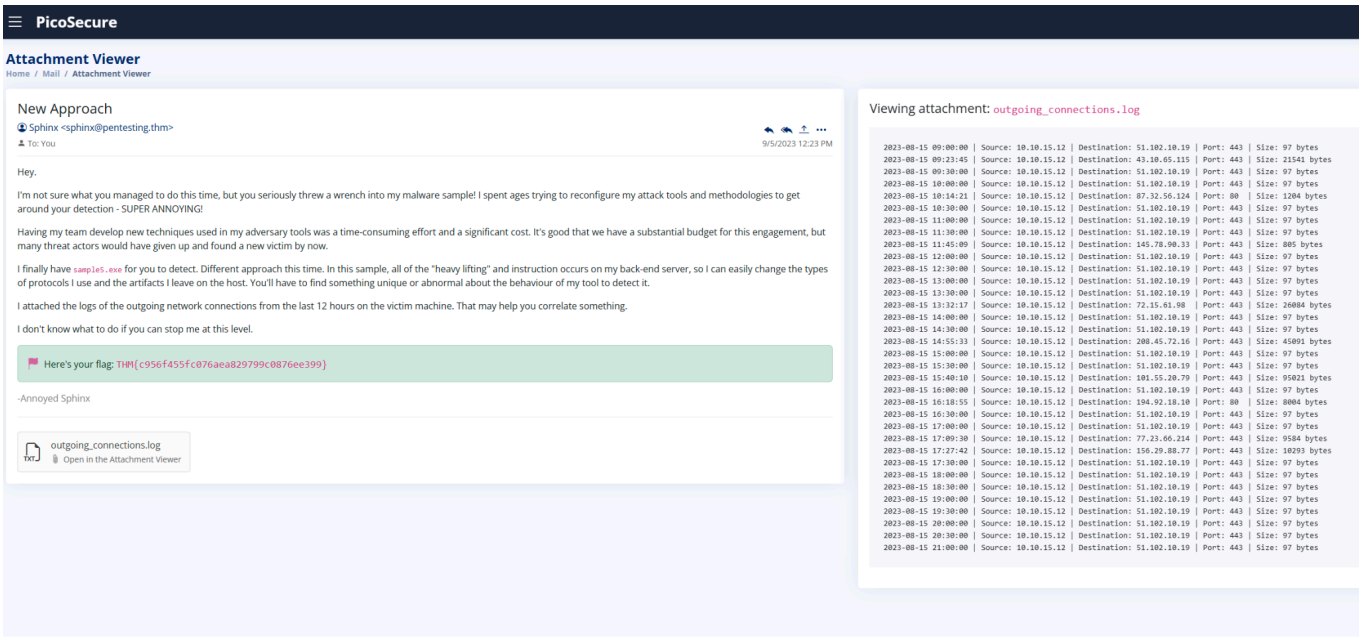
Since it is modifying the registry on windows, lets select registry modifications



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

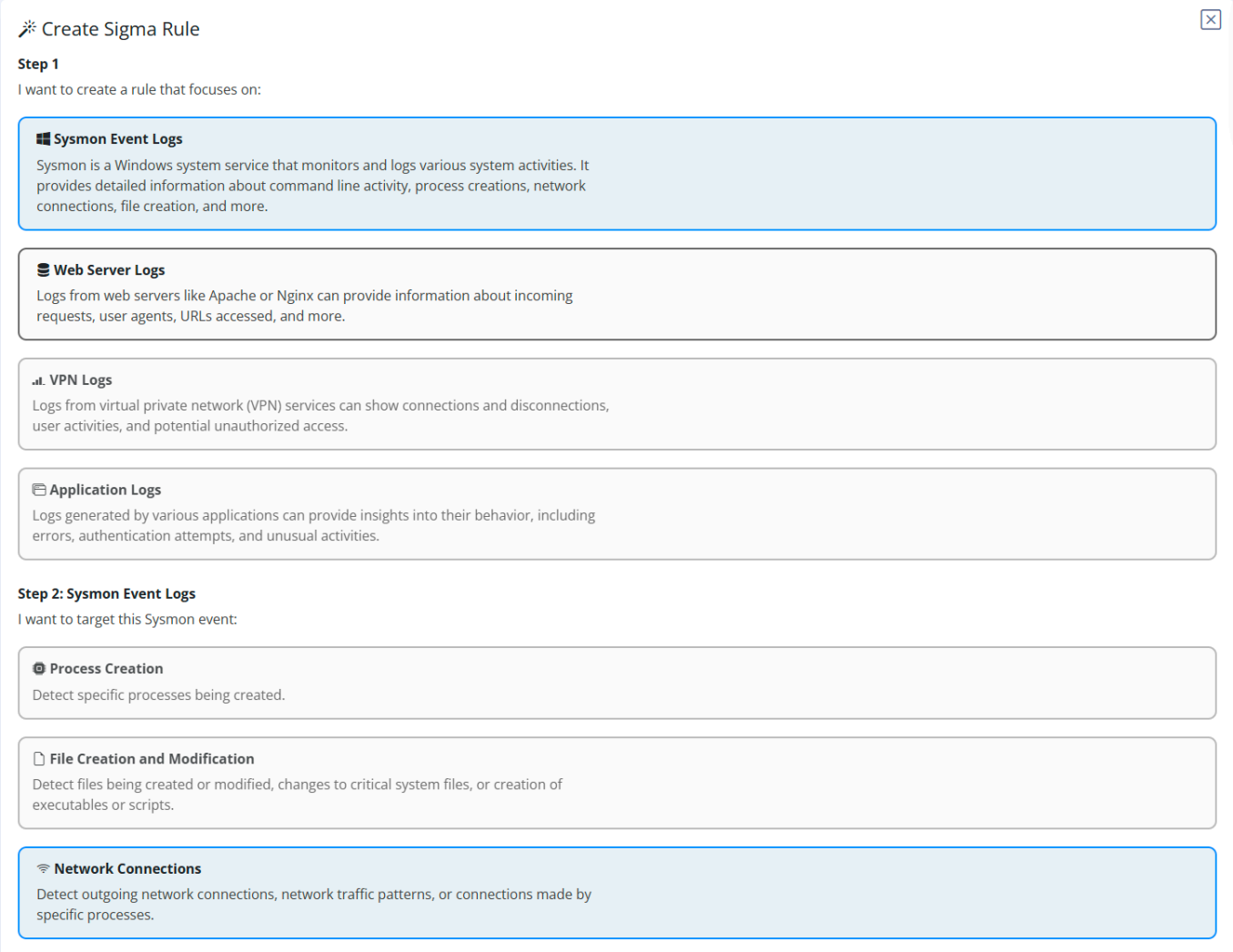


Rule is created.

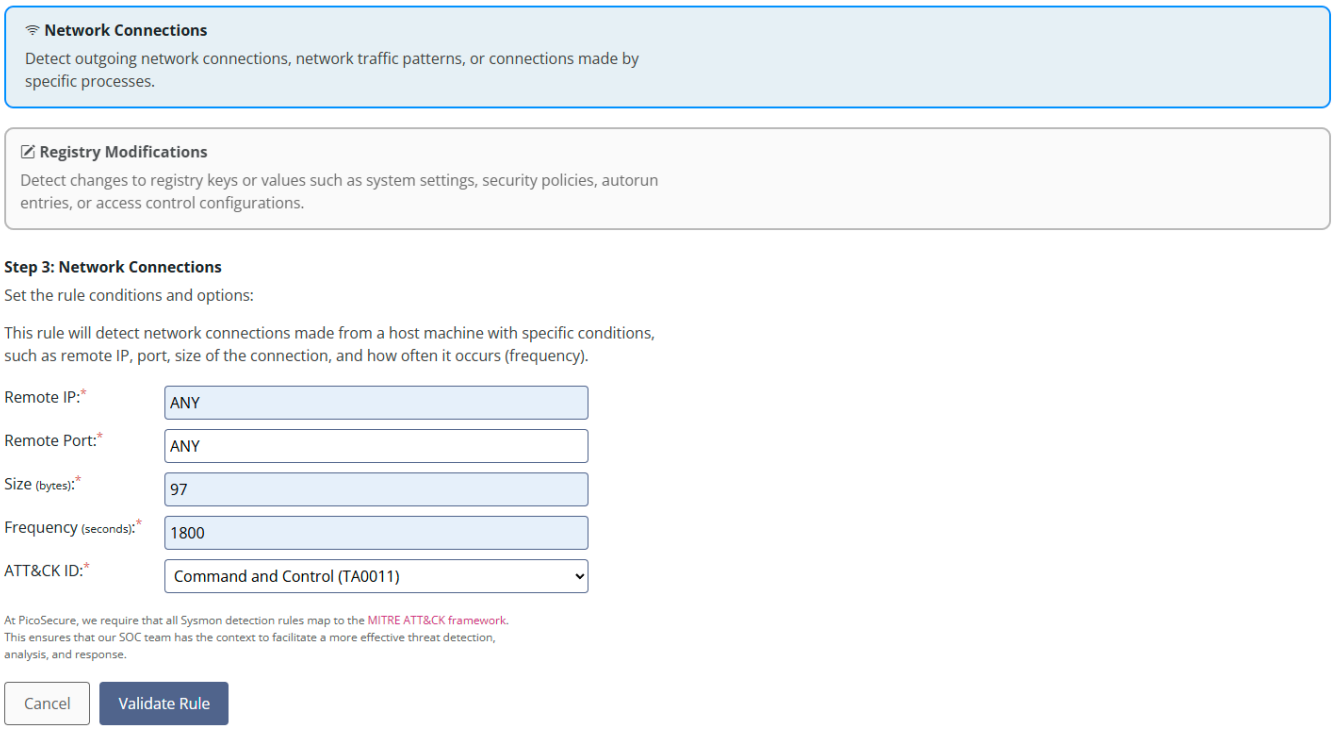


We get the flag and a new log for outgoing connections, after opening it we get a list of ips. This seems to be a C2 based on the smaller bits of communications.

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



We select sysmon then network connections

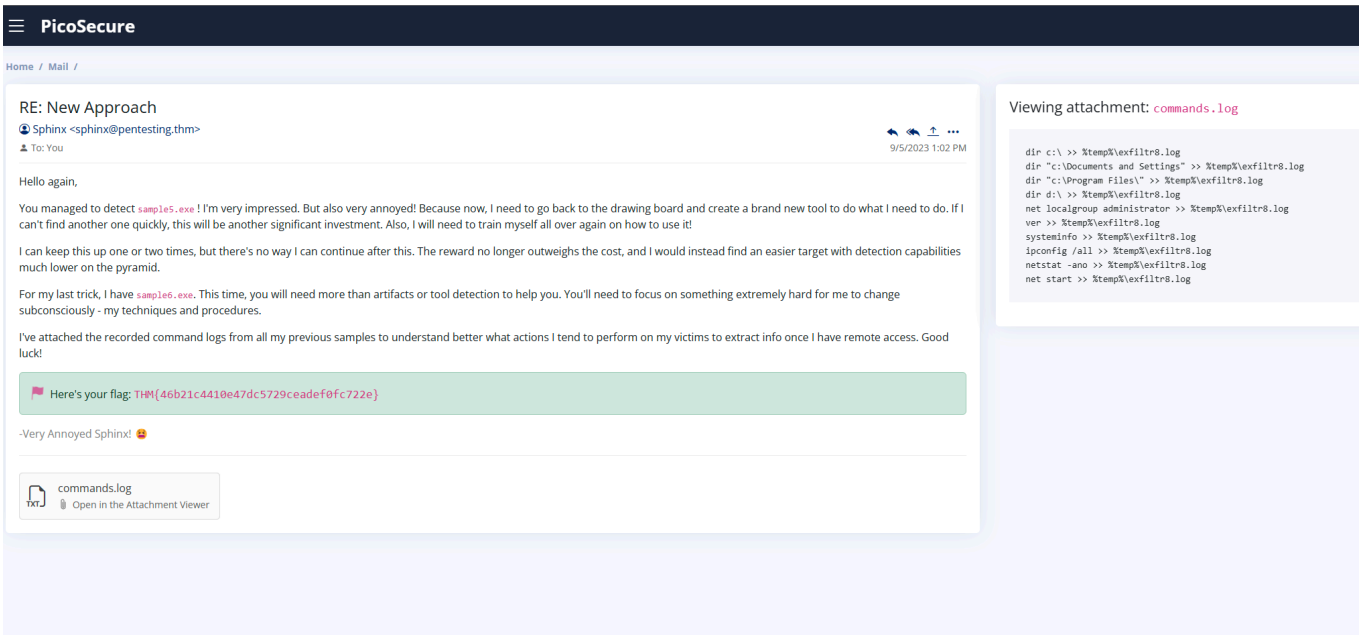


Since we know the attacker is using multiple ports and ip, we go by patterns, we see that the attacker is sending beaconing signals of 97 bits every 1800 seconds or 30 mins, just making sure the bot is alive, and this is a common c2 tactic

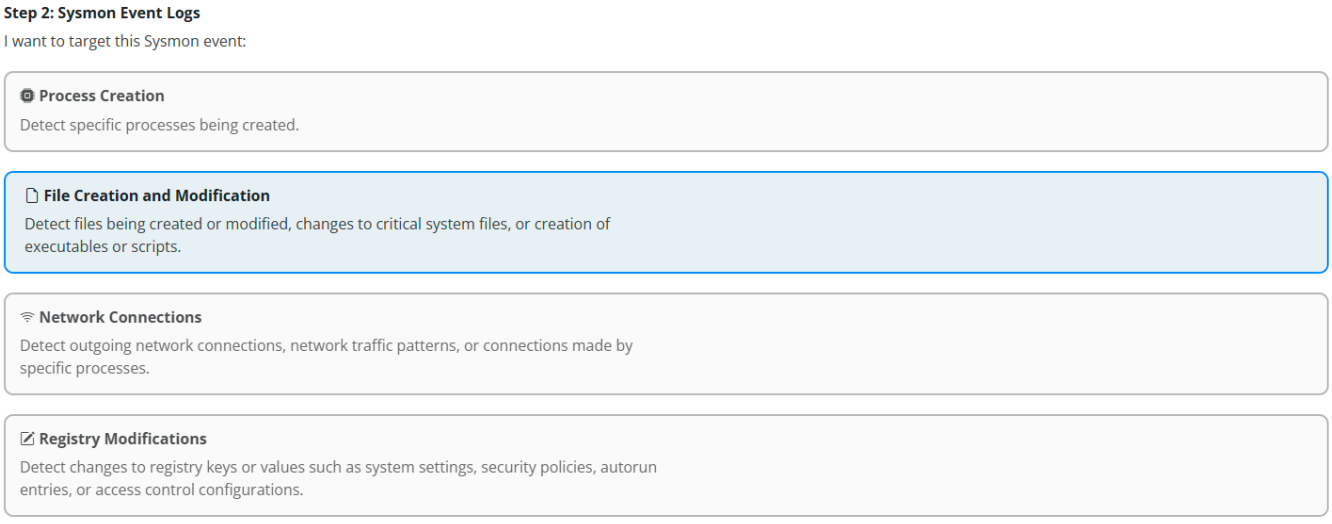
Sigma Rule Validation

```
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
```

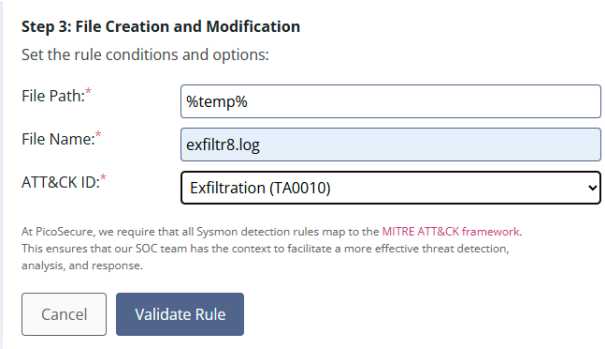
Here is the sigma rule validation



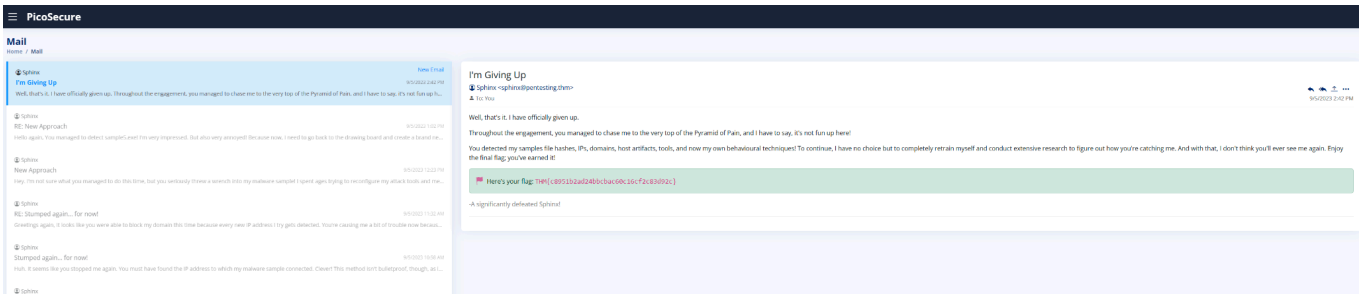
For the final tactic the attacker is getting desperate and is trying to exfiltrate all data from our endpoint into a log in the temp folder. We can block that with a sigma rule builder.



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



Fill the file path, name and type of attack from MITRE



We get the final flag.