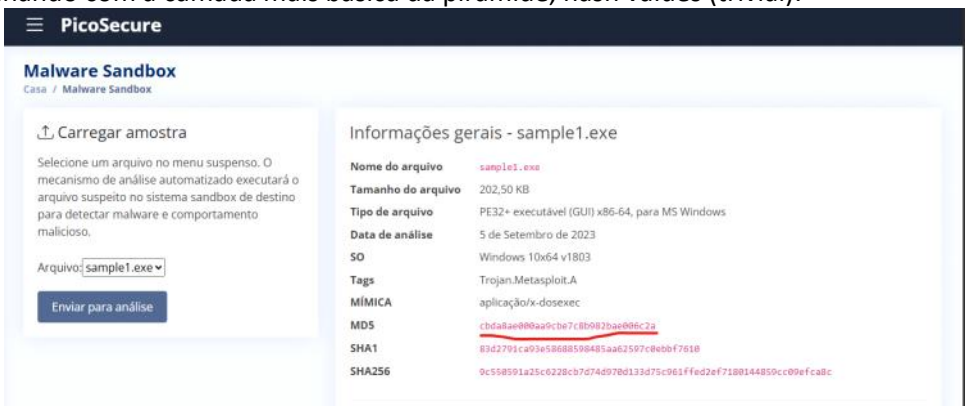
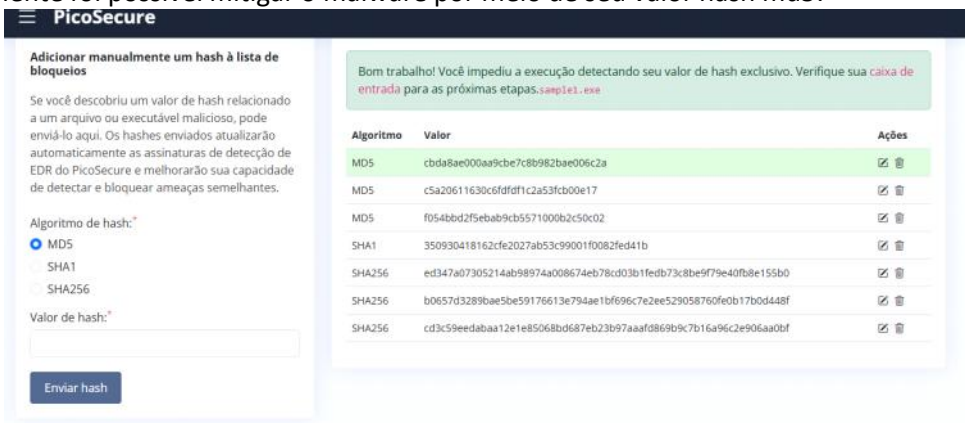
The Summit

terça-feira, 21 de outubro de 2025 22:59

- Propósito do desafio:
  - O desafio trata-se basicamente de mitigar as atividades do atacante por meio de cada camada da pirâmide da dor, a medida que se vai avançando, a maneira de mitigar vai ficando mais complexa.

- Task1:
  - No e-mail da guia, ela disse que havia uma maneira única de distinguir esse arquivo, ou seja, está se referindo ao hash que o arquivo malicioso contém, então estaremos trabalhando com a camada mais básica da pirâmide, hash values (trivial):
    - 

  - Facilmente foi possível mitigar o malware por meio de seu valor hash md5:
    - 

- Task 2:
  - Sabemos que parar uma ameaça apenas bloqueando o valor hash não é suficiente, pois basta o atacante alterar 1 único bit e terá um novo hash para aquele malware.

  - No e-mail da guia, foi alertado que o malware voltou, agora com um novo hash, então teremos que ver uma outra forma para tentar bloquear.

  - Analisando mais a fundo o malware, foi notado solicitações para um endereço ip suspeito para qual o malware estava se comunicando:

Atividade de rede

Solicitações HTTP(S)	Conexões TCP/UDP	Solicitações de DNS	Ameaças
1	3	0	0

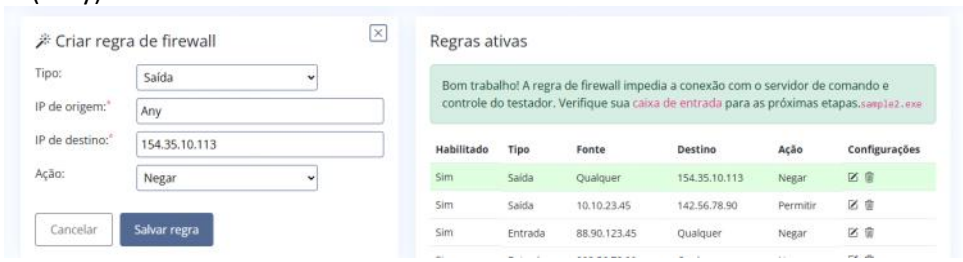
Solicitações HTTP

PID	Processo	Método	IP	URL
1927	sample2.exe	OBTER	154.35.10.113:4444	http://154.35.10.113:4444/uvLk8YI32

Conexões

PID	Processo	IP	Domínio	ASN
1927	sample2.exe	154.35.10.113:4444	-	Intrabuzz Hosting Limited
1927	sample2.exe	40.97.128.3:443	-	Corporação Microsoft
1927	sample2.exe	40.97.128.4:443	-	Corporação Microsoft

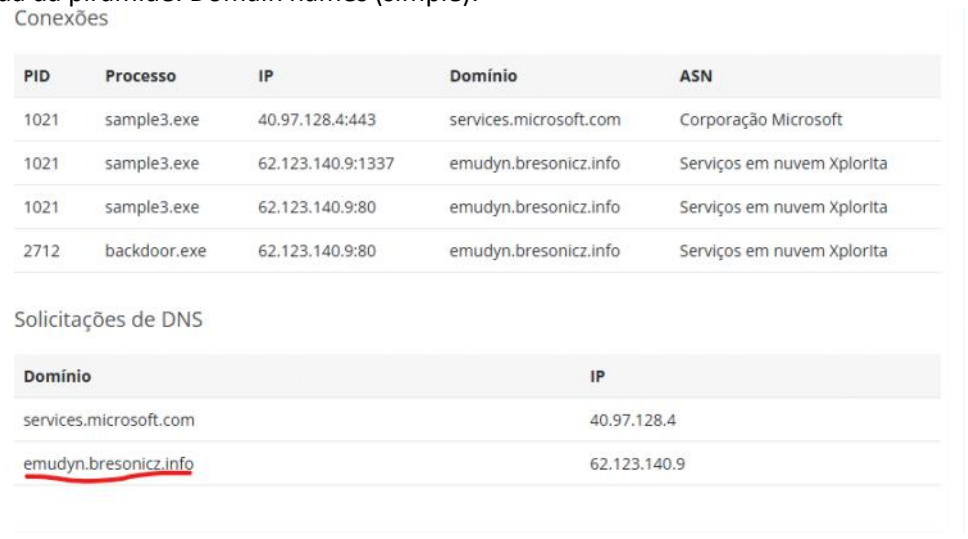
- O malware então se comunica primeiro com o ip suspeito (154.35.10.113) e depois com o ip da vítima (40.97.128.3), provavelmente algum tipo de payload deve ter sido pego desse ip suspeito, então, para tentar parar isso, podemos bloquear o ip na qual o malware se comunica, ou seja, estamos lidando com a próxima camada da pirâmide: ip address (easy):



- Assim, bloqueamos que qualquer processo ou host da nossa rede se comunique com esse ip.

- Task 3:
  - Mas como sabemos, bloquear um endereço ip não resolve, pois isso também pode ser fácil para o atacante alterar e reestabelecer comunicação com o malware.

  - Então se mesmo bloquear o ip não resolve, teremos que focar naquilo que seria a raíz do funcionamento dos Ips, que seria o domínio, nesse caso, estaremos focando na próxima camada da pirâmide: Domain names (simple):

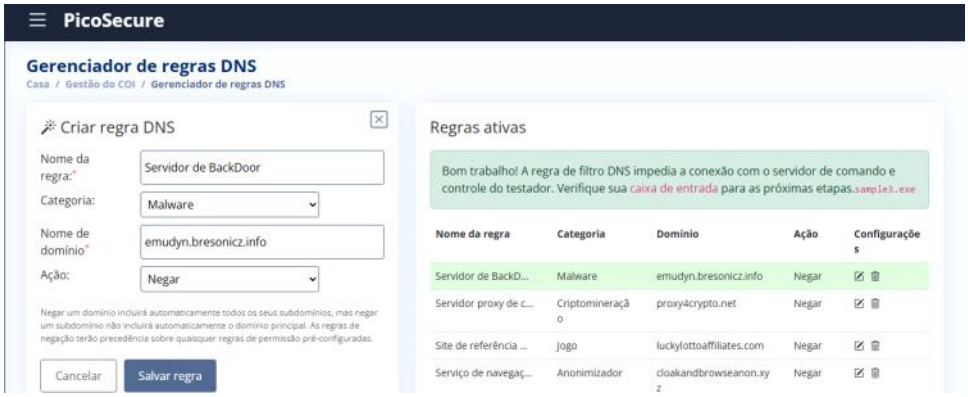


Conexões

PID	Processo	IP	Domínio	ASN
1021	sample3.exe	40.97.128.4:443	services.microsoft.com	Corporação Microsoft
1021	sample3.exe	62.123.140.9:1337	emudyn.bresonicz.info	Serviços em nuvem Xplorita
1021	sample3.exe	62.123.140.9:80	emudyn.bresonicz.info	Serviços em nuvem Xplorita
2712	backdoor.exe	62.123.140.9:80	emudyn.bresonicz.info	Serviços em nuvem Xplorita

Solicitações de DNS

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



- Assim, conseguimos bloquear todo o domínio do atacante, então mesmo que ele altere o endereço ip, não poderá se comunicar devido ao domínio inativo.

- Task 4:
  - Apesar de que pode ser um pouco mais trabalhoso para o atacante alterar, fica fácil para o atacante retornar com um novo domínio e todo problema recomeçar, então, teremos que focar em algo mais sólido, que pode começar a dar uma verdadeira dor de cabeça ao atacante, os hosts artifacts(annoying) - Artefatos observáveis que o atacante deixa no sistema:

    - Na imagem de análise de eventos de modificação, nota-se que o registro da pasta KEY_LOCAL_MACHINE sofreu alguma modificação de escrita, na qual foi para desativar o monitoramento em tempo real, ou seja, fazendo isso, permite que o atacante desative a capacidade do sistema em detectar hashes, ips e domínios maliciosos, mesmo registrados como tal, então para isso, devemos bloquear esse tipo de modificação do nosso dispositivo:

Validação de regra Sigma

```
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 regis

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
```

- Com isso, bloqueamos o artefato de host, retornando ao funcionamento normal do sistema de defesa em detectar recursos maliciosos.

- Task 5:
  - Se afetar um artefato de host daria muita dor de cabeça para o atacante, atingir o artefato de rede afetará mais ainda, pois se o analista conseguir bloquear os artefatos de rede, será muito mais difícil para o atacante reestruturar o ataque, mesmo modificando os artefatos de host, e por isso, dessa vez, focaremos na antepenúltima camada da pirâmide da dor: network artifact(annoying):

HTTP requests

PID	Process	Method	IP	URL
8374	sample5.exe	GET	51.102.10.19:1382	http://bababa10la.cn:1382/zz89j3uf
8374	sample5.exe	GET	51.102.10.19:443	https://bababa10la.cn/beacon.bat
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beacon.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
-	Too many results to display	-	-	-

Connections

PID	Process	IP	Domain	ASN
8374	sample5.exe	51.102.10.19:1382	bababa10la.cn	Xplorita Cloud Services
8374	sample5.exe	51.102.10.19:80	bababa10la.cn	Xplorita Cloud Services
1702	beacon.bat	51.102.10.19:443	bababa10la.cn	Xplorita Cloud Services

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
```

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:*	Any
Remote Port:*	Any
Size (bytes):*	97
Frequency (seconds):*	1800
ATT&CK ID:*	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

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
```

- O que foi feito foi um bloqueio de artefato de rede, bloqueamos o comportamento de tráfego que fazia comando & controle com 97 bytes, então mesmo que o atacante altere ip, domínio ou artefato de host, ele terá que pensar em uma forma de alterar o comportamento do artefato de rede, o que com certeza será bastante trabalhoso.

- Task 6:
  - Se apesar de todas essas camadas o atacante ainda perserverar (o que merece um salva de palmas porque esse cara é muito bom) ainda haverá uma última coisa para se mitigar, o funcionamento da sua ferramenta, onde ai, afetarmos a penúltima camada da pirâmidade da dor: Tools(challenging):

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
4	0	1	0

Process information

PID	CMD	Path	Parent
8374	sample6.exe	C:\Users\admin\AppData\Local\Temp\sample6.exe	explorer.exe
3992	cmd.exe	C:\Windows\system32\cmd.exe	sample6.exe
1432	cmd.exe	C:\Windows\system32\cmd.exe	sample6.exe
2312	cmd.exe	C:\Windows\system32\cmd.exe	sample6.exe

Files Activity

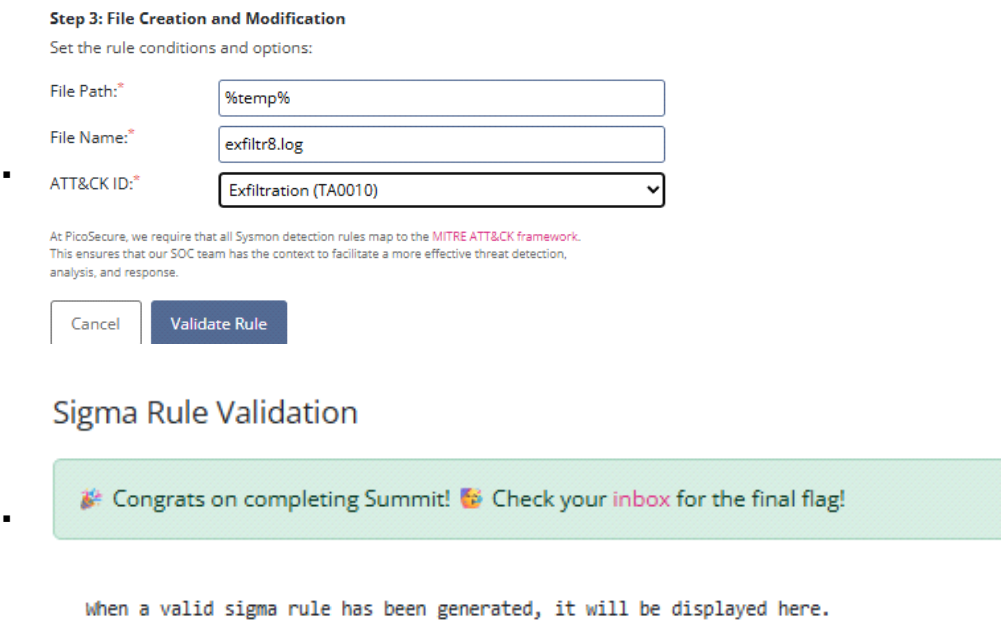
Executable files	Suspicious files	Text files	Unknown types
0	1	1	0

Dropped files

PID	Process	Filename	Type
2312	cmd.exe	%temp%\exfiltr8.log	text

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
```



- Por meio do relatório gerado pela ferramenta, vimos que o malware estava usando variáveis temporárias do sistema operacional para fazer exfiltração de informações do sistema, provavelmente para ter mais conhecimento do seu local de ataque, felizmente isso foi mitigado, e agora, como ele não tem mais acesso a variáveis temporárias para se safar da exfiltração, está com muita dificuldade sob o que fará para conseguir tais informações, podemos dar isso como um xeque-mate para as atividades desse atacante.

- Observação: A última camada - TTP(Tough!) já é dada como mitigada por conta das outras mitigações feitas.