

# 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):

The screenshot shows the PicoSecure Malware Sandbox interface. On the left, there's a 'Carregar amostra' (Load sample) section with a file input field containing 'sample1.exe' and a 'Enviar para análise' (Send for analysis) button. On the right, the 'Informações gerais - sample1.exe' (General information - sample1.exe) section displays the following details:

Nome do arquivo	sample1.exe
Tamanho do arquivo	202,50 KB
Tipo de arquivo	PE32+ executável (GUI) x86-64, para MS Windows
Data de análise	5 de Setembro de 2023
SO	Windows 10x64 v1803
Tags	Trojan.Metasploit.A
MÍMICA	aplicação/x-dosexec
MD5	cbda8ae00aa9cbe7c8b982bae006c2a
SHA1	83d2701ca03e58688598485aa62597c9ebbf7618
SHA256	9c558991a25c6228cb7d74d970d133d75c961ffed2ef7180144850cc09efca8c

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

The screenshot shows the PicoSecure interface with the 'Adicionar manualmente um hash à lista de bloqueios' (Add manually a hash to the list of blockades) section active. It includes a text box for 'Algoritmo de hash:' with 'MD5' selected, and a 'Valor de hash:' input field. A 'Enviar hash' (Send hash) button is at the bottom. On the right, a table displays the list of hashes added to the blockades:

Algoritmo	Valor	Ações
MD5	cbda8ae00aa9cbe7c8b982bae006c2a	✕ 🗑
MD5	c5a20611630c6fdd1c2a53fcb00e17	✕ 🗑
MD5	f054bbd2f5ebab9cb5571009b2c50c02	✕ 🗑
SHA1	350930418162cfe2027ab53c99001f0082fed41b	✕ 🗑
SHA256	ed347a07305214ab98974a008674eb78cd03b1fedb73c8be9f79e40fb8e155b0	✕ 🗑
SHA256	b0657d3289bae5be59176613e794ae1bf696c7e2ee529058760fe0b17bod448f	✕ 🗑
SHA256	cd3c59eedabaa12e1e85068bd687eb23b97aaafd869b9c7b16a96c2e906aa0bf	✕ 🗑

- 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)

1

Conexões TCP/UDP

3

Solicitações de DNS

0

Ameaças

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):

⚙️ Criar regra de firewall

Tipo:

IP de origem:

IP de destino:

Ação:

Regras ativas

Bom trabalho! A regra de firewall impediu a conexão com o servidor de comando e controle do testador. Verifique sua caixa de entrada para as próximas etapas. sample2.exe

Habilitado	Tipo	Fonte	Destino	Ação	Configurações
Sim	Saída	Qualquer	154.35.10.113	Negar	<input checked="" type="checkbox"/> <input type="checkbox"/>
Sim	Saída	10.10.23.45	142.56.78.90	Permitir	<input checked="" type="checkbox"/> <input type="checkbox"/>
Sim	Entrada	88.90.123.45	Qualquer	Negar	<input checked="" type="checkbox"/> <input type="checkbox"/>

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

### • Task 3:

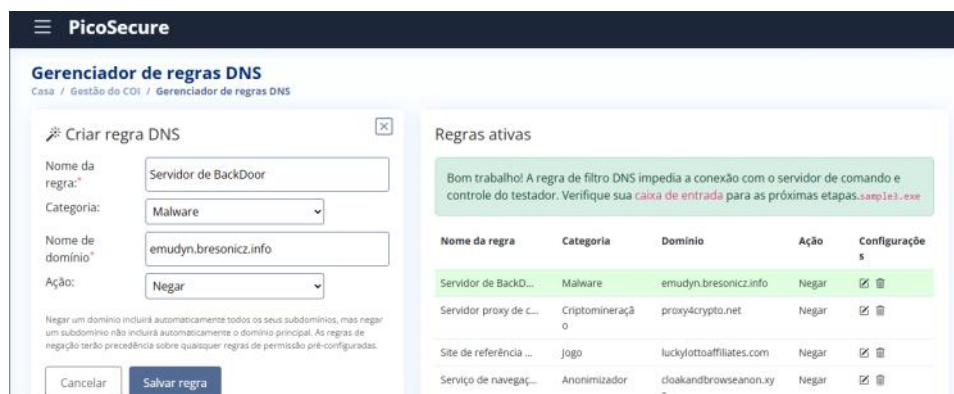
- Mas como sabemos, bloquear um endereço ip não resolve, pois isso também pode ser fácil para o atacante alterar e reestabelecer comunicação com o malware.
- Então se mesmo bloquear o ip não resolve, teremos que focar naquilo que seria a raiz do funcionamento dos Ips, que seria o domínio, nesse caso, 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
<u>emudyn.bresonicz.info</u>	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:

#### Eventos de modificação

<b>(PID) Processo:</b> (3806) sample4.exe	<b>Chave:</b> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Proteção em tempo real
<b>Operação:</b> escrever	<b>Nome:</b> DesativarMonitoramento em tempo real
<b>Valor:</b> 1	

- 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:

### Etapa 3: Modificações no registro

Defina as condições e opções da regra:

Chave do Registro:*	HKEY_LOCAL_MACHINE\SOFTWARE\Micr
Nome do Registro:*	DisableRealtimeMonitoring
Valor:*	1
ID ATT&CK:*	Evasão de Defesa (TA0005) ▼

No PicoSecure, exigimos que todas as regras de detecção do Sysmon sejam mapeadas para a **estrutura MITRE ATT&CK**. Isso garante que nossa equipe de SOC tenha o contexto para facilitar uma detecção, análise e resposta a ameaças mais eficazes.

Cancelar	Regra de validação
----------	--------------------

Validação de regra Sigma

## 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/beaton.bat
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.bat	POST	51.102.10.19:443	https://bababa10la.cn/keep-alive?hostname=WK102
1702	beaton.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	beaton.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:*	<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

## 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 pirâmide 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

```

### Step 3: File Creation and Modification

Set the rule conditions and options:

File Path:*	<input type="text" value="%temp%"/>
File Name:*	<input type="text" value="exfiltr8.log"/>
ATT&CK ID:*	<input type="text" value="Exfiltration (TA0010)"/>

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.

<input type="button" value="Cancel"/>	<input type="button" value="Validate Rule"/>
---------------------------------------	--

## Sigma Rule Validation

🎉 Congrats on completing Summit! 🎉 Check your **inbox** for the final flag!

When a valid sigma rule has been generated, it will be displayed here.

- 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.