Summit Challenge

Andres Valdivieso Pinilla - Líder de Ciberseguridad (Consultor)
www.linkedin.com/in/andres-valdivieso-pinilla

Introducción

En el contexto de la ciberseguridad, la detección y respuesta a incidentes son fundamentales para mitigar amenazas en entornos empresariales. Tras múltiples experiencias en respuesta a incidentes, debemos fortalecer nuestras capacidades mediante simulaciones de amenazas para ampliar nuestro conocimiento en la detección.

Por lo que para este modulo nos presentan un desafío que se desarrolla en un escenario de equipo púrpura, donde un evaluador de penetración externo intentará ejecutar muestras de malware en una estación de trabajo simulada. Como defensor, la tarea consiste en configurar herramientas de seguridad para detectar y bloquear estas amenazas, siguiendo el enfoque progresivo de la **Pirámide del Dolor**. El objetivo es incrementar el costo operativo del adversario, dificultando sus tácticas y reforzando la resiliencia del entorno.

Para abordar este reto de manera efectiva, se recomienda familiarizarse con los marcos de ciberdefensa relevantes, incluyendo **MITRE ATT&CK** y la **Pirámide del Dolor**, disponibles en TryHackMe.

El Desafío

*Objetivo

Después de participar en demasiadas actividades de respuesta a incidentes, PicoSecure decidió realizar una simulación de amenazas y un proyecto de ingeniería de detección para reforzar sus capacidades de detección de malware. Se le ha asignado trabajar con un evaluador de penetración externo en un escenario iterativo de equipo púrpura. El evaluador intentará ejecutar muestras de malware en una estación de trabajo simulada de un usuario interno. Al mismo tiempo, deberá

configurar las herramientas de seguridad de PicoSecure para detectar y evitar que se ejecute el malware.

Siguiendo la prioridad ascendente de los indicadores de la **Pirámide del Dolor** , tu objetivo es aumentar el coste de las operaciones de los adversarios simulados y ahuyentarlos para siempre. Cada nivel de la pirámide te permite detectar y prevenir varios indicadores de ataque.

**Detalles de la conexión

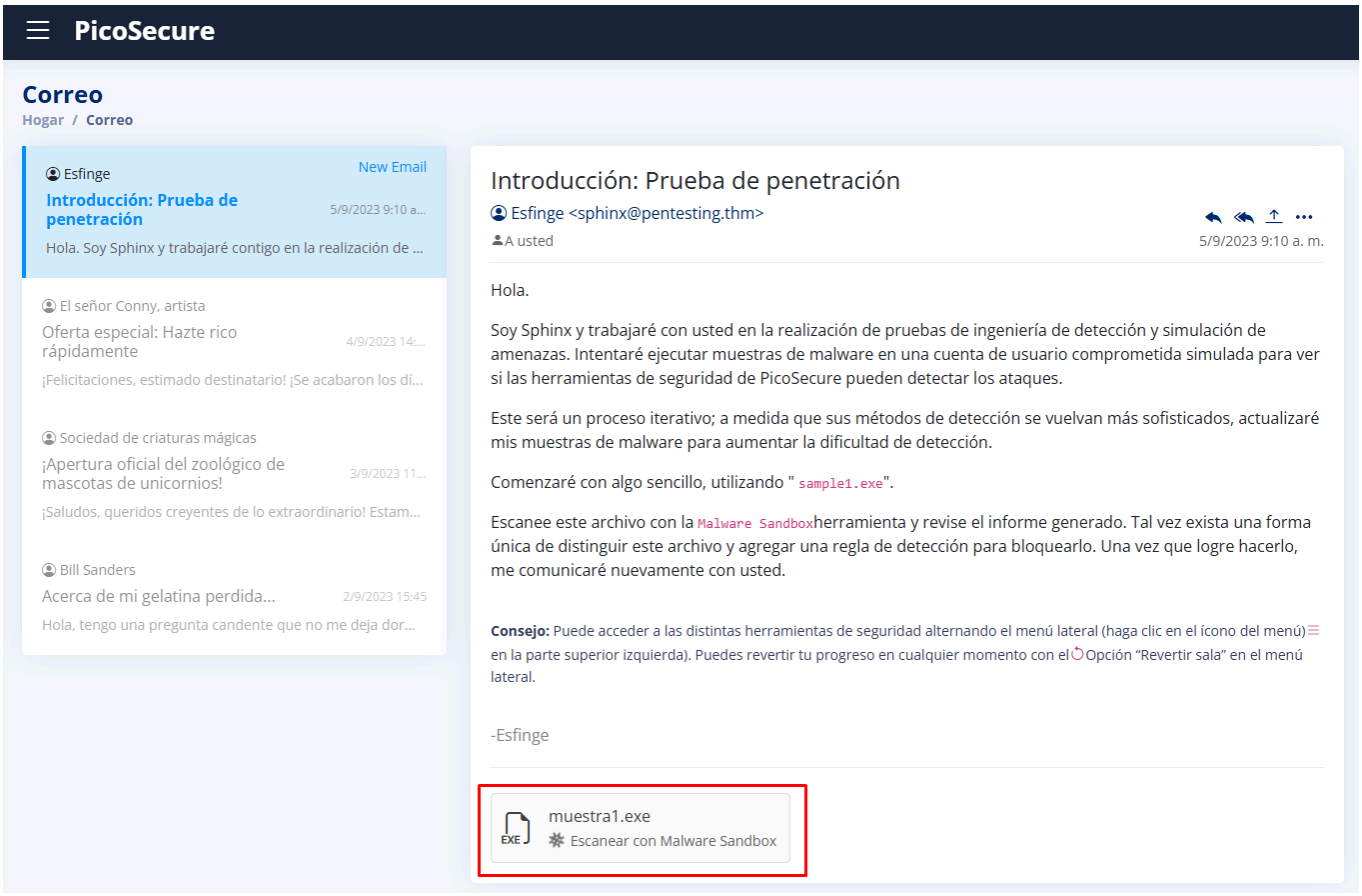
Haga clic en **Iniciar máquina** para implementar la aplicación y navegue a https://LAB_WEB_URL.p.thmlabs.com una vez que se haya completado la URL.

Proceso de solución de las preguntas

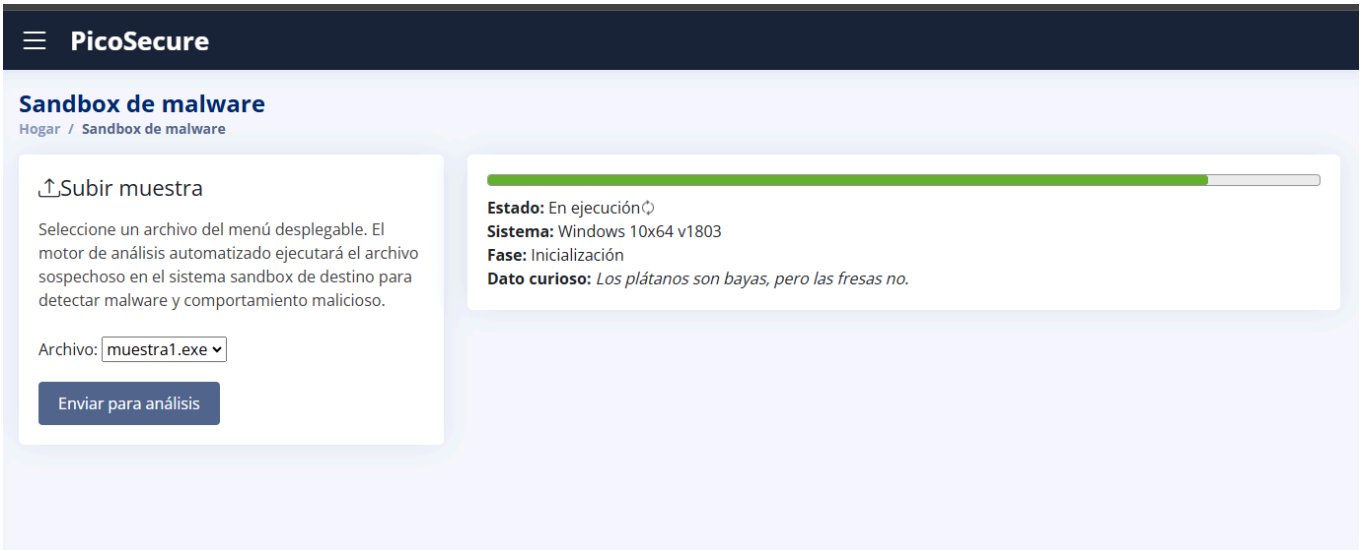
A lo largo de este desafío, se nos presentan seis escenarios con distintas muestras de malware proporcionadas por el evaluador. El objetivo es analizar el comportamiento de cada muestra, identificar los indicadores de compromiso generados y aplicar controles de seguridad para bloquear su ejecución.

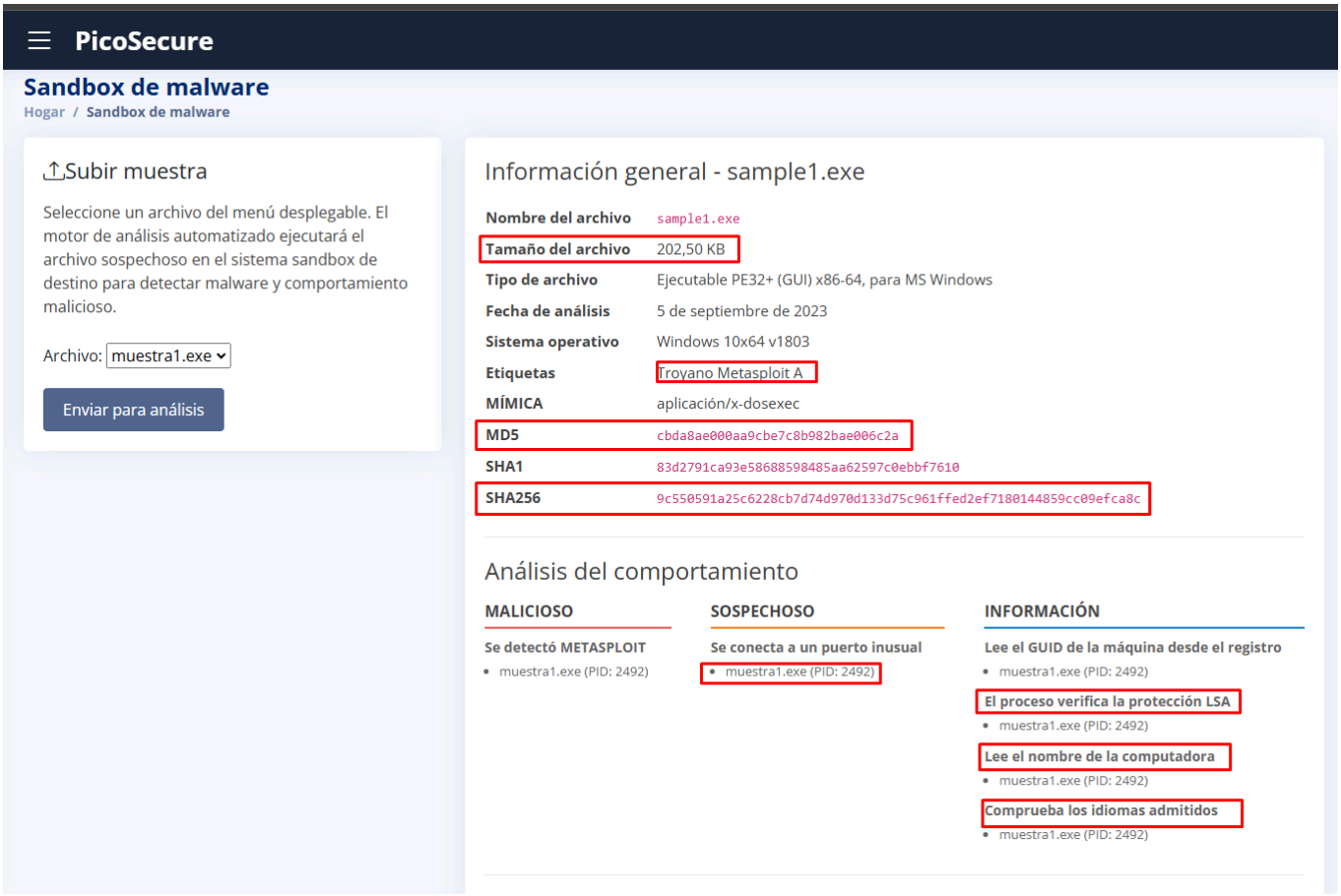
Cada escenario nos permitirá evaluar la efectividad de nuestras herramientas de detección, mejorar nuestras reglas de seguridad y fortalecer la postura defensiva de PicoSecure. Siguiendo un enfoque iterativo, ajustaremos nuestras estrategias para incrementar el costo operativo del adversario y minimizar el impacto de futuras amenazas.

Lo primero al abrir la plataforma es leer el primer correo donde nos indican que tenemos una muestra del malware llamado **sample1.exe** .

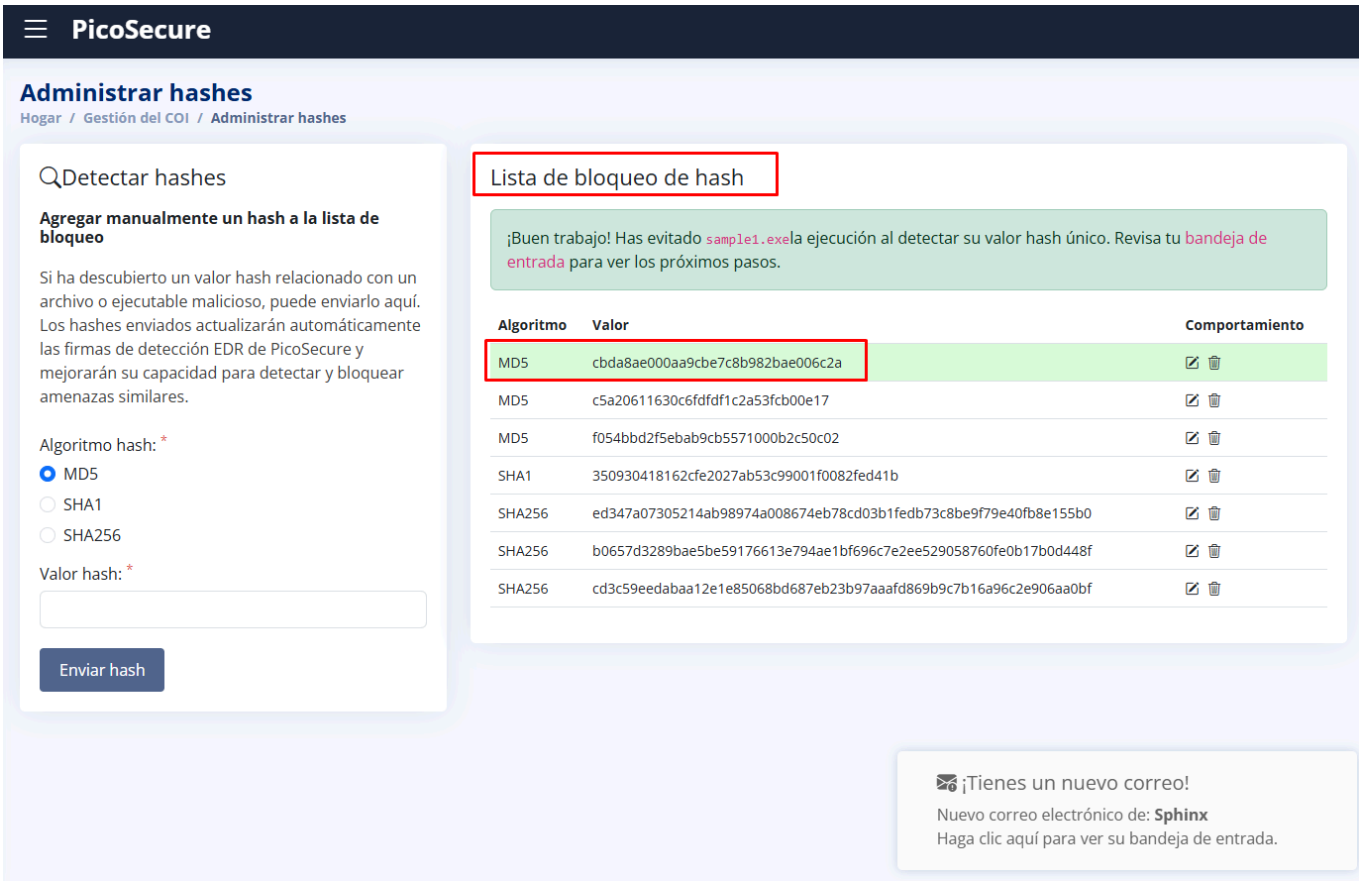


Si miramos las opciones desplegables vemos que contamos con varias opciones entre estas un sandbox, lo primero es validar la muestra en el sandbox para ver que información arroja.



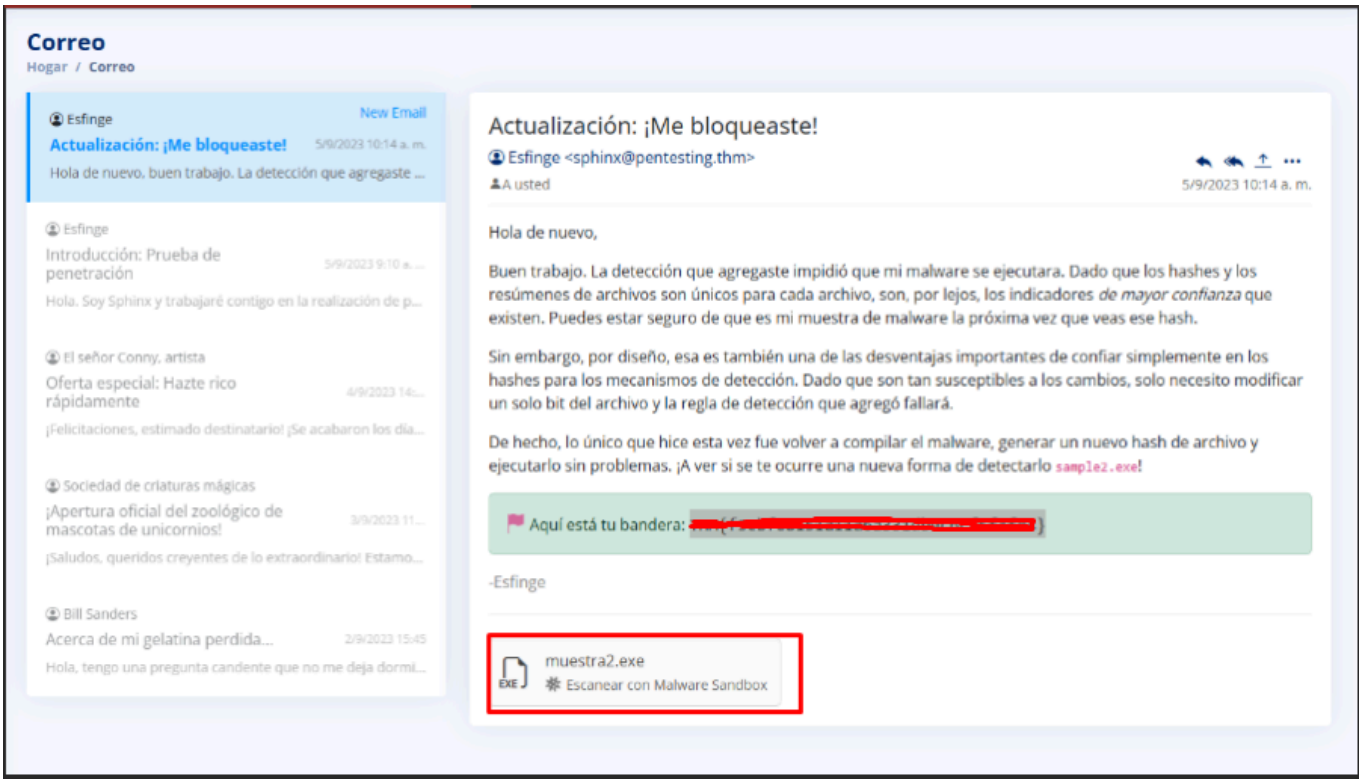


Esta información nos permite identificar el tamaño del archivo el tipo de malware que es y vemos que solo tenemos a nuestra disposición el MD5 y el sha256, por lo que dentro de nuestras opciones tenemos el poder realizar el bloqueo del hash en el administrador de hashes, esto nos ayudara a que la muestra en un futuro no se bloque directamente.

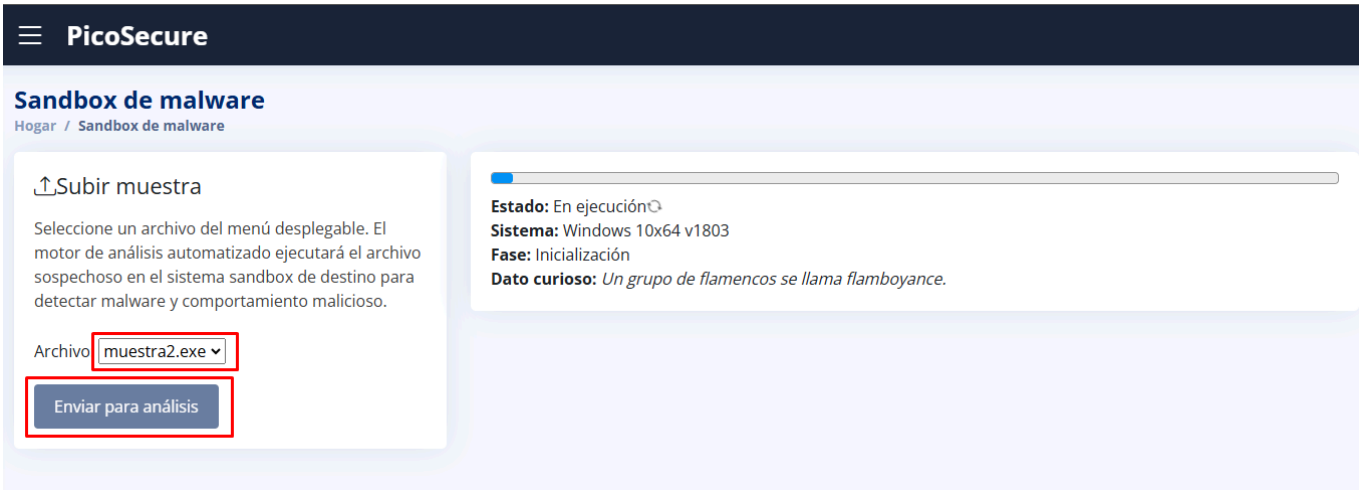


Esto nos generar la primera FLAg.

Posteriormente nos indicaran que se ha actualizado el malware ahora llamado **sample2.exe** que este ya no tendrá el mismo comportamiento que debemos validar y generar un nuevo bloqueo.



Realizo el mismo proceso valido la muestra en el sandbox:



Ahora ya tengo nueva informacion ademas de la basica para este ya me permite ver conexiones a IP:

PicoSecure

Sandbox de malware

Hogar / Sandbox de malware

Subir muestra

Seleccione un archivo del menú desplegable. El motor de análisis automatizado ejecutará el archivo sospechoso en el sistema sandbox de destino para detectar malware y comportamiento malicioso.

Archivo: muestra2.exe

Enviar para análisis

Información general - sample2.exe

Nombre del archivo	sample2.exe
Tamaño del archivo	202,73 KB
Tipo de archivo	PEXE - PE32+ ejecutable (GUI) x86-64, para MS Windows
Fecha de análisis	5 de septiembre de 2023
Sistema operativo	Windows 10x64 v1803
Etiquetas	Troyano Metasploit A
MÍMICA	aplicación/x-dosexec
MD5	4d661bf605d6b0b15915a533b572a6bd
SHA1	6878976974c27c8547cfc5acc90fb28ad2f0e975
SHA256	d576245e85e6b752b2fdffa43abaab1b2e1383556b0169fd04924d6cebc1cdf9

Análisis del comportamiento

MALICIOSO

Se detectó METASPLOIT
- sample2.exe (ID: 1927)

SOSPECHOSO

Se conecta a una dirección IP inusual
- sample2.exe (ID: 1927)

Se conecta a un puerto inusual
- sample2.exe (ID: 1927)

INFORMACIÓN

Lee el GUID de la máquina desde el registro
- sample2.exe (ID: 1927)

El proceso verifica la protección LSA
- sample2.exe (ID: 1927)

Lee el nombre de la computadora
- sample2.exe (ID: 1927)

Comprueba los idiomas admitidos
- sample2.exe (ID: 1927)

Actividad de red

Solicitudes HTTP(S)	Conexiones TCP/UDP	Solicitudes de DNS	Amenazas
1	3	0	0

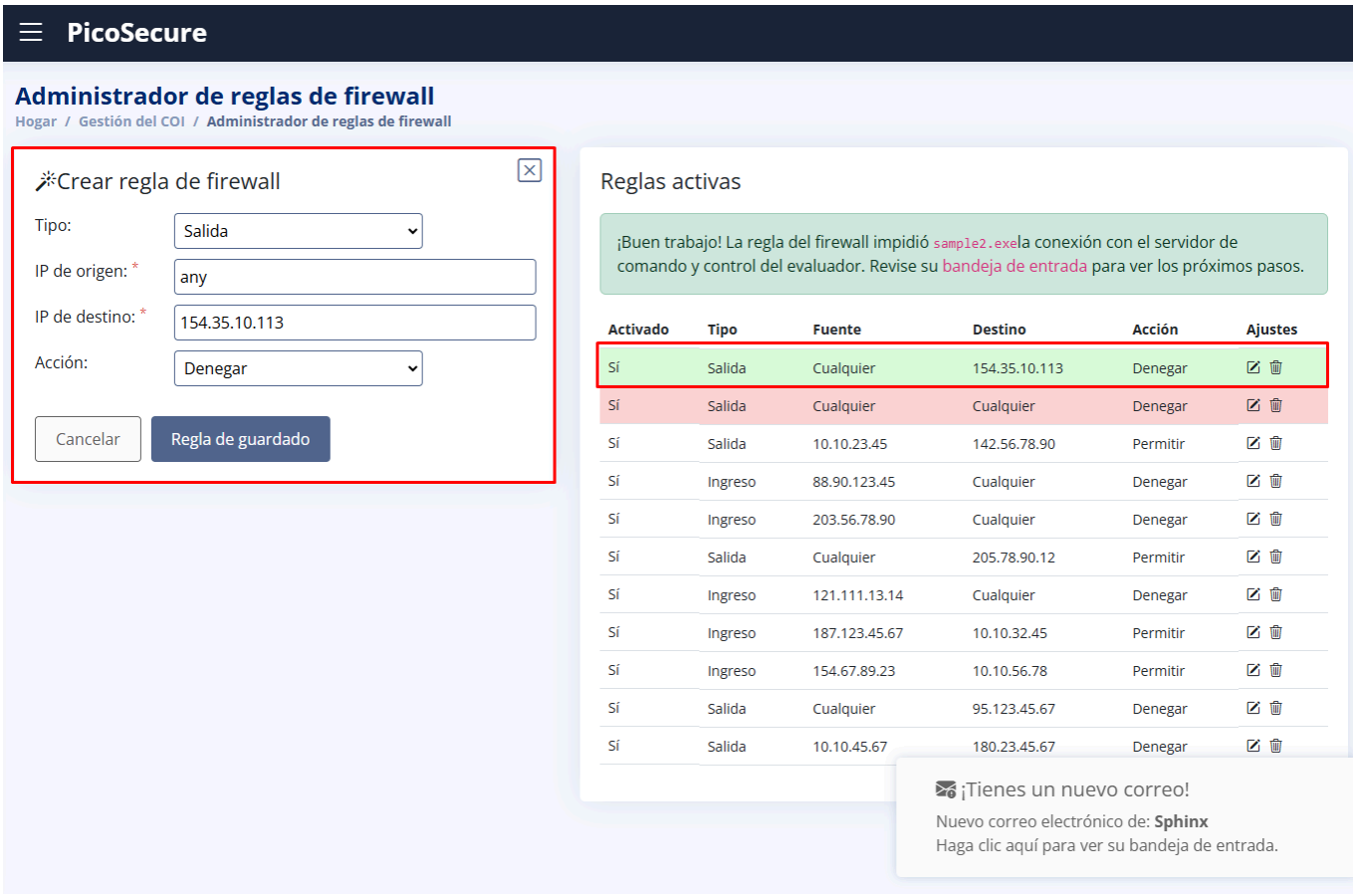
Solicitudes HTTP

Identificador PID	Proceso	Método	Propiedad intelectual	URL
1927	muestra2.exe	CONSEGUIR	154.35.10.113:4444	http://154.35.10.113:4444/uvLk8YI32

Conexiones

Identificador PID	Proceso	Propiedad intelectual	Dominio	ASN
1927	muestra2.exe	154.35.10.113:4444	-	Alojamiento Intrabuzz limitado
1927	muestra2.exe	40.97.128.3:443	-	Corporación Microsoft
1927	muestra2.exe	40.97.128.4:443	-	Corporación Microsoft

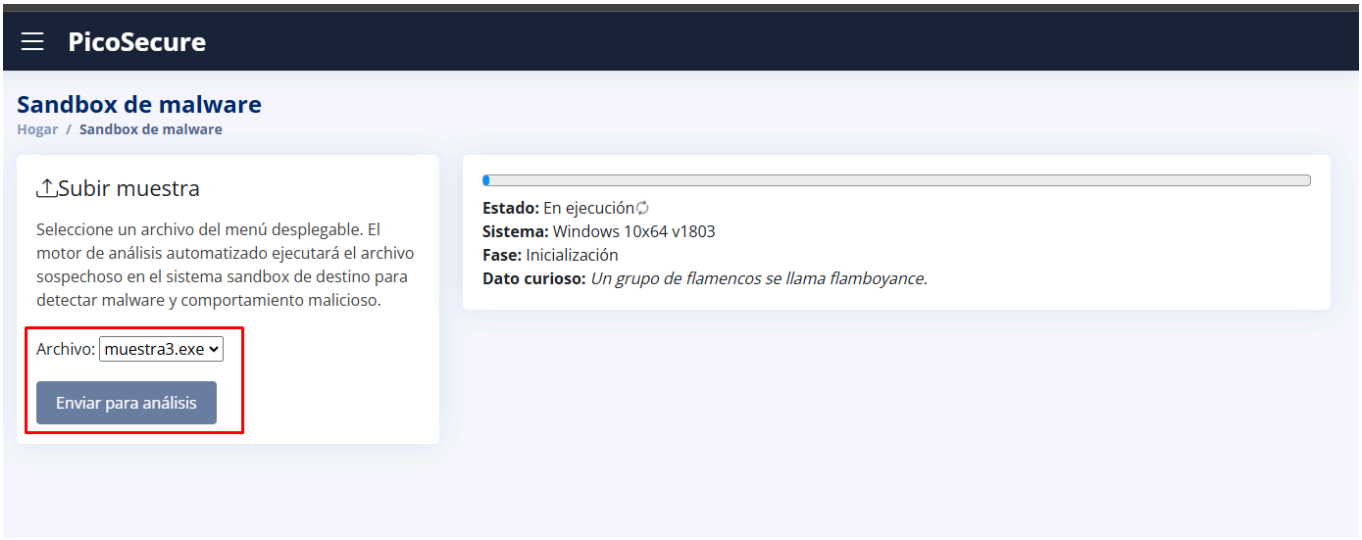
Con esta infamación lo que podemos realizar es un bloqueo en el FW para los datos salientes desde cualquier punto de nuestra red a esa dirección ip, no es algo totalmente seguro pero ponemos la IP en nuestra blacklist.

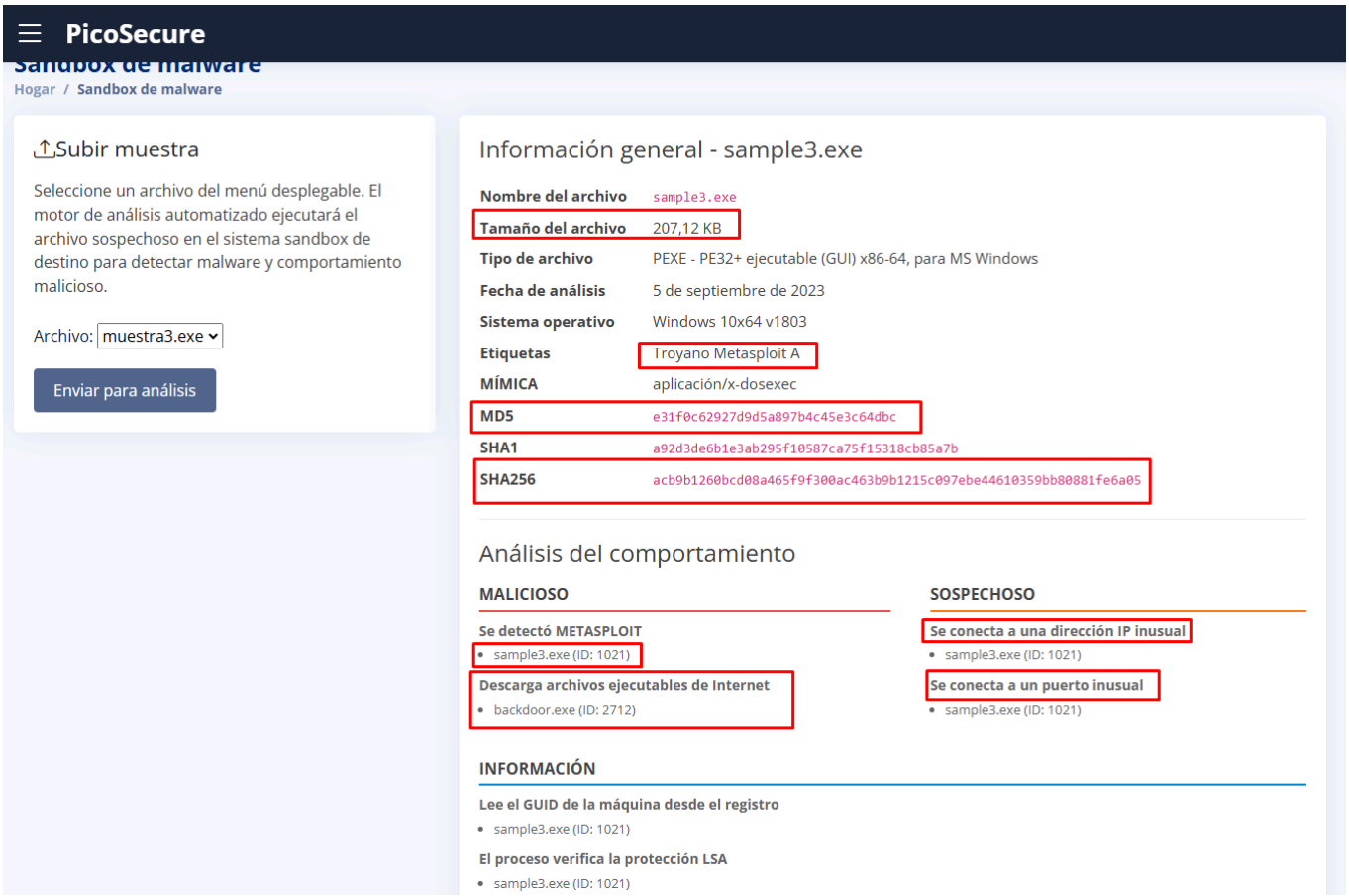


Con este proceso podremos obtener nuestra segunda FLAG.

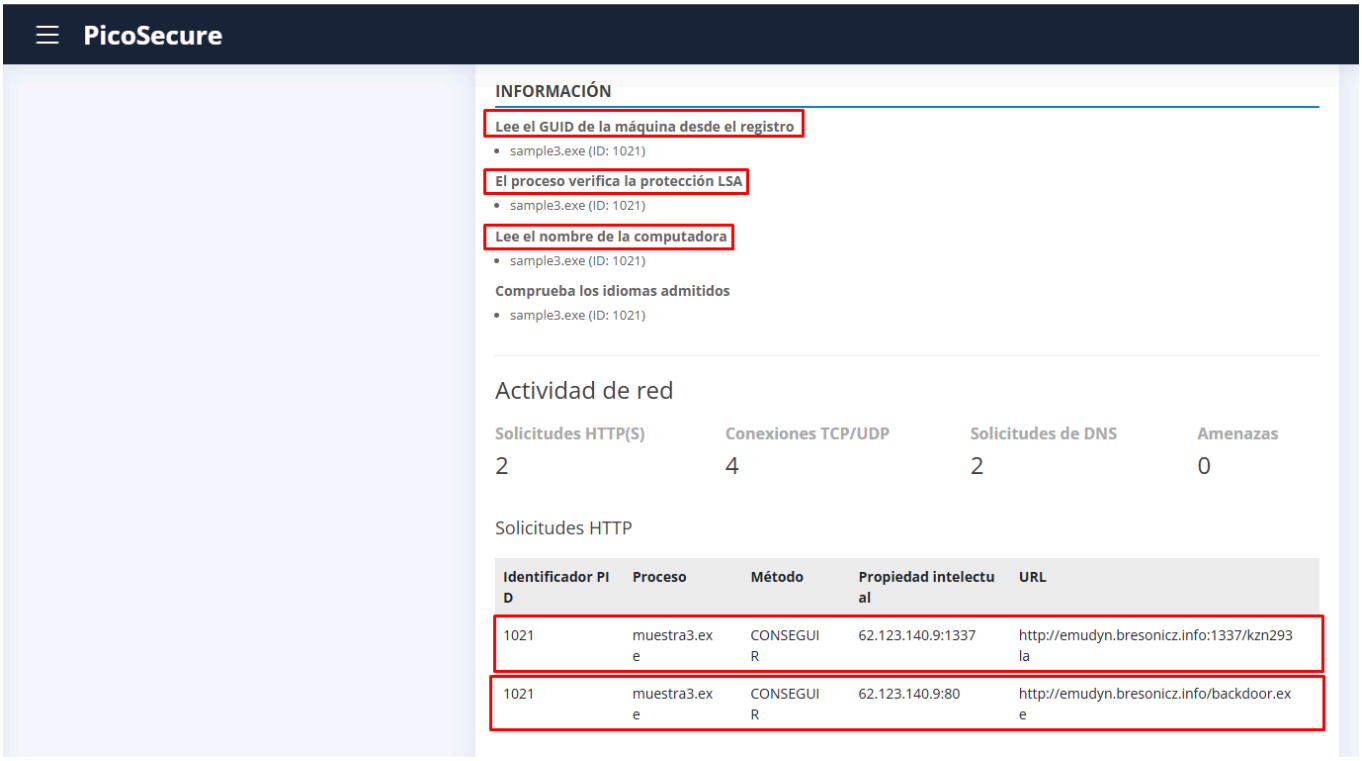
Ahora tenemos un nuevo intento esta vez e malware se llama *sample3.exe* como indique realizar el bloqueo solo a la ip no es algo que valla a bloquear aun atacante del todo estos pueden usar mas métodos para obtener nuevas ip y continuar realizando el ataque.

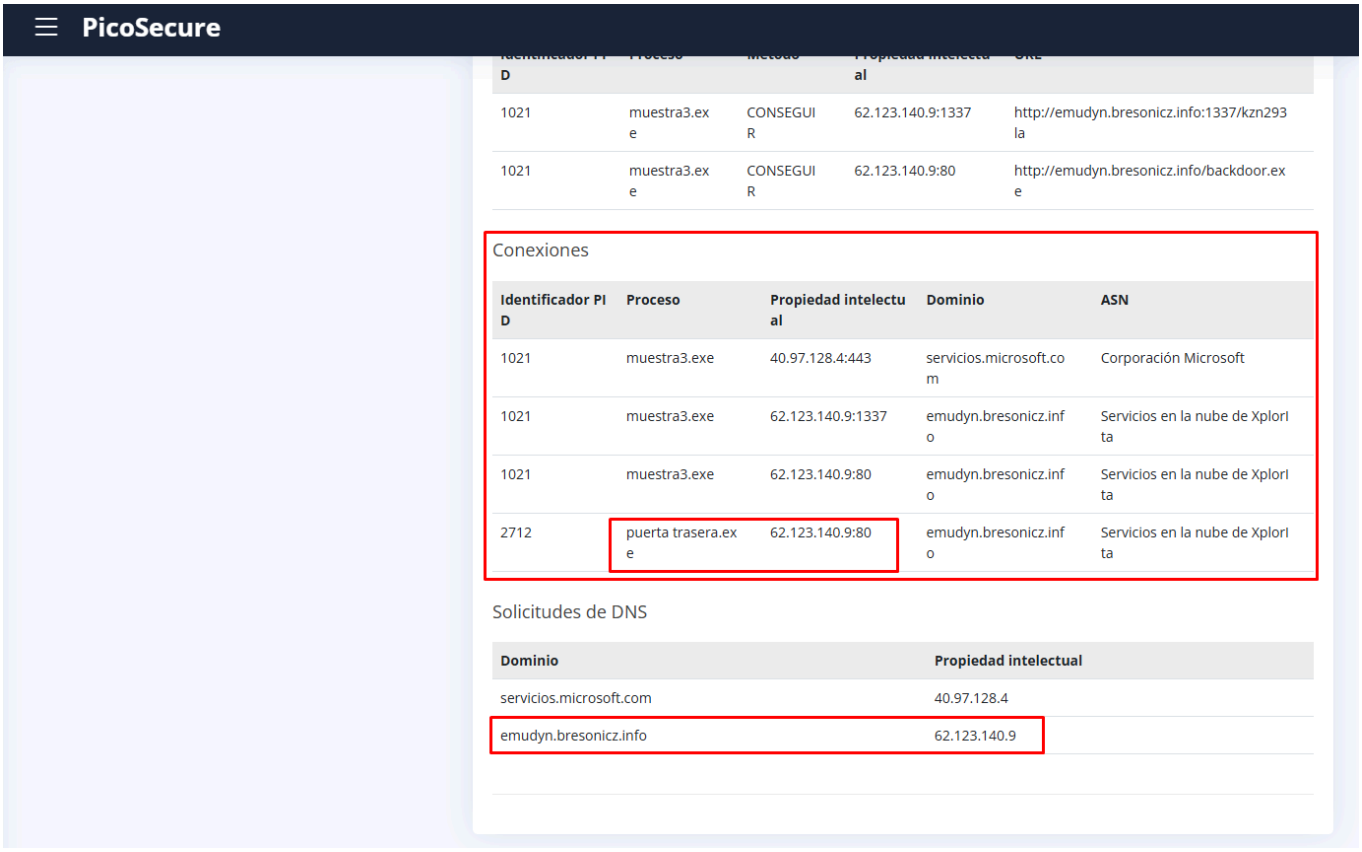
Por lo que volvemos a subir nuestra muestra al sandbox:



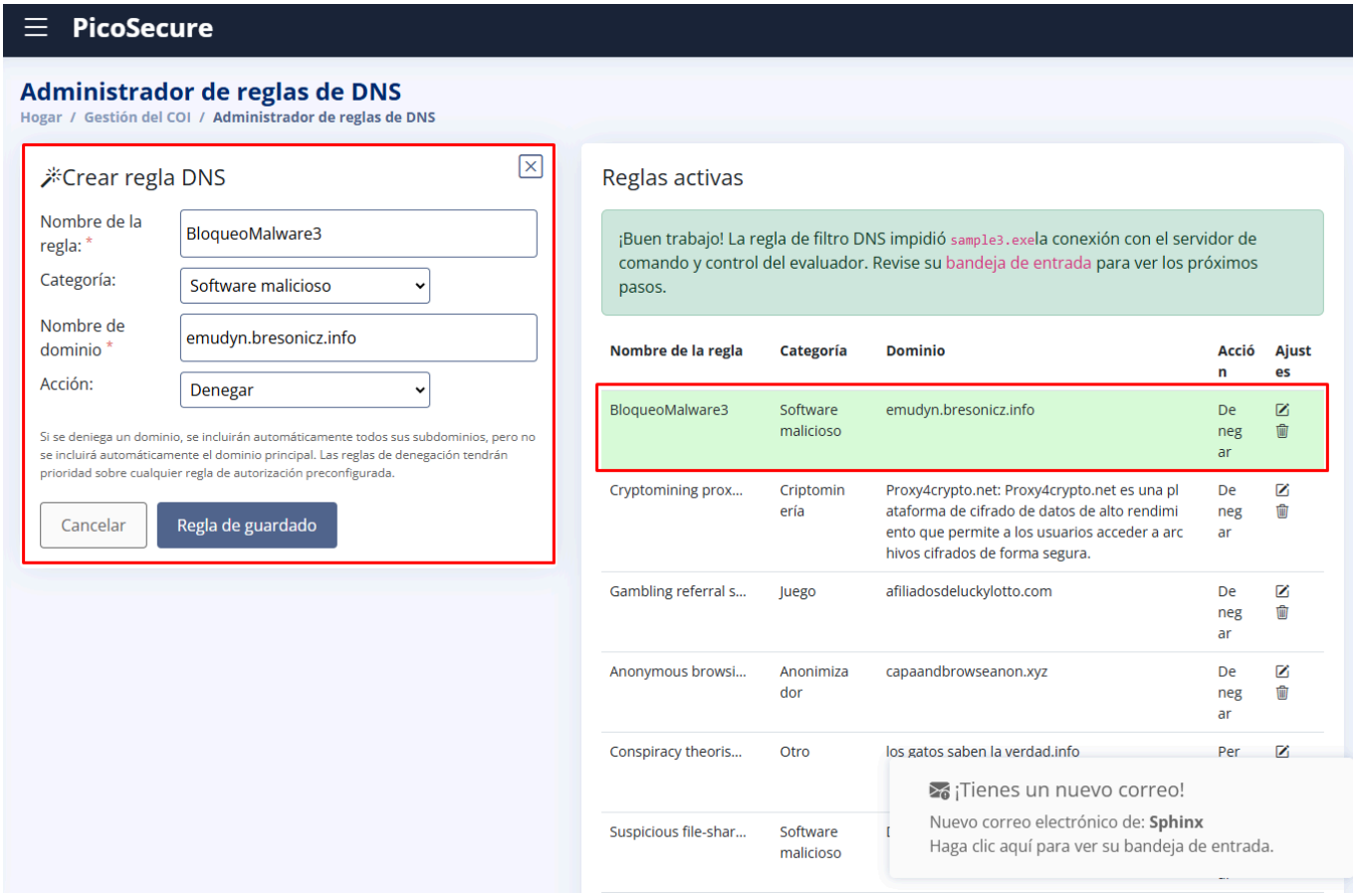


En esta muestra ya encontramos nueva información ya tenemos solicitudes http conexiones y dns records



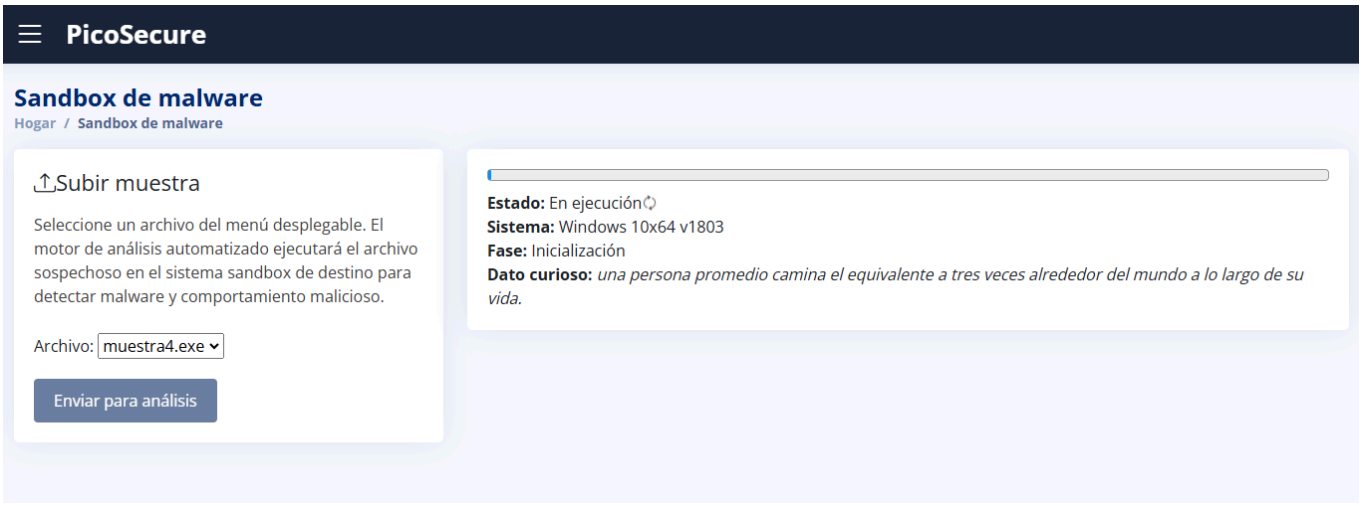


Dentro de la información mas relevante en esta nueva muestra es el record DNS: emudyn.bresonicz.info lo cual nos permitiria genera una regla de bloqueo para estos DNS especificos:



Nuevamente obtenemos la siguiente FLAG.

Ahora nos presentan la muestra *sample4.exe* debido a que ya hemos logrado cerrar conexiones ip por el FW accesos desde a los dominios con los bloqueos de DNS Records y bloqueos a hash, nos presentan esta nueva muestra la cual al llevarla al sandbox nos presenta infamación mas relévate y diferente que podemos usar:



PicoSecure

Sandbox de malware

Hogar / Sandbox de malware

Subir muestra

Seleccione un archivo del menú desplegable. El motor de análisis automatizado ejecutará el archivo sospechoso en el sistema sandbox de destino para detectar malware y comportamiento malicioso.

Archivo: muestra4.exe

Enviar para análisis

Información general - sample4.exe

Nombre del archivo	sample4.exe
Tamaño del archivo	219,46 KB
Tipo de archivo	PEXE - PE32+ ejecutable (GUI) x86-64, para MS Windows
Fecha de análisis	5 de septiembre de 2023
Sistema operativo	Windows 10x64 v1803
Etiquetas	Ninguno
MÍMICA	aplicación/x-dosexec
MD5	5f29ff19d99fe244eaf5835ce01a4631
SHA1	cd12d2328f700ae1ba1296a5f011bfc5a49f456d
SHA256	a80cffb40cea83c1a20973a5b803828e67691f71f3c878edb5a139634d7dd422

Análisis del comportamiento

MALICIOSO

Desactiva la supervisión en tiempo real de Windows Defender
- sample4.exe (ID: 3806)

Descarga archivos ejecutables de Internet
- backdoor.exe (ID: 1367)

SOSPECHOSO

Se conecta a una dirección IP inusual
- sample4.exe (ID: 3806)

Se conecta a un puerto inusual
- sample4.exe (ID: 3806)

Realiza cambios en el registro
- sample4.exe (ID: 3806)

PicoSecure

INFORMACIÓN

Lee el GUID de la máquina desde el registro
- sample4.exe (ID: 3806)

El proceso verifica la protección LSA
- sample4.exe (ID: 3806)

Lee el nombre de la computadora
- sample4.exe (ID: 3806)

Comprueba los idiomas admitidos
- sample4.exe (ID: 3806)

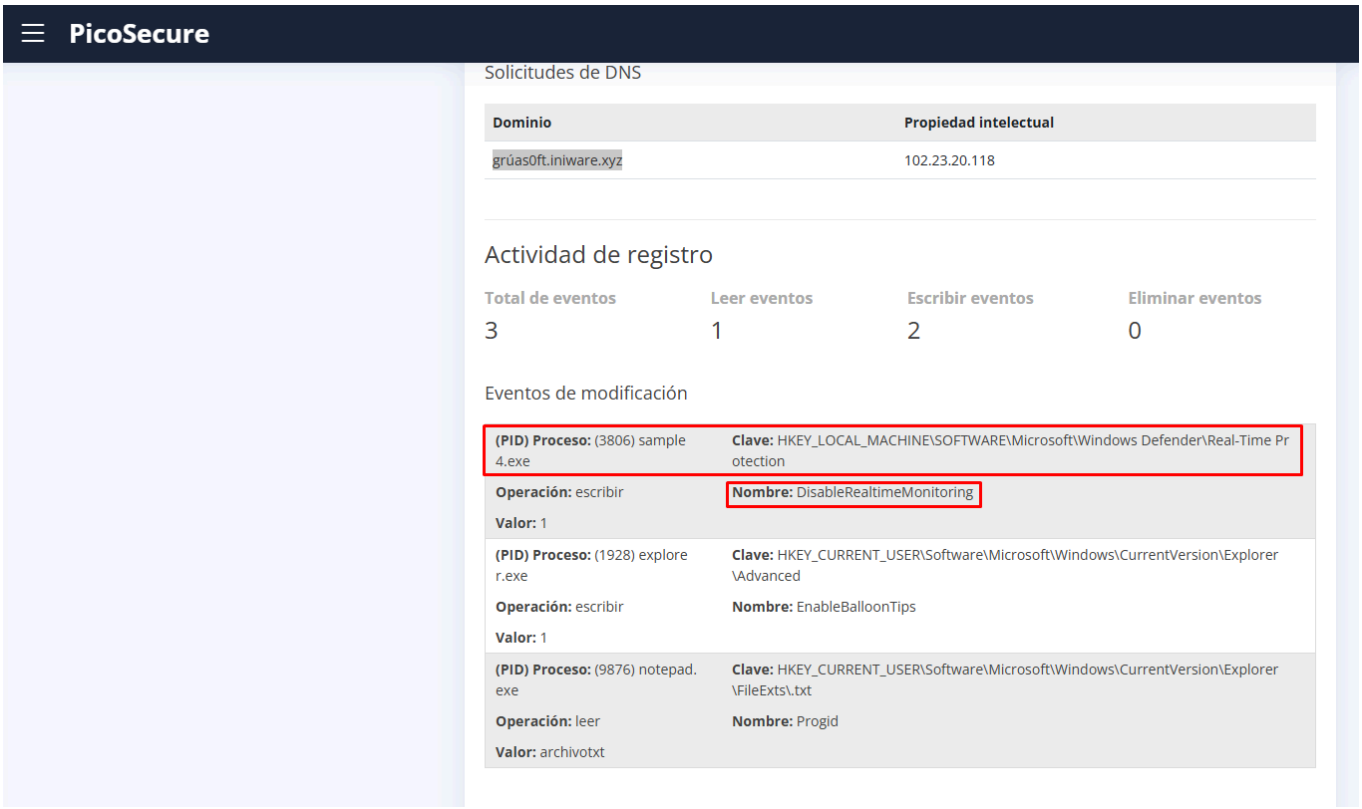
Actividad de red

Solicitudes HTTP(S)	Conexiones TCP/UDP	Solicitudes de DNS	Amenazas
2	3	1	0

Solicitudes HTTP

Identificador PID	Proceso	Método	Propiedad intelectual	URL
3806	muestra4.exe	CONSEGUIR	102.23.20.118:1337	http://cranes0ft.iniware.xyz:1337/ab9z83ja
3806	muestra4.exe	CONSEGUIR	102.23.20.118:80	http://cranes0ft.iniware.xyz/backdoor.exe

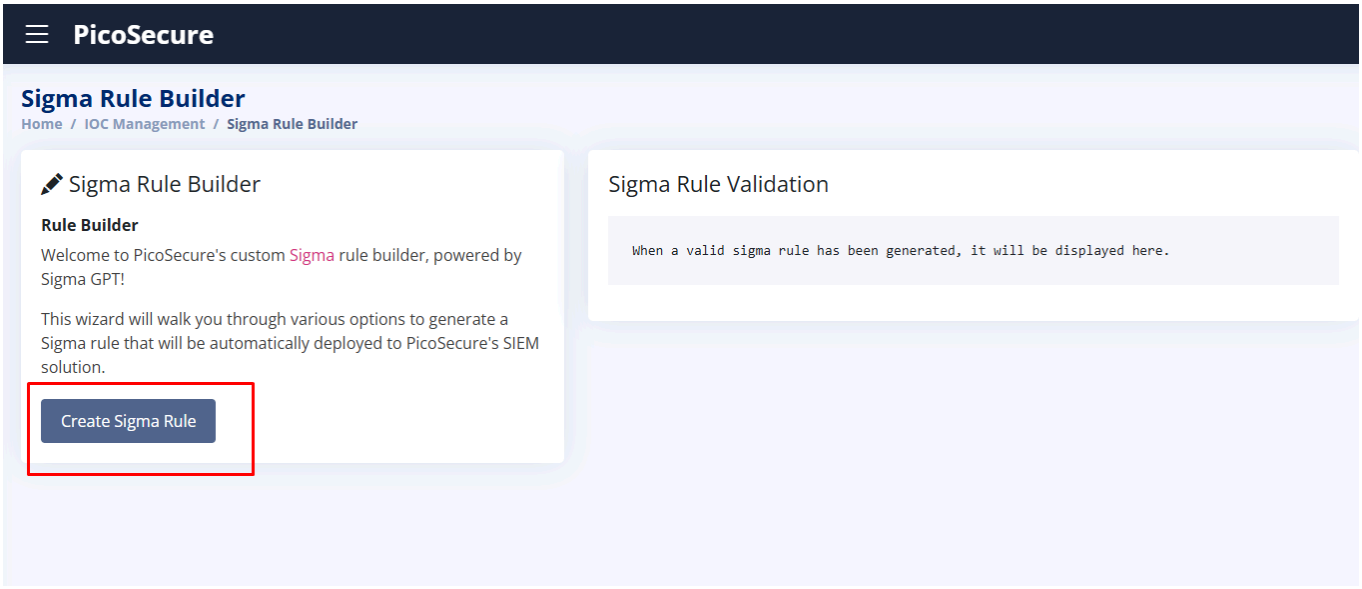
Tenemos nuevamente una nueva solicitud de DNS: grúas0ft.iniware.xyz & 102.23.20.118.

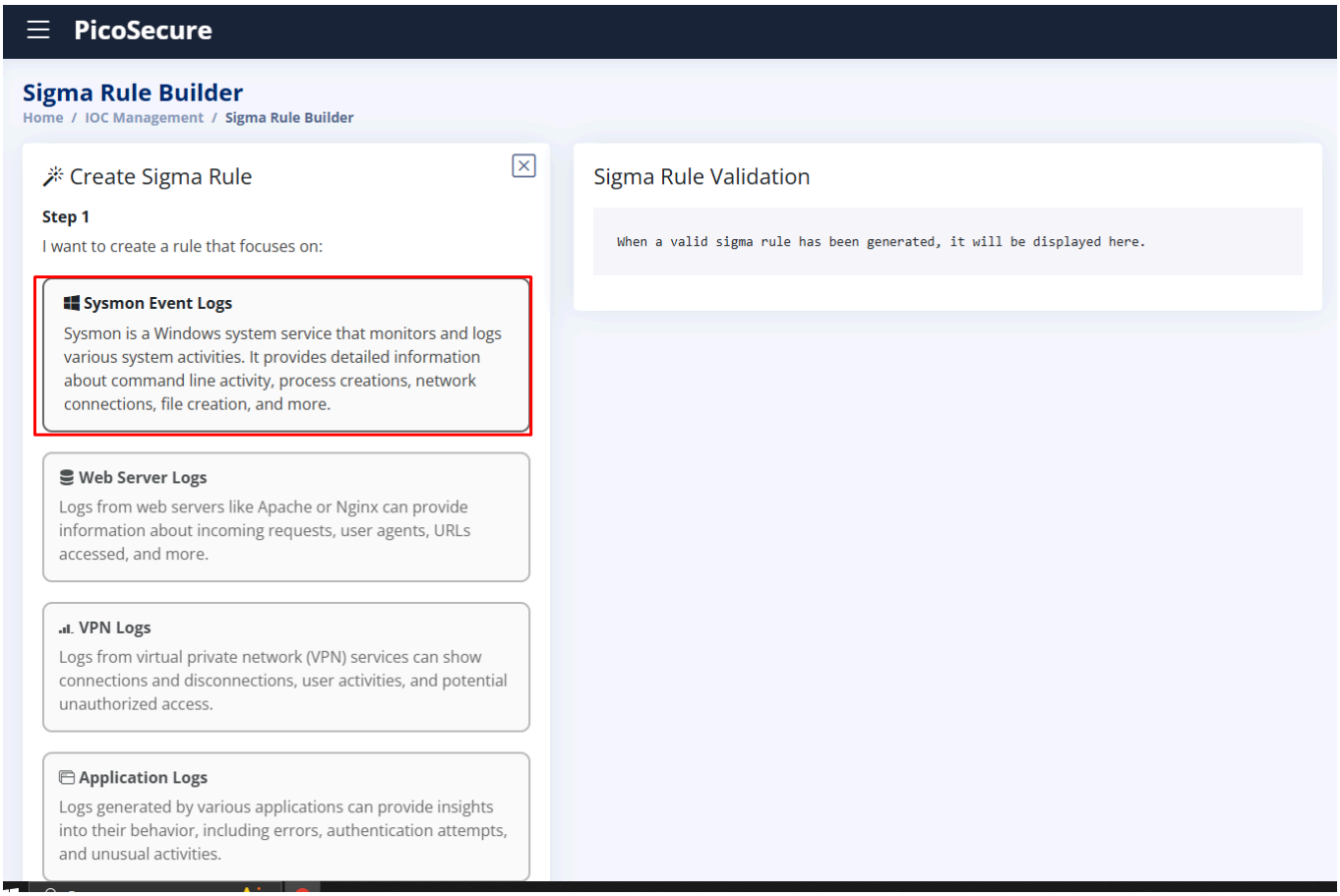


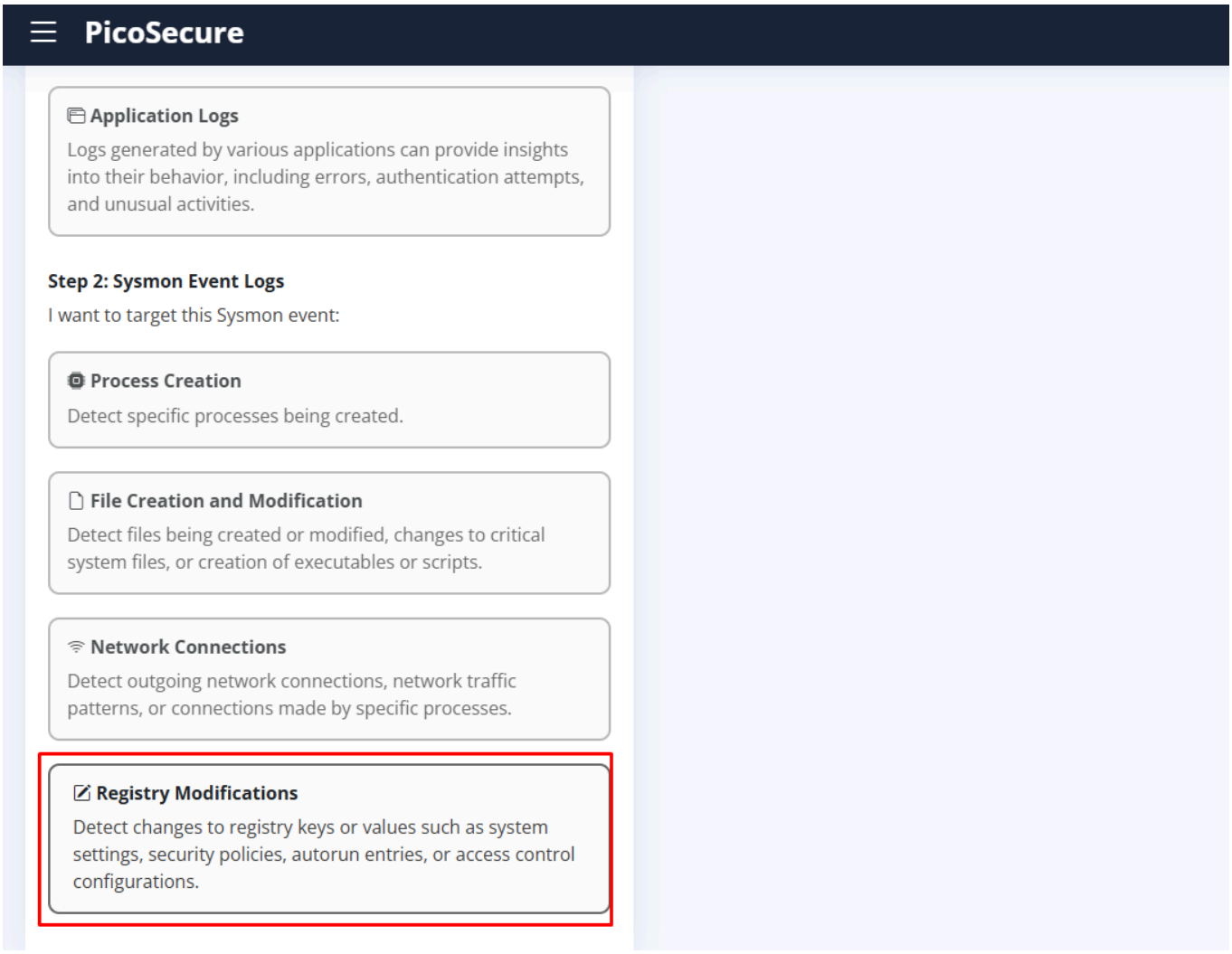
Pero esta ves vemos que se ha interactuado con un evento a nivel de maquina el evento es:

- Nombre: DisableRealtimeMonitoring
- Key:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
- Value:1

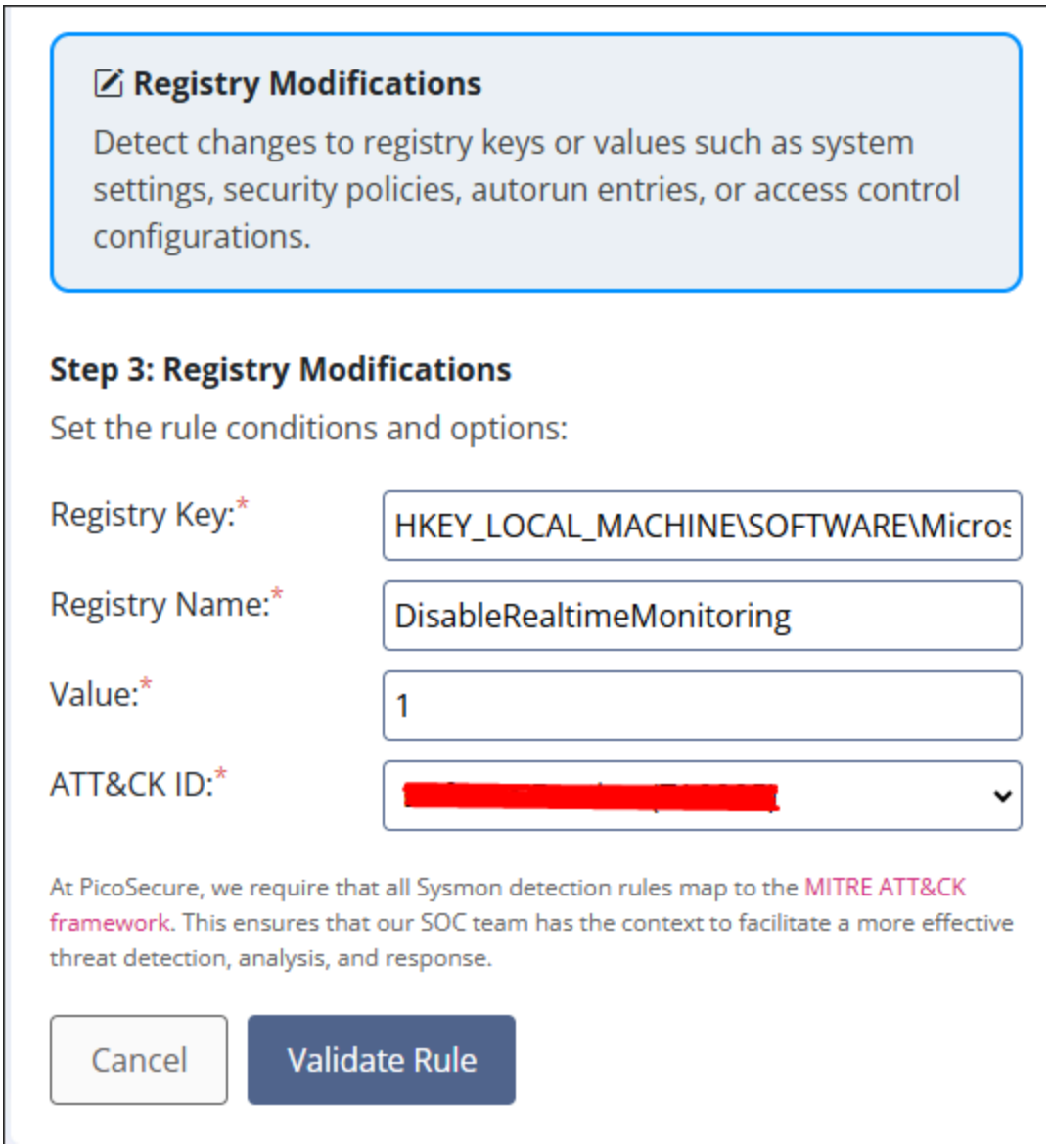
Esto nos va a permitir crear una regla de detección a nivel de maquina usando los registros del sistema:



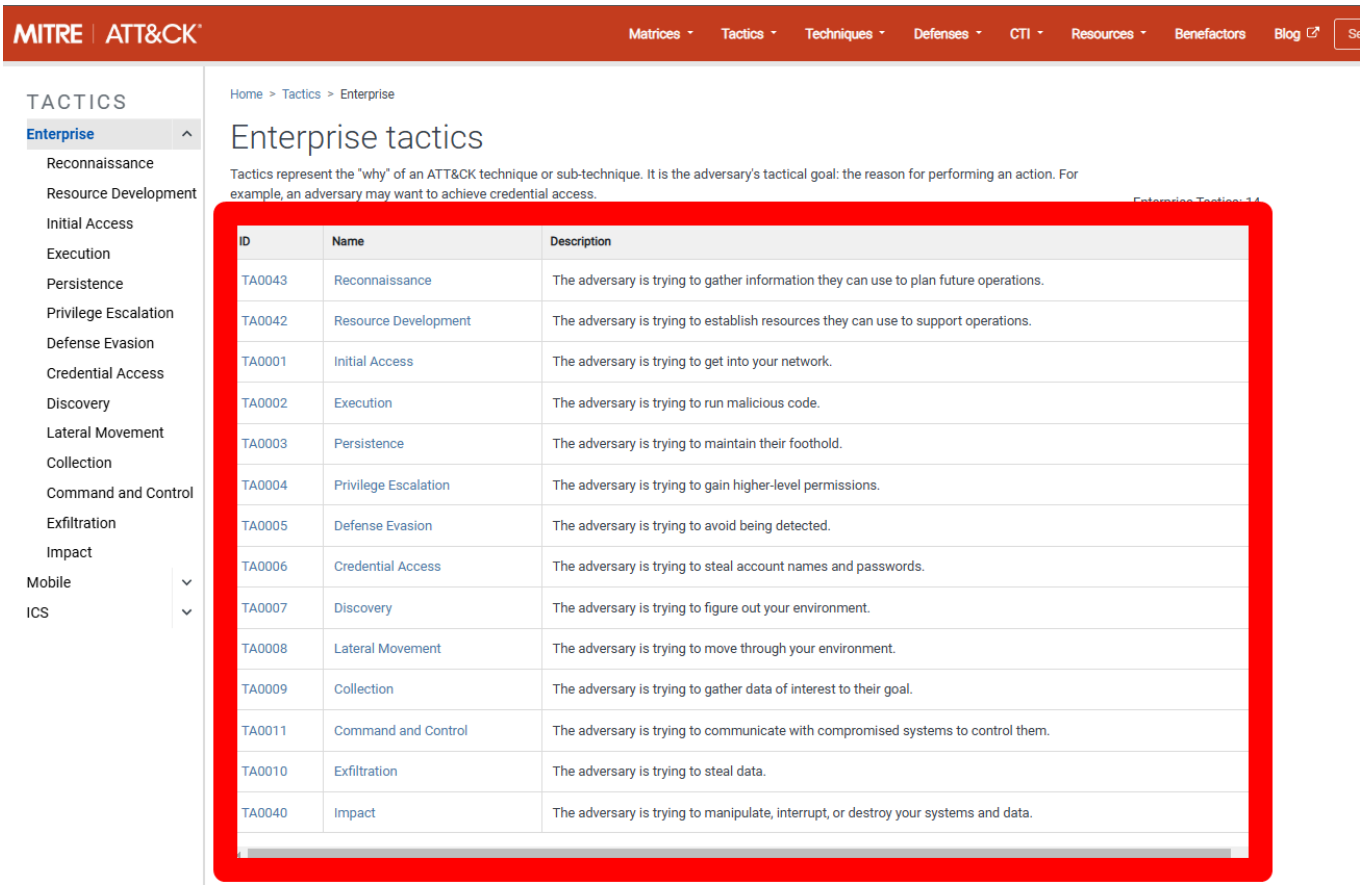




Esta regla contiene el parámetro del registro que encontramos el nombre y el valor y determinamos el tipo de ataque al que corresponde para pode crearla:



Para este caso ya podemos hacer uso de lo aprendido acerca de Mitre dado que nos proporcionan diferentes tácticas para escoger como sabemos en el marco de mitre tenemos 14 tácticas que son las siguientes:



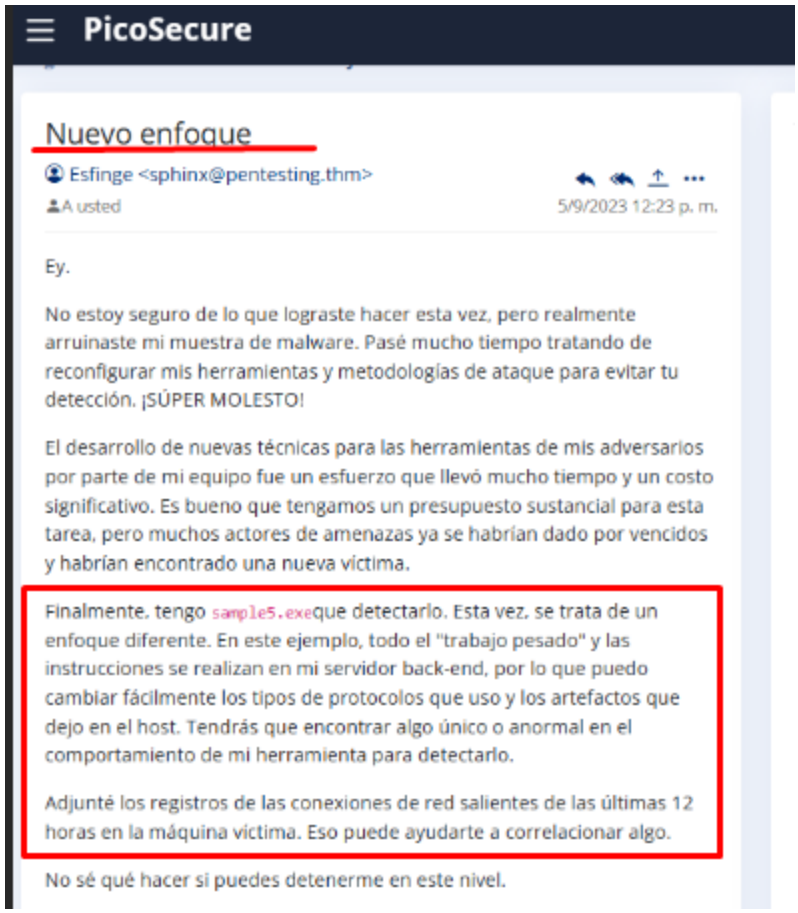
Según el evento que vimos tenemos que saber que esta buscando realizar el malware para asociarlo en la detección leer la descripción de las tácticas para escoger la correcta el resultado de la regla se vera algo así.

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 DisableRe

references:
  - https://attack.mitre.org/tactics[redacted]

tags:
  [redacted]
  - sysmon

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

  condition: selection

falsepositives:
  - Legitimate changes to Windows Defender settings.

level: high
```

Esto nos dará nuestra Cuarta FLAG.

Ahora nos proporcionan un log que es la muestra *sample5.exe* y nos indican que:



PicoSecure

Nuevo enfoque

Esfinge <sphinx@pentesting.thm>

A usted

5/9/2023 12:23 p. m.

Ey.

No estoy seguro de lo que lograste hacer esta vez, pero realmente arruinaste mi muestra de malware. Pasé mucho tiempo tratando de reconfigurar mis herramientas y metodologías de ataque para evitar tu detección. ¡SÚPER MOLESTO!

El desarrollo de nuevas técnicas para las herramientas de mis adversarios por parte de mi equipo fue un esfuerzo que llevó mucho tiempo y un costo significativo. Es bueno que tengamos un presupuesto sustancial para esta tarea, pero muchos actores de amenazas ya se habrían dado por vencidos y habrían encontrado una nueva víctima.

Finalmente, tengo `sample5.exe`que detectarlo. Esta vez, se trata de un enfoque diferente. En este ejemplo, todo el "trabajo pesado" y las instrucciones se realizan en mi servidor back-end, por lo que puedo cambiar fácilmente los tipos de protocolos que uso y los artefactos que dejo en el host. Tendrás que encontrar algo único o anormal en el comportamiento de mi herramienta para detectarlo.

Adjunté los registros de las conexiones de red salientes de las últimas 12 horas en la máquina víctima. Eso puede ayudarte a correlacionar algo.

No sé qué hacer si puedes detenerme en este nivel.

Viendo archivo adjunto:`outgoing_connections.log`

```
2023-08-15 09:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 09:23:45 | Origen: 10.10.15.12 | Destino: 43.10.65.115 | Puerto: 443 | Tamaño: 21541 bytes
2023-08-15 09:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 10:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 10:14:21 | Origen: 10.10.15.12 | Destino: 87.32.56.124 | Puerto: 80 | Tamaño: 1204 bytes
2023-08-15 10:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 11:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 11:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 11:45:09 | Origen: 10.10.15.12 | Destino: 145.78.90.33 | Puerto: 443 | Tamaño: 805 bytes
2023-08-15 12:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 12:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 13:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 13:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 13:32:17 | Origen: 10.10.15.12 | Destino: 72.15.61.98 | Puerto: 443 | Tamaño: 26084 bytes
2023-08-15 14:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 14:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 14:55:33 | Origen: 10.10.15.12 | Destino: 208.45.72.16 | Puerto: 443 | Tamaño: 45091 bytes
2023-08-15 15:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 15:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 15:40:10 | Origen: 10.10.15.12 | Destino: 101.55.20.79 | Puerto: 443 | Tamaño: 95021 bytes
2023-08-15 16:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 16:18:55 | Origen: 10.10.15.12 | Destino: 194.92.18.10 | Puerto: 80 | Tamaño: 8004 bytes
2023-08-15 16:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 17:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 17:09:30 | Origen: 10.10.15.12 | Destino: 77.23.66.214 | Puerto: 443 | Tamaño: 9584 bytes
2023-08-15 17:27:42 | Origen: 10.10.15.12 | Destino: 156.29.88.77 | Puerto: 443 | Tamaño: 10293 bytes
2023-08-15 17:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 18:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 18:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 19:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 19:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 20:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 20:30:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
2023-08-15 21:00:00 | Origen: 10.10.15.12 | Destino: 51.102.10.19 | Puerto: 443 | Tamaño: 97 bytes
```

En este log podemos ver varios detalles los cuales son interesantes por el numero de bytes que se generan, estos nos ayuda a identificar que patrón es el que debería ser y cual es el anómalo, no obstante también vemos diferentes destinos generando este comportamiento a la misma ip de origen y un puerto especifico, con esta información lo mas lógico es realizar un bloqueo a partir de reglas de conexión para poder identificar patrones anómalos en la red:

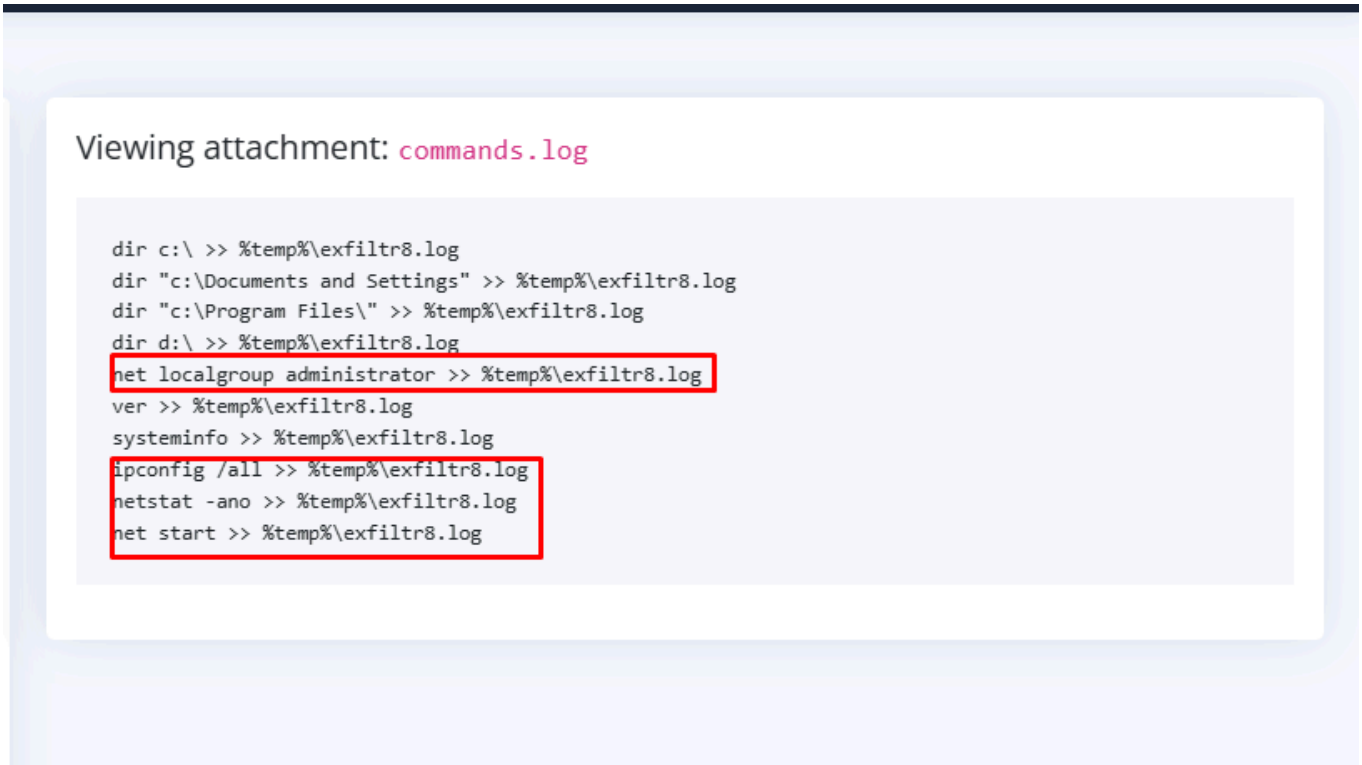
Usamos la misma teoría del anterior debemos interpretar que se debe bloquear a cual debería ser el comportamiento en bytes regular y que identificación le damos a ese comportamiento anómalo, al finalizar tendremos una regla de esta manera.

Validación de la regla Sigma

```
Título: Alerta sobre conexiones sospechosas a la red Beacon
id: criterios_de_conexiones_de_red_sysmon
Descripción: |
  Detecta conexiones de red con criterios específicos en los registros de Sysmon: IP remota, puerto re

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

etiquetas:
  - [redacted]1
  - sysmon

detección:
  selección:
    Identificador de evento: 3
    IP remota: '*'
    Puerto remoto: '*'
    [redacted]
    Frecuencia: 1800 segundos

  condición: selección

falsos positivos:
  - El tráfico de red legítimo puede cumplir estos criterios.

nivel: alto
```

Con esto obtenemos nuestra FLAG y ampliamos la seguridad.

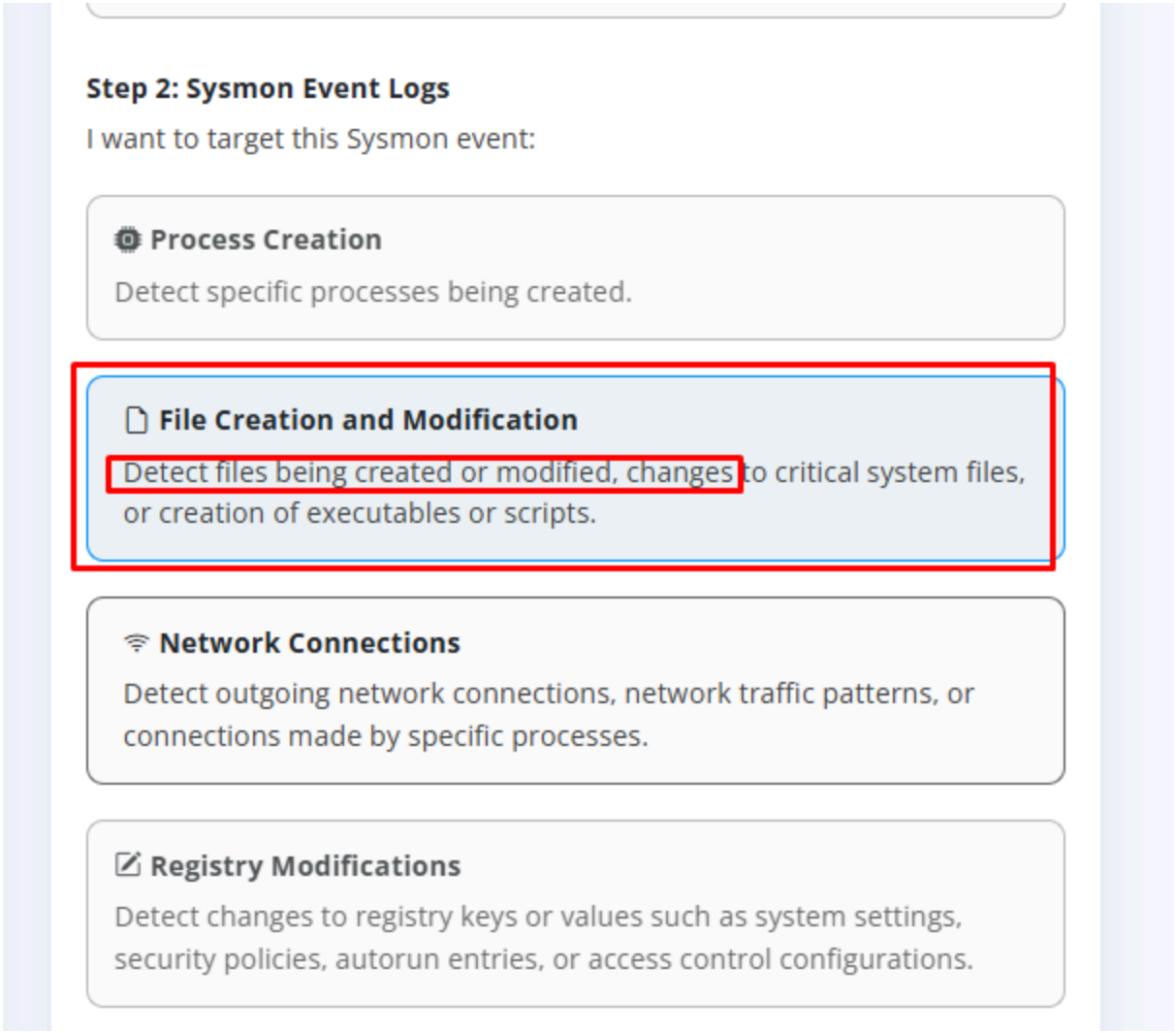
Por lo que para la ultima parte del reto nos proporcionan unos logs de comandos.



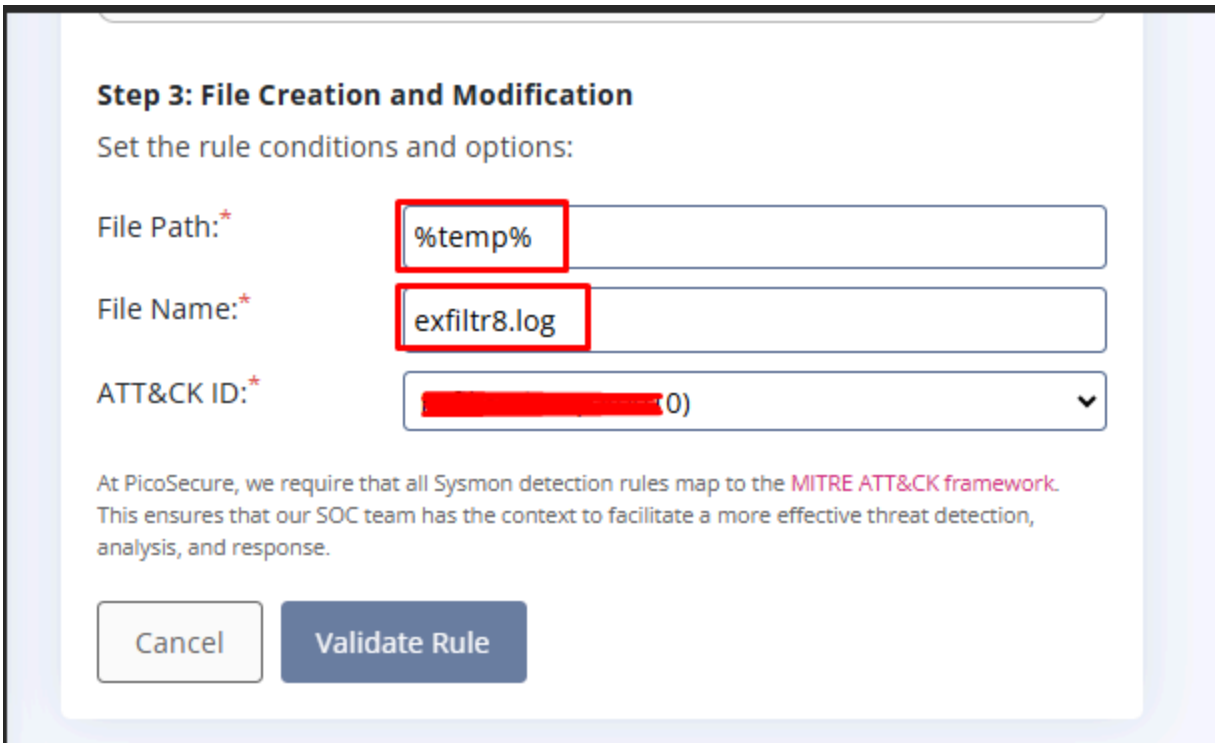
En este log vemos que el atacante crea un archivo log en una ruta del sistema, lista los usuarios del grupo local muestra la información del sistema valida todas las opciones de red usando netstat para enumerar los sockets abiertos y las conexiones activas, mostrar de forma numérica las direcciones y los números de puerto y presentar las conexiones con el ID de proceso correspondiente además de inicializar el net start para subir el servicio. Debido a esto las líneas que nos muestran información relevante son las siguientes:

- %temp%\exfiltr8.log
- dir "c:\Program Files" >> %temp%\exfiltr8.log
- dir d:\ >> %temp%\exfiltr8.log
- net localgroup administrator >> %temp%\exfiltr8.log
- systeminfo >> %temp%\exfiltr8.log
- ipconfig /all >> %temp%\exfiltr8.log
- netstat -ano >> %temp%\exfiltr8.log
- net start >> %temp%\exfiltr8.log

Con esto podemos crear una nueva regla para validar los registros cuando haya una creación o modificación de archivos en el sistema:



Los parámetros quedarían así:



Hacemos uso de las tácticas de mitre y generamos el bloqueo, con ello recibimos la ultima FLAG indicando que hemos finalizado.

Gracias.