

Laboratorio - Investigación de un ataque en un host de Windows

Objetivos

En esta práctica de laboratorio:

Parte 1: Investigue el ataque con Sguil

Parte 2: Usa Kibana para investigar alertas

Esta práctica de laboratorio se basa en un ejercicio del sitio web malware-traffic-analysis.net que es un excelente recurso para aprender a analizar los ataques de red y host. Gracias a brad@malware-traffic-analysis.net por el permiso para usar materiales de su sitio.

Aspectos básicos/Situación

En marzo de 2019, las herramientas de supervisión de seguridad de red alertaron de que un equipo Windows de la red estaba infectado con malware. En esta tarea, debe investigar las alertas y responder a las siguientes preguntas:

- ¿Cuál fue la hora específica del ataque en 2019-03-19?
- ¿Qué equipo host de Windows se infectó? ¿Quién era el usuario?
- ¿Con qué estaba infectada la computadora?

Recursos necesarios

- En mi máquina virtual de Security Onion
- Acceso a Internet

Instrucciones

Parte 1: Investiga el ataque con Sguil

En la Parte 1, usará Sguil para comprobar las alertas de IDS y recopilar más información sobre la serie de eventos relacionados con un ataque del 3-19-2019.

Nota: Los ID de alerta utilizados en este laboratorio son únicamente ilustrativos. Las alertas IDs en su MV (máquina virtual) pueden ser diferentes.

Paso 1: Abra Sguil y localice las alertas en 3-19-2019.

- a. Inicie sesión en Security Onion VM con el nombre de usuario **analyst** y la contraseña **cyberops**.
- b. Inicie Sguil desde el escritorio. Inicie sesión con username **analyst** and password **cyberops**. Haga clic en **Seleccionar todo** e **Iniciar Sguil** para ver todas las alertas generadas por los sensores de red.
- c. Localice el grupo de alertas a partir del 19 de marzo de 2019.

Según Sguil, ¿cuáles son las marcas de tiempo para la primera y última de las alertas que ocurrieron el 3-19-2019? ¿Qué es interesante acerca de las marcas de tiempo de todas las alertas del 3-19-2019?

Paso 2: Revise las alertas en detalle.

- En Sguil, haga clic en la primera de las alertas del 3-19-2019 (ID de alerta 5.439). Asegúrese de marcar las casillas de verificación **Mostrar datos del paquete** y **Mostrar regla** para examinar la información del encabezado del paquete y la regla de firma IDS relacionada con la alerta. Clic derecho en el **ID de alerta** y pívote hacia Wireshark. Sobre la base de la información derivada de esta alerta inicial, responda a las siguientes preguntas:

¿Cuál era la dirección IP de origen y el número de puerto y la dirección IP de destino y el número de puerto?

¿Qué tipo de protocolo y solicitud o respuesta estuvo involucrado?

¿Qué es la alerta y el mensaje de IDS?

¿Cree que esta alerta fue el resultado de una mala configuración de IDS o de una comunicación sospechosa legítima?

¿Cuál es el nombre de host, el nombre de dominio y la dirección IP del host de origen en la actualización DNS?

- En Sguil, seleccione la segunda de las alertas del 3-19-2019. Haga clic con el botón derecho en el ID de alerta 5.440 y seleccione **Transcript**.

The screenshot shows the Sguil interface with the title 'seconion-import-1_411'. On the left, there's a text-based transcript of the network interaction. On the right, there's a detailed packet analysis view with columns for DST, Connection, Content-Type, and various hex and ASCII representations of the data. The transcript shows an HTTP GET request from 'SRC' to 'DST' for the URL '/test1.css'. The response code is 200 OK. The packet analysis shows the raw bytes of the HTTP exchange, including headers like 'Content-Type: application/octet-stream' and body content related to Windows file paths and registry keys.

```
seconion-import-1_411

Serial Name: seconion-import-1
Timestamp: 2019-03-19 01:47:04
Connection ID: seconion-import-1_411
Src IP: 10.0.90.215
Dst IP: 209.141.34.8
Src Port: 49204
Dst Port: 80
OS Fingerprint: 10.0.90.215-49204 - Windows XP/2000 (RFC1323+, w*, timestamp) [GENERIC]
OS Fingerprint: 0192:128:152:152:15460:NWBN,N,S, -Windows??
OS Fingerprint: -> 209.141.34.8:90 [instance 0, link: ethernet/modem]

SRC: GET /test1.css HTTP/1.1
SRC: Accept: "text/css, application/javascript, application/json, application/xml, */*"
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
SRC: Host: 209.141.34.8
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 19 Mar 2019 01:45:55 GMT
DST: Server: Apache/2.4.6 (CentOS)
DST: Last-Modified: Mon, 18 Mar 2019 22:00:46 GMT
DST: ETag: "cd209-5b4656544ff90"
DST: Accept-Ranges: bytes
DST: Content-Length: 811520
DST: Keep-Alive: timeout=5, max=100
DST: Connection: Keep-Alive

Search Abort Close
Debug Messages
```

De la transcripción responda las siguientes preguntas.

¿Cuáles son las direcciones MAC e IP y los números de puerto de origen y de destino?

Mirando la solicitud (azul) ¿para qué fue la solicitud?

Al mirar la respuesta (roja), muchos archivos revelarán su firma en los primeros caracteres del archivo cuando se vean como texto. Las firmas de archivo ayudan a identificar el tipo de archivo que se representa. Utilice un explorador web para buscar una lista de firmas de archivo comunes.

¿Cuáles son los primeros caracteres del archivo? ¿Busca esta firma de archivo para averiguar qué tipo de archivo se ha descargado en los datos?

- c. Cierre la transcripción. Utilice Wireshark para exportar el archivo ejecutable para el análisis de malware (**Archivo > Exportar objetos > HTTP...**). Guarde el archivo en la carpeta principal del analista.
- d. Abra un terminal en Security Onion VM y cree un hash SHA256 desde el archivo exportado. Use el siguiente comando:

```
analyst @SecOnion: ~$ sha256sum test1.exe  
2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85 test1.exe
```

- e. Copie el hash del archivo y envíelo al centro de reputación de archivos Talos de Cisco en https://talosintelligence.com/talos_file_reputation.



¿Reconoció Talos el hash del archivo y lo identificó como malware? Si es así, ¿qué tipo de malware?

- f. En Sguil, seleccione la alerta con **Alert ID 5.480** y el **Event Message** Remcos RAT Checkin 23. Observe que la firma IDS ha detectado la RAT Remcos basada en los códigos hexadecimales binarios al comienzo de la comunicación.

L	S	D	T	P	C	Protocol
8	80	10.0.90.215	49204	6	ET POLICY PE EXE or DLL Windows file download HTTP	
5	49205	103.1.184.108	2404	6	ET TROJAN Remcos RAT Checkin 23	
5	49206	217.23.14.81	80	6	ET CURRENT EVENTS Terse alphanumeric executable dow...	

Show Packet Data		Show Rule										
<pre>alert tcp \$HOME_NET any -> \$EXTERNAL_NET any (msg:"ET TROJAN Remcos RAT Checkin 23"; flow.established_to_server, dsizer<=500; content:"[1b 84 d5 b0 5d f4 c4 93 c5 39 c2]"; depth:11; fast_pattern; content:"[da b1]"; distance:2; within:2; threshold.type limit, seconds:30, count:1, track_by_src; metadata: former_category TROJAN; reference:md5,14f2425e9735f92cc9f7571aa8cb210; classtype:trojan-activity; sid:2025637;</pre>												
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum	
	10.0.90.215	103.1.184.108	4	5	0	160	613	2	0	128	29614	
TCP	Source	Dest	U	A	P	R	S	F				
	Port	Port	R	R	R	C	S	Y	I			
	19205	2404	.	.	X	X	.	.				
DATA	Seq #								Ack #	Offset	Res	
										Res	Window	Up
	1B 84 D5 B0 5D F4 C4 93 C5 39 C2	C6	B0	DA	B1 D8	.	.	.	1150900601	5	0	64213
	AC AF 6E 7F F8 10 18 23 33 8E D8 54 53 91 AA 53
	DB FF 93 6F B0 73 AF 72 36 49 AD 18 72 29 98 AD
	77 D9 10 6C 3E 32 A0 E9 12 18 7E A8 DD A0 9E 60

Search Packet Payload		Hex		Text		NoCase	

- g. Haga clic con el botón derecho en el ID de alerta 5.440 y seleccione **Transcript**. Desplácese por la transcripción y responda a las siguientes preguntas:

¿Cuál es el puerto de destino de la comunicación? ¿Es este un puerto conocido?

¿Es legible la comunicación o está encriptada?

Haga algunas investigaciones en línea sobre Remcos RAT Checkin 23. ¿Qué hace Remcos?

¿Qué tipo de comunicación crees que se estaba transmitiendo?

¿Qué tipo de encriptación y ofuscación se usó para eludir la detección?

- h. Usando Sguil y las alertas restantes del 3-19-2019, localice el segundo archivo ejecutable que se descargó y compruebe si se trata de malware conocido.

¿Qué ID alerta a un segundo archivo ejecutable que se está descargando?

¿Desde qué dirección IP del servidor y número de puerto se descargó el archivo?

¿Cuál es el nombre del archivo que se ha descargado?

Cree un hash SHA256 del archivo y envíe el hash en línea en el Centro de Reputación de Archivos de Talos de Cisco para ver si coincide con el malware conocido. ¿Es el archivo ejecutable malware conocido y, en caso afirmativo, de qué tipo? ¿Cuáles es el nombre de la detección de AMP?

- i. Examine las tres alertas restantes del 3-19-2019 mirando la información del encabezado en Mostrar datos del paquete, la firma IDS en Mostrar regla y las transcripciones de ID de alerta.

¿Cómo se relacionan las tres alertas?

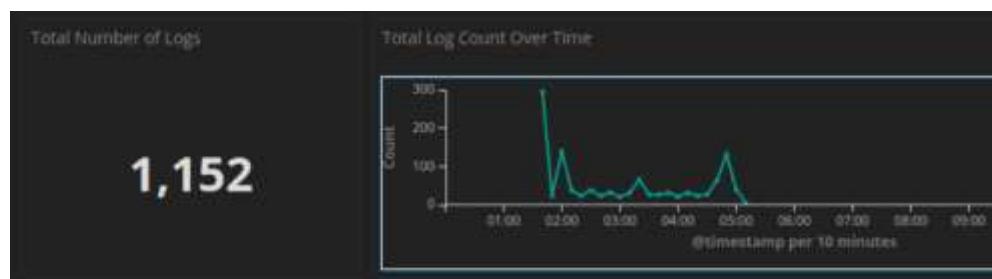
- j. Aunque ha examinado todas las alertas de Sguil relacionadas con un ataque a un host de Windows el 3-19-2019, puede haber información relacionada adicional disponible en Kibana. Cierre Sguil e inicie Kibana desde el escritorio.

Parte 2: Usar Kibana para investigar alertas

En la Parte 2, use Kibana para investigar más a fondo el ataque del 3-19-2019.

Paso 1: Abre Kibana y reduce el plazo.

- a. Inicie sesión en Kibana VM con el nombre de usuario **analyst** y la contraseña **ciberops**
- b. Abra Kibana (**analyst** de nombre de usuario y **ciberops** de contraseña), haga clic en **Últimas 24 horas** y en la pestaña Intervalo de tiempo **absoluto** para cambiar el intervalo de tiempo al 1 de marzo de 2019 al 31 de marzo de 2019.
- c. La línea de tiempo **Recuento total de registros** a lo largo del tiempo mostrará un evento el 19 de marzo. Haga clic en ese evento para limitar el enfoque al intervalo de tiempo específico del ataque.



Paso 2: Revise las alertas en el marco de tiempo reducido.

- En el panel de control de Kibana, desplácese hacia abajo hasta la visualización **Todos los sensores - Tipo de registro**. Revise ambas páginas y tenga en cuenta la variedad de tipos de registro relacionados con este ataque.

Log Type(s)	Count
snort	541
bro_conn	271
bro_dns	85
bro_dce_rpc	51
bro_kerberos	50
bro_files	35
bro_smb_mapping	29
bro_ssl	29
bro_x509	25
bro_dhcp	8

Log Type(s)	Count
bro_weird	8
bro_notice	7
bro_smb_files	7
bro_http	4
bro_pe	2

- Desplácese hacia abajo y observe que el Resumen de Alertas de NIDS en Kibana tiene muchas de las mismas alertas de IDS que aparecen en Sguil. Haga clic en la lupa para filtrar en la segunda alerta ET TROJAN ABUSE.CH SSL Lista negra Certificado SSL malintencionado detectado (Dridex) de la dirección IP de origen 31.22.4.176.

Alert	Source IP Address	Destination IP Address	Count
ET TROJAN Remcos RAT Checkin 23	10.0.90.215	103.1.184.108	404
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	31.22.4.176	10.0.90.215	16
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	203.45.1.75	10.0.90.215	13
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	115.112.43.81	10.0.90.215	3
ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2	209.141.34.8	10.0.90.215	12
ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2	217.23.14.81	10.0.90.215	12
ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referrer from HFS webserver (used by Unknown EK)	217.23.14.81	10.0.90.215	12
ET INFO EXE - Served Attached HTTP	217.23.14.81	10.0.90.215	12

Laboratorio - Investigación de un ataque en un host de Windows

- c. Desplácese hacia abajo hasta Todos los registros y haga clic en la flecha para expandir el primer registro de la lista con la dirección IP de origen 31.22.4.176.

All Logs					
Time	source_ip	source_port	destination_ip	destination_port	Limited to 10 results
▶ March 19th 2019, 04:55:13.000	115.112.43.81	443	10.0.90.215	49280	
▶ March 19th 2019, 04:54:57.000	115.112.43.81	443	10.0.90.215	49295	
▶ March 19th 2019, 04:54:34.000	115.112.43.81	443	10.0.90.215	49282	
▶ March 19th 2019, 04:50:21.000	31.22.4.176	3389	10.0.90.215	49281	
▶ March 19th 2019, 04:50:21.000	31.22.4.176	3389	10.0.90.215	49281	
▶ March 19th 2019, 04:50:15.000	31.22.4.176	3389	10.0.90.215	49280	
▶ March 19th 2019, 04:50:15.000	31.22.4.176	3389	10.0.90.215	49280	

¿Cuál es el geopáis y la ubicación de la ciudad para esta alerta?

¿Cuál es el país y la ciudad geográficos para la alerta de 115.112.43.81?

- d. Desplácese hacia atrás hasta la parte superior de la página y haga clic en el enlace Inicio en Navegación.
- e. Anteriormente notamos tipos de registro como bro_http enumerados en el panel de inicio. Puede filtrar por los distintos tipos de registro, pero los paneles integrados probablemente tendrán más información. Desplácese hacia atrás a la parte superior de la página y haga clic en **HTTP** en el enlace del panel bajo Zeek Hunting in Navigation.

Zeek Hunting	
Connections	
DCE/RPC	
DHCP	
DNP3	
DNS	
Files	
FTP	
HTTP	
Intel	
IRC	
Kerberos	
Modbus	
MySQL	

All Sensors - Log Type

Log Type(s)	Count
snort	32

- f. Desplácese por el panel HTTP tomando nota de la información presentada y responda a las siguientes preguntas:

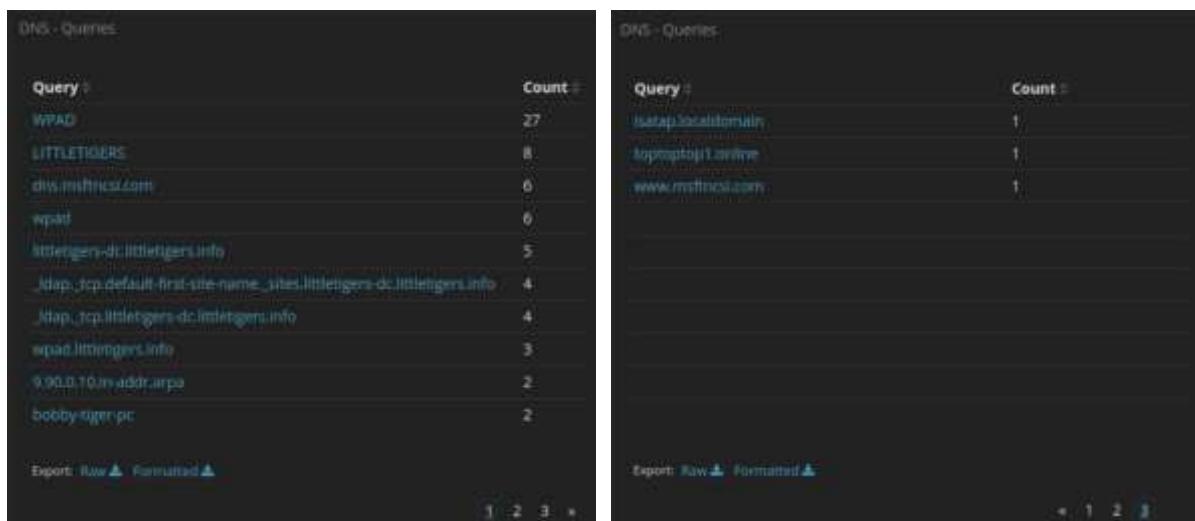
¿Qué es el recuento de registros en el panel HTTP? ¿De qué países?

¿Cuáles son los URI de los archivos descargados?

- g. Haga coincidir los **URI HTTP** con los **sitios HTTP** - en el panel de control.

¿A qué están relacionados los archivos CSPCA.crl y ncsi.txt? Utilice un navegador web y un motor de búsqueda para obtener información adicional.

- h. Desplácese hacia atrás hasta la parte superior de la página web y en Navegación - Zeek Hunting haga clic en **DNS**. Desplácese hasta la visualización de consultas DNS. Observe la página 1 y página 3 de las consultas DNS.



¿Alguno de los dominios parece potencialmente inseguro? Intente enviar la URL toptoptop1.online a virustotal.com. ¿Cuál es el resultado?

- i. Para más investigación, intente examinar los siguientes paneles de Zeek Hunting:
- DCE/RPC: para obtener información sobre los procedimientos remotos de la red de Windows y los recursos involucrados
 - Kerberos: para obtener información sobre los nombres de host y los nombres de dominio que se utilizaron
 - PE: para obtener información sobre los ejecutables portátiles

Laboratorio - Investigación de un ataque en un host de Windows

SSL y x.509: para obtener información sobre los nombres de los certificados de seguridad y los países que se utilizaron

SMB : para obtener más información sobre las acciones de SMB en la red de littletigers

Weird: para anomalías de protocolo y servicio y comunicaciones mal formadas