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.

a. 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 pivote 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?

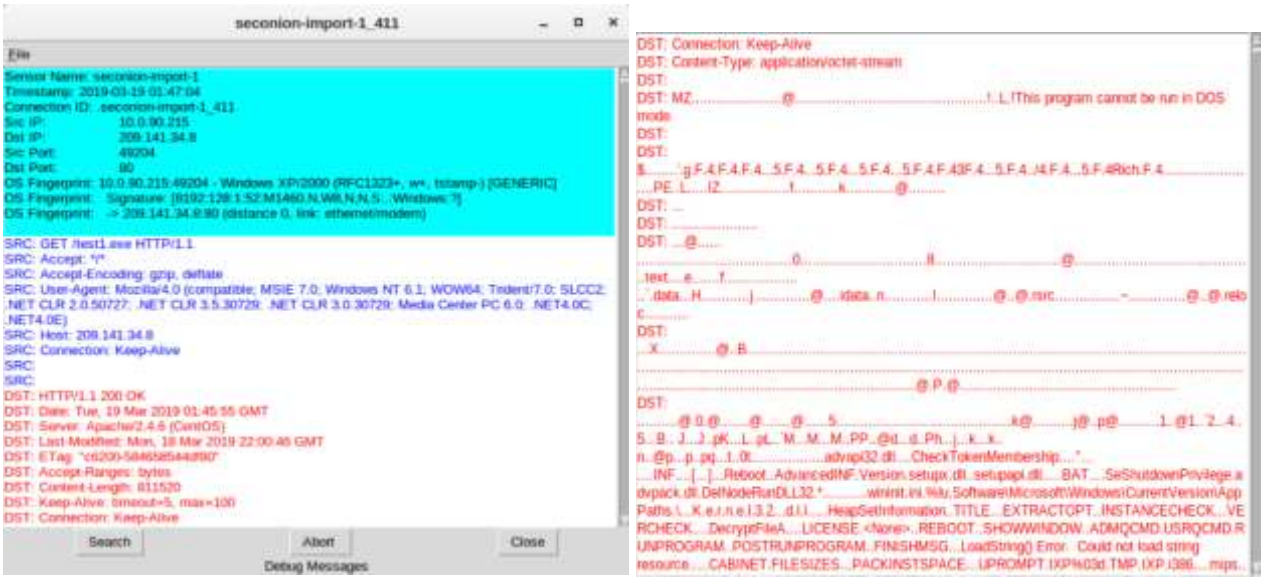
¿Qué tipo de protocolo y solicitud o respuesta estuvo involucrado?

¿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?

b. 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**.



De la trasncripción 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.

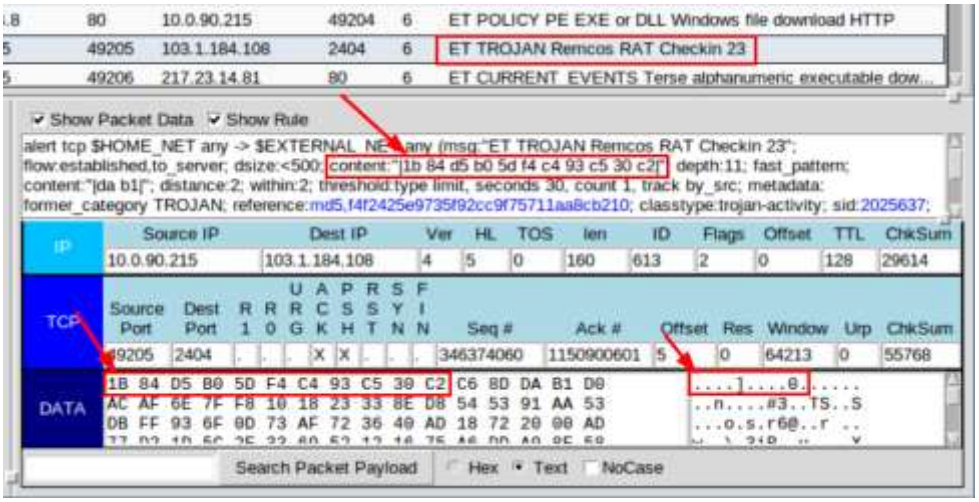
d. Abra un terminal en Security Onion VM y cree un hash SHA256 desde el archivo exportado. Use el siguiente comando:

```
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.



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 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.

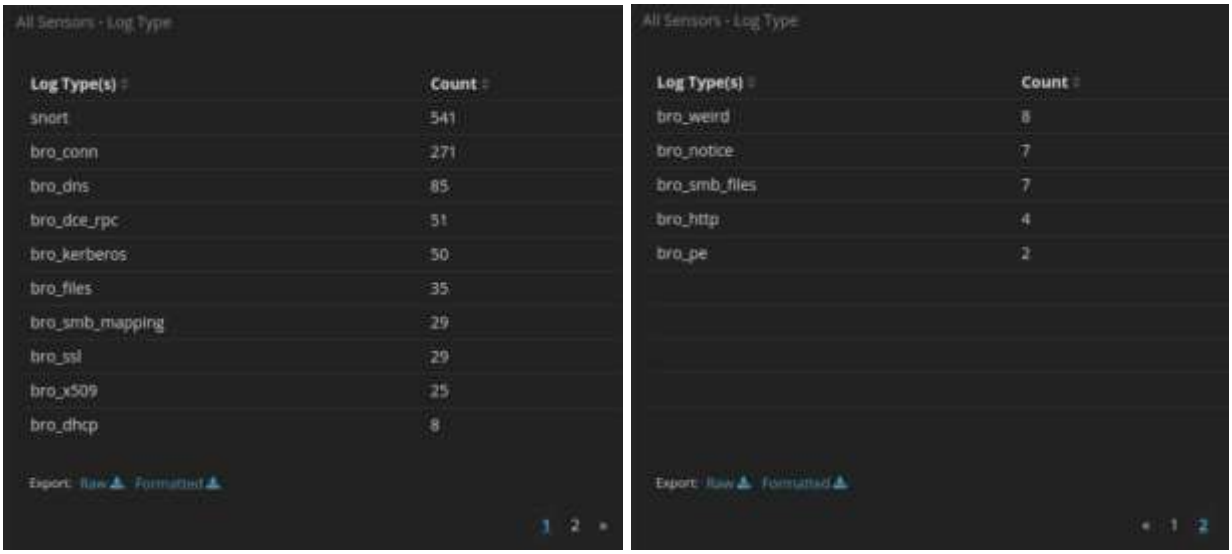
a. Inicie sesión en Kibana VM con el nombre de usuario **analyst** y la contraseña **cyberops**

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.

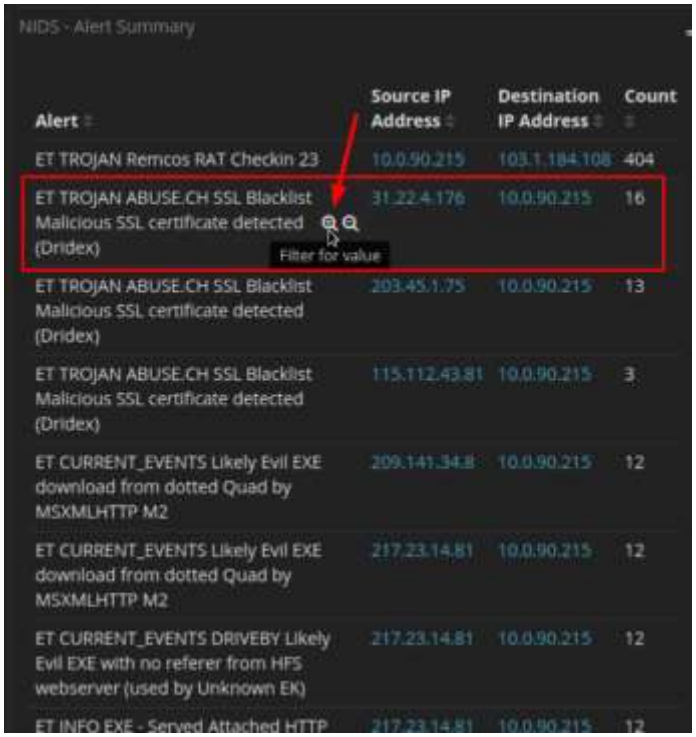
c. La línea de tiempo **Recuento total de registros** a lo largo del tiempo mostrará un evento el 19 de marzo. Haga clic en ese evento para limitar el enfoque al intervalo de tiempo específico del ataque.

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

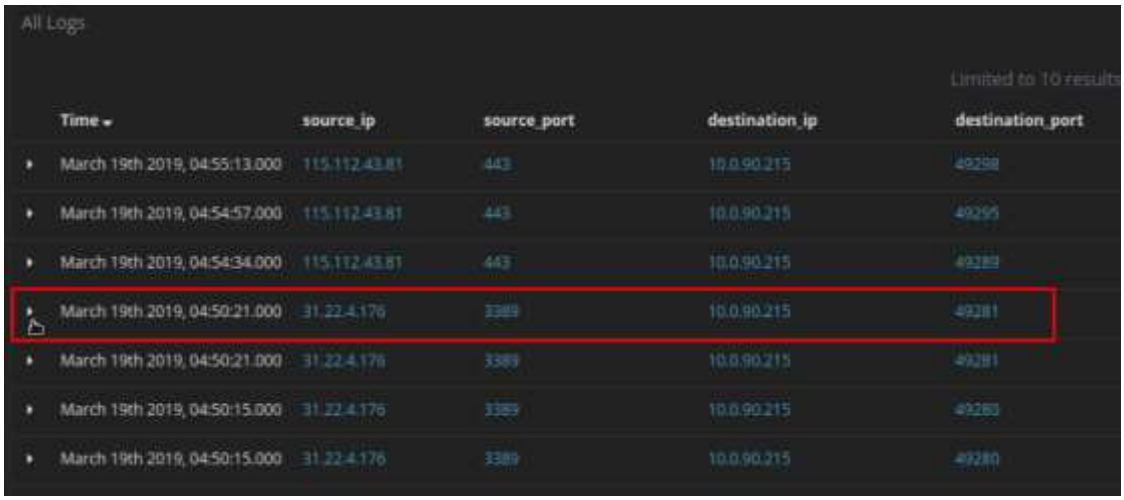
a. En el panel de control de Kibana, desplácese hacia abajo hasta la visualización **Todos los sensores - Tipo de registro**. Revise ambas páginas y tenga en cuenta la variedad de tipos de registro relacionados con este ataque.



b. 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.



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.



¿Cuál es el geopaís 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.

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

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