­

1. **Information Security**
2. **Chapter 12: Digital Forensics and Incident Analysis and Response**
4. Lab 42 - Investigating an Attack on a Windows Host

# Objectives

In this lab you will:

Part 1: Investigate the Attack with Sguil.

Part 2: Use Kibana to Investigate Alerts.

This lab is based on an exercise from the website malware-traffic-analysis.net which is an excellent resource for learning how to analyze network and host attacks. Thanks to brad@malware-traffic-analysis.net for permission to use materials from his site.

**Note**: This lab requires a host computer that can access the internet.

# Background / Scenario

In March 2019, network security monitoring tools alerted that a Windows computer on the network was infected with malware. In this task, you are to investigate the alerts and answer the following questions:

* What was the specific time of the attack on 2019-03-19?
* Which Windows host computer was infected? Who was the user?
* What was the computer infected with?

# Required Resources

* Security Onion virtual machine
* Internet access

# Instructions

## Investigate the Attack with Sguil

In Part 1, you will use Sguil to check the IDS alerts and gather more information about the series of events related to an attack on 3-19-2019.

**Note**: The alert IDs used in this lab are for example only. The alert IDs on your VM may be different.

### Open Sguil and locate the alerts on 3-19-2019.

* + - 1. Login to Security Onion VM with the **analyst** username and **cyberops** password.
      2. Launch Sguil from the desktop. Login with username **analyst** and password **cyberops**. Click **Select All** and **Start Sguil** to view all the alerts generated by the network sensors.
      3. Locate the group of alerts from 19 March 2019.

#### Question:

According to Sguil, what are the timestamps for the first and last of the alerts that occurred on 3-19-2019? What is interesting about the timestamps of all the alerts on 3-19-2019?

***Ans:***

Start: 3-19-2019 01:45:03

End: 3-19-2019 04:54:54

It is interesting that the most of the attacks are done in just the initial 5 minutes and the last attack took more time.

### Review the alerts in detail.

* + - 1. In Sguil, click the first of the alerts on 3-19-2019 (Alert ID 5.439). Make sure to check the **Show Packet Data** and **Show Rule** checkboxes to examine the packet header information and the IDS signature rule related to the alert. Right on the **Alert ID** and pivot to Wireshark. Based on the information derived from this initial alert answer the following questions:

#### Questions:

What was the source IP address and port number and destination IP address and port number?

***Ans:*** SRC IP: 10.0.90.215 PORT: 52609

DST: 10.0.90.9 PORT: 53

What type of protocol and request or response was involved?

***Ans:*** DNS and UNDP

What is the IDS alert and message?

***Ans:***

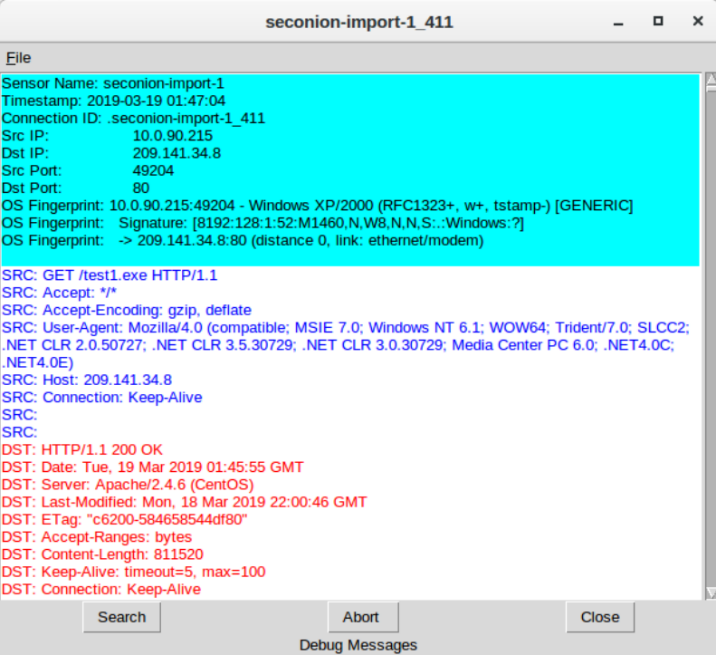
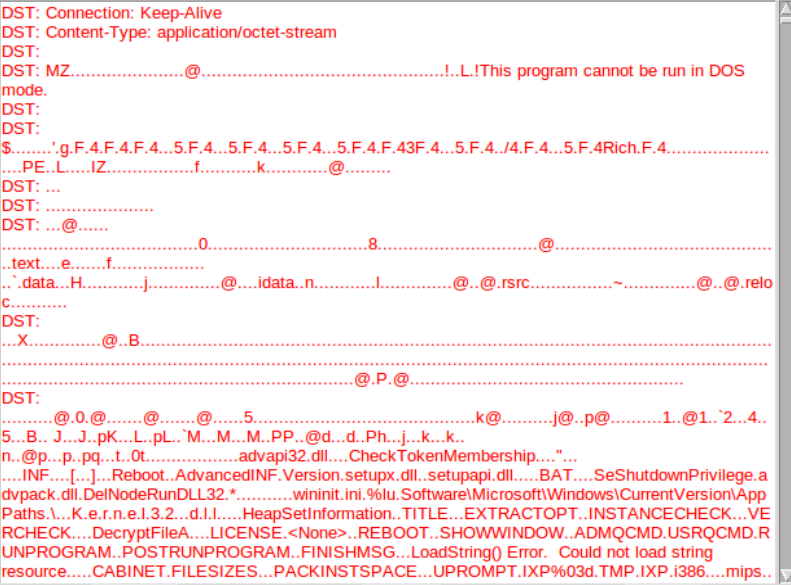
Do you think this alert was the result of an IDS misconfiguration or a legitimate suspicious communication?

***Type your answers here.***

What is the hostname, domain name, and IP address of the source host in the DNS update?

***Type your answers here.***

* + - 1. In Sguil, select the second of the alerts on 3-19-2019. Right click the Alert ID 5.440 and select **Transcript**.

From the transcript answer the following questions:

#### Questions:

What is the source and destination IP address and port numbers?

***Type your answers here.***

Looking at the request (blue) what was the request for?

***Type your answers here.***

Looking at the reply (red) many files will reveal their file signature in the initial few characters of the file when viewed as text. File signatures help identify the type of file that is represented. Use a web browser to search for a list of common file signatures.

#### Question:

What is the initial few characters of the file file. Search for this file signature to find out what type of file was downloaded in the data?

***Type your answers here.***

* + - 1. Close the transcript. Use Wireshark to export the executable file for malware analysis (**File** > **Export Objects** > **HTTP…**). Save the file to the analyst's home folder.
      2. Open a terminal in Security Onion VM and create a SHA256 hash from the exported file. Use the following command:

analyst@SecOnion:~$ **sha256sum test1.exe**

**2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85** test1.exe

* + - 1. Copy the file hash and submit it to the Cisco Talos file reputation center at <https://talosintelligence.com/talos_file_reputation>.

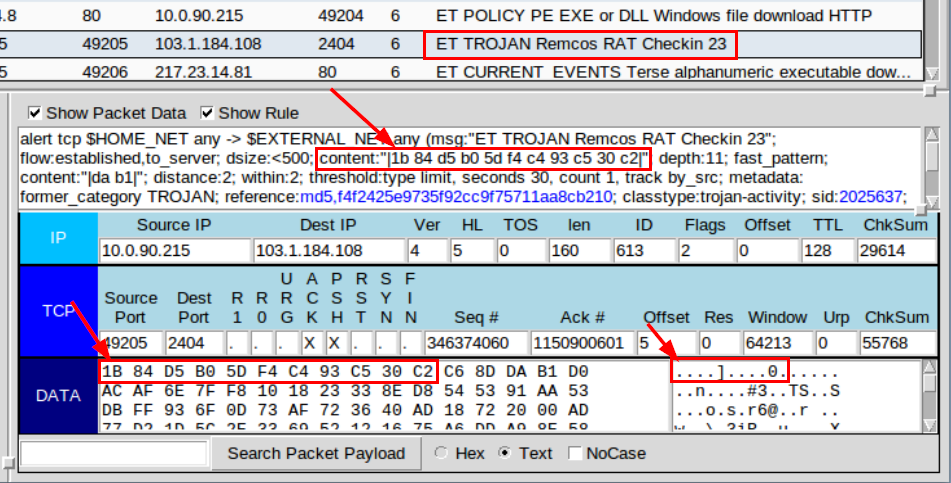


#### Question:

Did Talos recognize the file hash and identify it as malware? If so, what kind of malware?

***Type your answers here.***

* + - 1. In Sguil select the alert with **Alert ID** **5.480** and the **Event Message** Remcos RAT Checkin 23. Notice that the IDS signature has detected the Remcos RAT based on the binary hex codes at the beginning of communication.



* + - 1. Right click the Alert ID and select **Transcript**. Scroll through the transcript and answer the following questions:

#### Questions:

What is the destination port of the communication? Is it a well-known port?

***Type your answers here.***

Is the communication readable or is it encrypted?

***Type your answers here.***

Do some online research on Remcos RAT Checkin 23. What does Remcos stand for?

***Type your answers here.***

What type of communication do you think was being transmitted?

***Type your answers here.***

What type of encryption and obfuscation was used to bypass detection?

***Type your answers here.***

* + - 1. Using Sguil and the remaining alerts from 3-19-2019, locate the second executable file that was downloaded and check to see if it is known malware.

#### Questions:

What Alert IDs alert to a second executable file being downloaded?

***Type your answers here.***

From which server IP address and port number was the file downloaded from?

***Type your answers here.***

What is the name of the file that was downloaded?

***Type your answers here.***

Create a SHA256 hash of the file and submit the hash online at Cisco Talos File Reputation Center to see if it matches known malware. Is the executable file known malware and if so, what type? What is the AMP DETECTION NAME?

***Type your answers here.***

* + - 1. Examine the remaining three alerts from 3-19-2019 by looking at the header information in Show Packet Data, the IDS signature in Show Rule, and the Alert ID Transcripts.

#### Question:

How are all three alerts related?

***Type your answers here.***

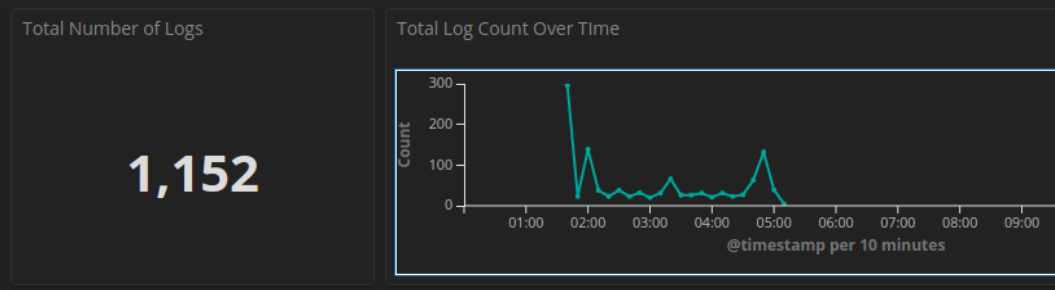
* + - 1. Even though you have examined all the alerts in Sguil related to an attack on a Windows host on 3-19-2019, there may be additional related information available in Kibana. Close Sguil and launch Kibana from the desktop.

## Use Kibana to Investigate Alerts

In Part 2, use Kibana to further investigate the attack on 3-19-2019.

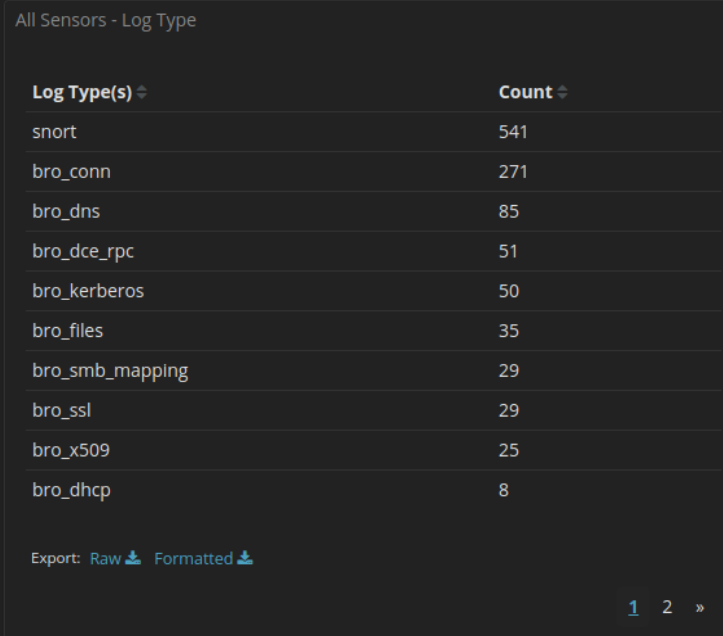
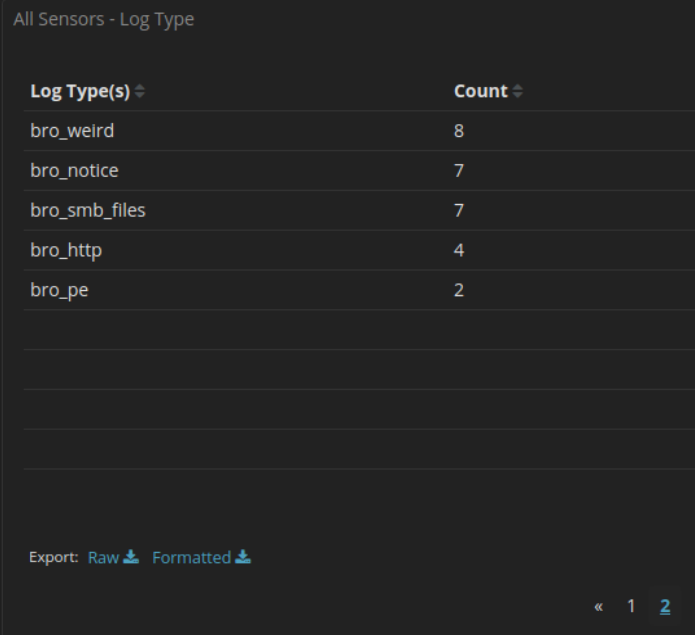
### Open Kibana and narrow the timeframe.

* + - 1. Login to Kibana with the **analyst** username and **cyberops** password.
      2. Open Kibana (username **analyst** and password **cyberops**), click **Last 24 Hours** and the **Absolute** time range tab to change the time range to March 1, 2019 to March 31, 2019.
      3. The **Total Log Count Over Time** timeline will show an event on March 19. Click that event to narrow the focus to the specific time range of the attack.

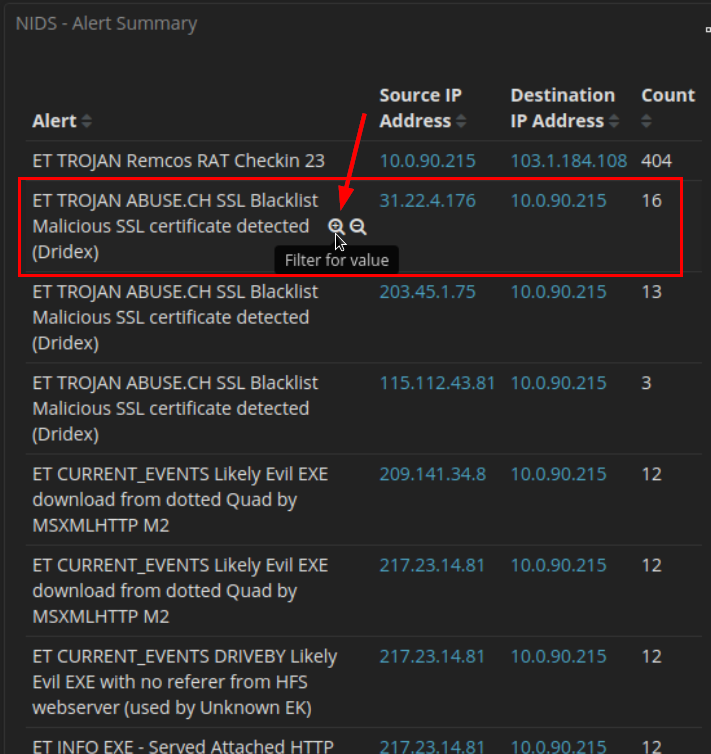


### Review the alerts in the narrowed timeframe.

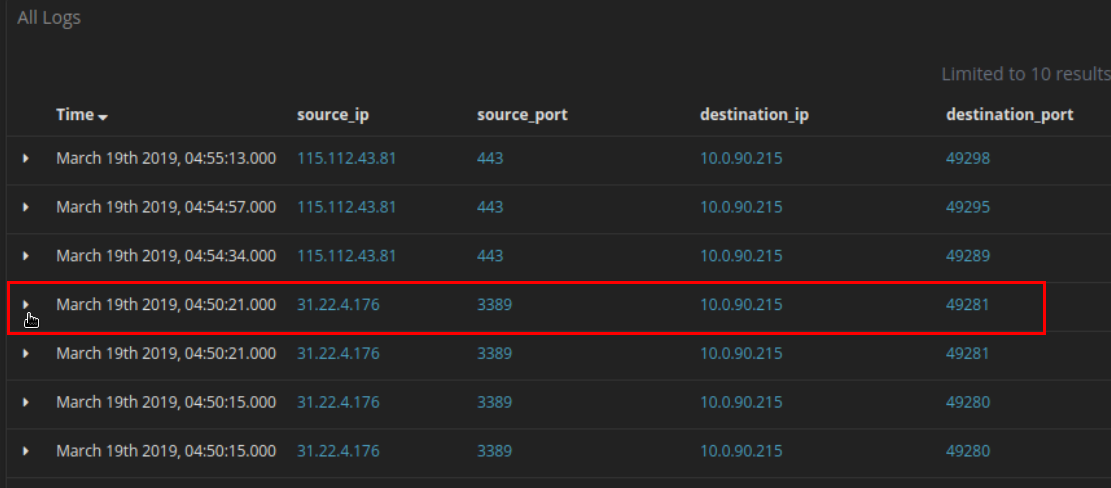
* + - 1. In the Kibana dashboard scroll down to the **All Sensors - Log Type** visualization. Review both pages and note the variety of log types related to this attack.

* + - 1. Scroll down and notice that the NIDS Alert Summary in Kibana has many of the same IDS alerts as listed in Sguil. Click the magnifier to filter on the second alert ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) from Source IP Address 31.22.4.176.



* + - 1. Scroll down to All Logs and click the arrow to expand the first log in the list with source IP address 31.22.4.176.



#### Questions:

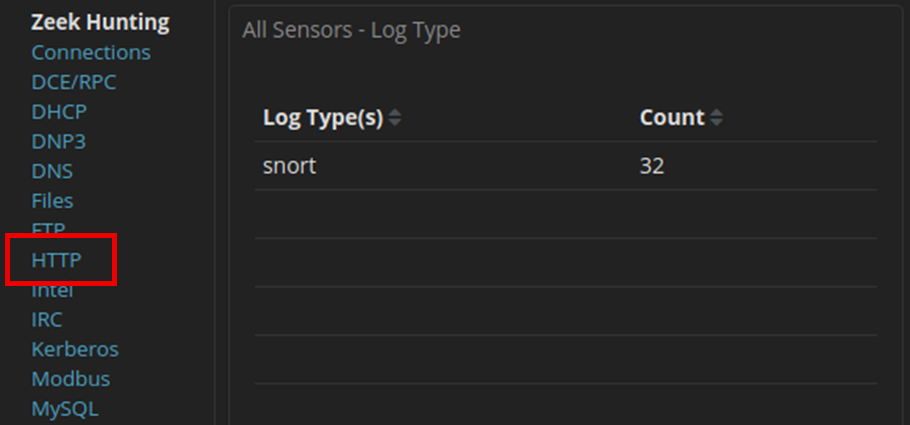
What is the geo country and city location for this alert?

***Type your answers here.***

What is the geo country and city for the alert from 115.112.43.81?

***Type your answers here.***

* + - 1. Scroll back to the top of the page and click the Home link under Navigation.
      2. Earlier we noted log types like bro\_http listed in the Home dashboard. You can filter for the various log type but the built-in dashboards will probably have more information. Scroll back to the top of the page and click **HTTP** in dashboard link under Zeek Hunting in Navigation.



* + - 1. Scroll through the HTTP dashboard taking notice of the information presented and answer the following questions:

#### Questions:

What is the Log Count in the HTTP dashboard? From what countries?

***Type your answers here.***

What are the URIs for the files that were downloaded?

***Type your answers here.***

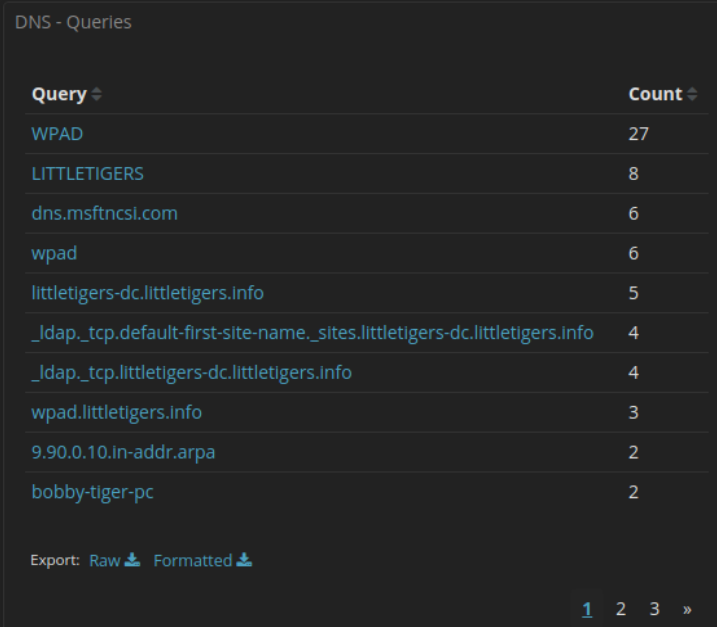
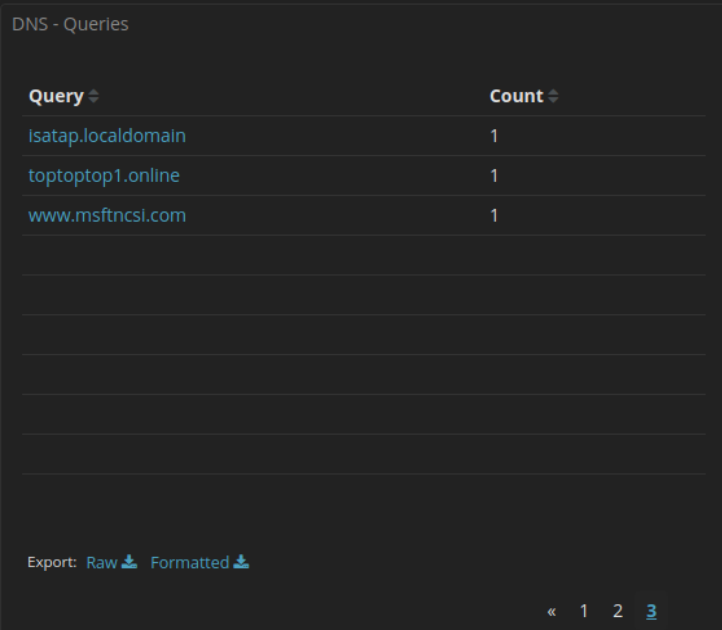
* + - 1. Match the **HTTP - URIs** to the **HTTP - Sites** on the dashboard.

#### Question:

What are the CSPCA.crl and ncsi.txt files related to? Use a web browser and a search engine for additional information.

***Type your answers here.***

* + - 1. Scroll back to the top of the web page and under Navigation - Zeek Hunting click **DNS**. Scroll to the DNS Queries visualization. Notice page 1 and page 3 of the DNS queries.

Do any of the domains seem potentially unsafe? Try submitting the URL toptoptop1.online to virustotal.com. What is the result?

***Type your answers here.***

* + - 1. For further investigation and curiosity, try examining the following Zeek Hunting dashboards:

DCE/RPC - for information about the Windows network remote procedures and resources involved

Kerberos – for information on the hostnames, and domain names that were used

PE – for information on the portable executables

SSL and x.509 – for information on the security certificate names and countries that were used

SMB – for more information on the SMB shares on the littletigers network

Weird – for protocol and service anomalies and malformed communications