



## **Lab - Investigating an Attack on a Windows Host**

## Lab - 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](http://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](mailto:brad@malware-traffic-analysis.net) for permission to use materials from his site.

### 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

#### Part 1: 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.

#### Step 1: Open Sguil and locate the alerts on 3-19-2019.

- a. Login to Security Onion VM with the **analyst** username and **cyberops** password.
- b. 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.
- c. Locate the group of alerts from 19 March 2019.

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?

**Answer: 2019-03-19 01:45:03 - 2019-03-19 04:54:34**

**The first alert occurred at 2019-03-19 01:45:03, and the last alert was at 2019-03-19 04:54:34. The initial alerts happened rapidly within 12 seconds, suggesting a coordinated attack, followed by a long gap of over 3 hours before the final alert, indicating potential persistence or delayed malicious activity.**

### Step 2: Review the alerts in detail.

- a. 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:

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

- **Source IP Address:** 10.0.90.215
- **Source Port:** 52609
- **Destination IP Address:** 10.0.90.9
- **Destination Port:** 53

What type of protocol and request or response was involved?

- **Protocol:** UDP
- **Request/Response:** This is a **DNS request** from the source IP to the destination IP (DNS server).

What is the IDS alert and message?

**Alert udp \$EXTERNAL\_NET any -> \$HOME\_NET 53, msg: "ET POLICY DNS Update from External net"**

- **Alert:** ET POLICY DNS Update From External net
- **Message:** The alert indicates a DNS update request originating from an external network, which could be suspicious if the source is not authorized to make DNS updates.

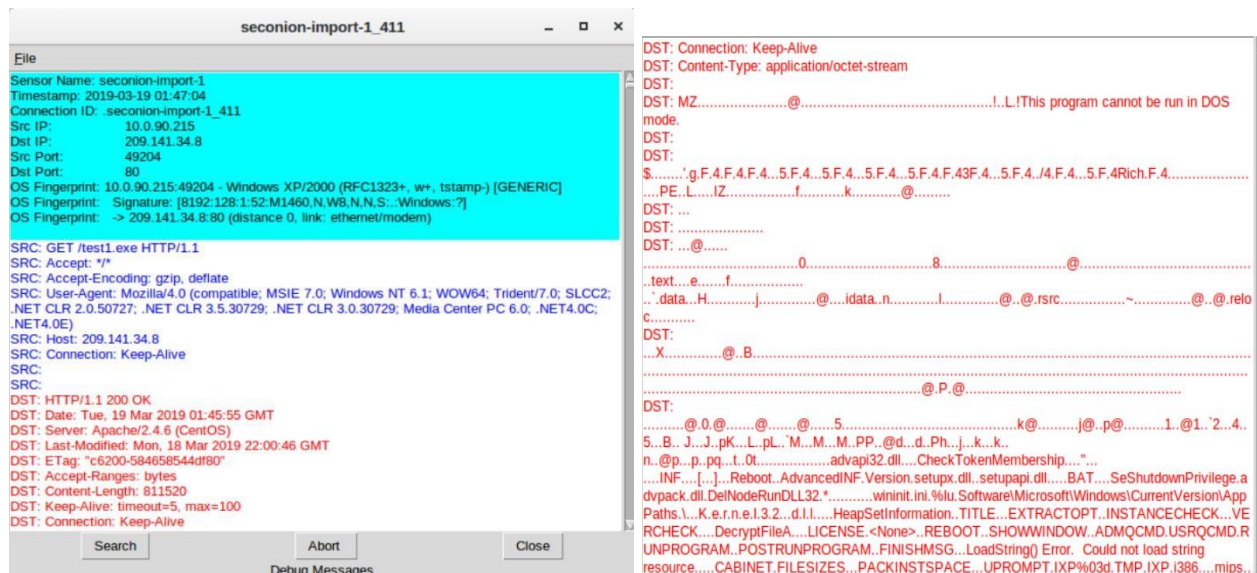
Do you think this alert was the result of an IDS misconfiguration or a legitimate suspicious communication?

**This alert may be the result of a misconfiguration in the IDS because the DNS request was a Dynamic DNS update from an internal host to a DNS server on the internal network and not from an external network to the internal network.**

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

**Bobby-Tiger-PC, littletigers.info, 10.0.90.215**

- b. 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:

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

- **Source IP Address:** 10.0.90.215
- **Source Port:** 49204
- **Destination IP Address:** 209.141.34.8
- **Destination Port:** 80

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

The request was for: **GET /testL.exe HTTP/1.1**

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.

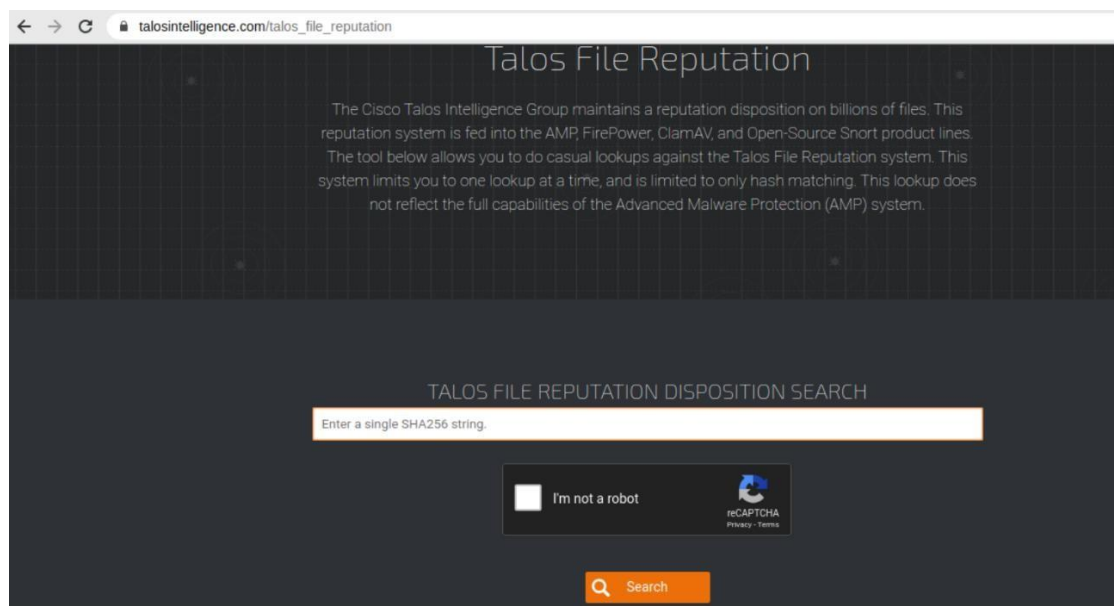
What is the initial few characters of the file file. Search for this file signature to find out what type of file was downloaded in the data?

- **File Signature:** MZ
- **File Type:** Windows Executable (EXE)
- The MZ signature is the **DOS header** found at the beginning of Windows executable files (.exe or .dll). It indicates that the downloaded file (testL.exe) is a Windows executable.

## Lab - Investigating an Attack on a Windows Host

- 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.
- Open a terminal in Security Onion VM and create a SHA256 hash from the exported file. Use the following command:  

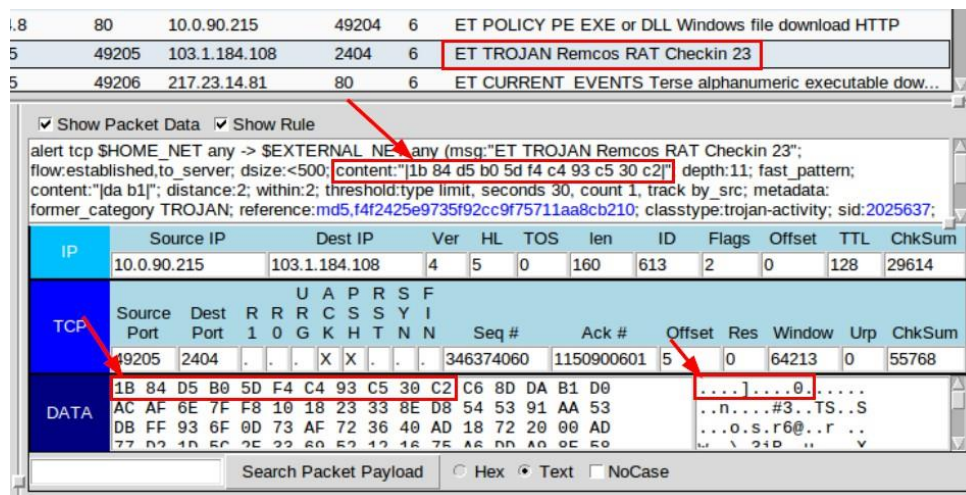
```
analyst@SecOnion:~$ sha256sum test1.exe
2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85 test1.exe
```
- Copy the file hash and submit it to the Cisco Talos file reputation center at [https://talosintelligence.com/talos\\_file\\_reputation](https://talosintelligence.com/talos_file_reputation).



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

**Yes, TROJAN**

- 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.



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

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

- **Destination Port:** 2404
- **Well-Known Port:** No, port 2404 is not a well-known port. Well-known ports typically range from 0 to 1023, and port 2404 is not associated with any standard service.

Is the communication readable or is it encrypted?

- **Encrypted:** The communication appears to be **encrypted** or **obfuscated**. The data in the transcript is not human-readable and consists of seemingly random characters, which is typical of encrypted or obfuscated traffic.

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

- **Remcos:** Remcos stands for **Remote Control and Surveillance Software**. It is a **Remote Access Trojan (RAT)** that allows attackers to gain full control over a compromised system. It is often used for espionage, data theft, and unauthorized surveillance.

What type of communication do you think was being transmitted?

The communication is likely a **command-and-control (C2) check-in** from the Remcos RAT to its C2 server. This type of communication is used by malware to receive instructions from the attacker or to exfiltrate data.

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

- **Encryption:** Remcos RAT typically uses **AES encryption** to secure its communications.
- **Obfuscation:** The traffic may also be obfuscated using techniques like **base64 encoding** or **custom encryption algorithms** to bypass detection by security tools.

- h. 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.

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

**ET INFO Packed Executable Download.**  
**This alert is triggered when a packed executable file (e.g., an EXE file) is downloaded.**

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

- **Server IP Address:** 217.23.14.81

- **Port Number: 80 (HTTP)**

What is the name of the file that was downloaded?

- **The downloaded file is named: 14.exe**

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?

**Yes, PE32 executable, trojan downloader Win.Dropper.Cridex::1201**

- i. 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.

How are all three alerts related?

- **All three alerts are classified as ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex).**
- **They involve malicious SSL certificates associated with the Dridex malware family.**
- **The destination IP (10.0.90.215) is consistent across all alerts, indicating that the same internal system is being targeted.**
- **The source IPs (31.22.4.176, 203.45.1.75, 115.112.43.81) are external and likely belong to command-and-control (C2) servers or malicious actors.**

- j. 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.

## Part 2: Use Kibana to Investigate Alerts

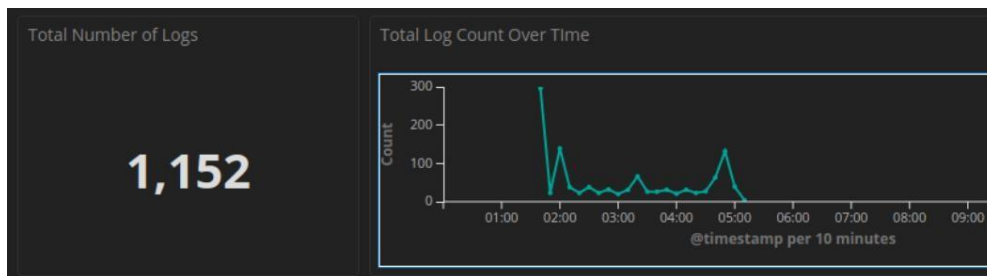
In Part 2, use Kibana to further investigate the attack on 3-19-2019.

### Step 1: Open Kibana and narrow the timeframe.

- a. Login to Kibana with the **analyst** username and **cyberops** password.
- b. 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.

## Lab - Investigating an Attack on a Windows Host

- c. 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.



### Step 2: Review the alerts in the narrowed timeframe.

- a. 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.

All Sensors - Log Type	
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

Export: [Raw](#) [Formatted](#)

1 2 »

All Sensors - Log Type	
Log Type(s) ▾	Count ▾
bro_weird	8
bro_notice	7
bro_smb_files	7
bro_http	4
bro_pe	2

Export: [Raw](#) [Formatted](#)

« 1 2



## Lab - Investigating an Attack on a Windows Host

- b. 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.

NIDS - Alert Summary

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 referer 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

- c. 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.

All Logs

Limited to 10 results

Time	source_ip	source_port	destination_ip	destination_port
▶ March 19th 2019, 04:55:13.000	115.112.43.81	443	10.0.90.215	49298
▶ 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	49289
▶ 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

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

**United Kingdom, Newcastle upon Tyne**

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

**India, Mumbai**

t	source_geo.city_name	🔍 🔍 📄 *	Mumbai
t	source_geo.country_name	🔍 🔍 📄 *	India
📄	source_geo.ip	🔍 🔍 📄 *	115.112.43.81

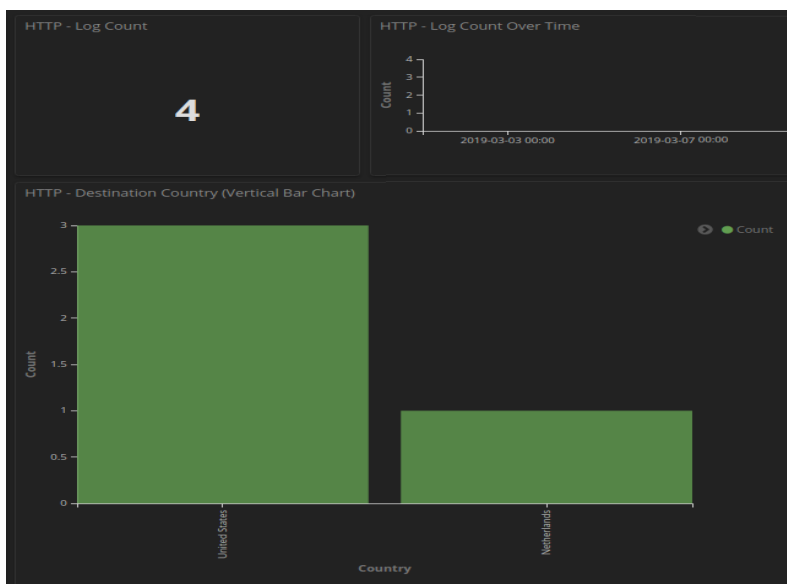
- Scroll back to the top of the page and click the Home link under Navigation.
- Earlier we noted log types like bro\_http listed in the Home dashboard. You can filter for the various log type but the built-in dashboards will probably have more information. Scroll back to the top of the page and click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

<b>Zeek Hunting</b> Connections DCE/RPC DHCP DNP3 DNS Files FTP <b>HTTP</b> Intel IRC Kerberos Modbus MySQL	All Sensors - Log Type  <table> <thead> <tr> <th>Log Type(s) ⚙</th><th>Count ⚙</th></tr> </thead> <tbody> <tr> <td>snort</td><td>32</td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </tbody> </table>	Log Type(s) ⚙	Count ⚙	snort	32										
Log Type(s) ⚙	Count ⚙														
snort	32														

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

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

**4 From USA and Netherlands**



What are the URIs for the files that were downloaded?

HTTP - URIs	
URI	Count
/f4.exe	1
/ncsi.txt	1
/pki/crl/products/CSPCA.crl	1
/test1.exe	1

- g. Match the **HTTP - URIs** to the **HTTP - Sites** on the dashboard.

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

**CSPCA.crl is a request for the Microsoft certificate revocation list and ncsi.txt refers to network connection status indicator and is used automatically by windows hosts as a self-test to verify online connectivity.**

- h. 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.


DNS - Queries	
Query	Count
WPAD	27
LITTLETIGERS	8
dns.msftncsi.com	6
wpad	6
littletigers-dc.littletigers.info	5
_ldap_tcp.default-first-site-name_sites.littletigers-dc.littletigers.info	4
_ldap_tcp.littletigers-dc.littletigers.info	4
wpad.littletigers.info	3
9.90.0.10.in-addr.arpa	2
bobby-tiger-pc	2
Export: Raw Formatted	
1 2 3 »	

DNS - Queries	
Query	Count
isatap.localdomain	1
toptoptop1.online	1
www.msftncsi.com	1
Export: Raw Formatted	
« 1 2 3	

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

Now No

## Lab - Investigating an Attack on a Windows Host

 toptoptop1.online

Did you intend to search across the file corpus instead? [Click here](#)

15  
/ 94

Community Score

1

15/94 security vendors flagged this domain as malicious

toptoptop1.online

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

alphaMountain.ai	Malicious	AlphaSOC	Malware
Antiy-AVL	Malicious	BitDefender	Phishing
CRDF	Malicious	CyRadar	Malicious
Dr.Web	Malicious	Fortinet	Malware
G-Data	Phishing	Lionic	Phishing