

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



This lab has been updated for use on NETLAB+.  
[www.netdevgroup.com](http://www.netdevgroup.com)

### 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?

### 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.

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

ST	CNT	Sensor	Alert ID	Date/Time	Δ	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	66	seconion-...	5.165	2018-08-11 05:...		192.168.1.95	50185	185.68.93.18	80	6	ET INFO GENERIC SUSPICIOUS POST to Dotted
RT	1	seconion-...	5.439	2019-03-19 01:...		10.0.90.215	52609	10.0.90.9	53	17	ET POLICY DNS Update From External net
RT	2	seconion-...	5.440	2019-03-19 01:...		10.0.90.215	49204	209.141.34.8	80	6	ET INFO Executable Download from dotted-quad Ho
RT	1	seconion-...	5.441	2019-03-19 01:...		10.0.90.215	49204	209.141.34.8	80	6	ET CURRENT_EVENTS Possible Malicious Macro I
RT	2	seconion-...	5.442	2019-03-19 01:...		209.141.34.8	80	10.0.90.215	49204	6	ET CURRENT_EVENTS Likely Evil EXE download f
RT	12	seconion-...	5.444	2019-03-19 01:...		209.141.34.8	80	10.0.90.215	49204	6	ET CURRENT_EVENTS Likely Evil EXE download f
RT	12	seconion-...	5.456	2019-03-19 01:...		209.141.34.8	80	10.0.90.215	49204	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Resp
RT	12	seconion-...	5.468	2019-03-19 01:...		209.141.34.8	80	10.0.90.215	49204	6	ET POLICY PE EXE or DLL Windows file download
RT	404	seconion-...	5.480	2019-03-19 01:...		10.0.90.215	49205	103.1.184.108	2404	6	ET TROJAN Remcos RAT Checkin 23
RT	1	seconion-...	5.482	2019-03-19 01:...		10.0.90.215	49206	217.23.14.81	80	6	ET CURRENT_EVENTS Terse alphanumeric execut
RT	2	seconion-...	5.483	2019-03-19 01:...		217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS Likely Evil EXE download f
RT	12	seconion-...	5.485	2019-03-19 01:...		217.23.14.81	80	10.0.90.215	49206	6	ET INFO EXE - Served Attached HTTP
RT	12	seconion-...	5.497	2019-03-19 01:...		217.23.14.81	80	10.0.90.215	49206	6	ET INFO Packed Executable Download
RT	12	seconion-...	5.509	2019-03-19 01:...		217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS DRIVEBY Likely Evil EXE
RT	12	seconion-...	5.521	2019-03-19 01:...		217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS Likely Evil EXE download f
RT	12	seconion-...	5.533	2019-03-19 01:...		217.23.14.81	80	10.0.90.215	49206	6	ET POLICY Terse Named Filename EXE Download
RT	16	seconion-...	5.571	2019-03-19 02:...		31.22.4.176	3389	10.0.90.215	49213	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious S
RT	13	seconion-...	5.589	2019-03-19 02:...		203.45.1.75	443	10.0.90.215	49218	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious S
RT	3	seconion-...	5.942	2019-03-19 04:...		115.112.43.81	443	10.0.90.215	49289	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious S
RT	3	seconion-...	5.1108	2019-04-15 16:...		10.0.90.175	55465	10.0.90.9	53	17	ET POLICY DNS Update From External net

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?

The alerts took place in 3 -19 -2019 for 3 hours since the first and last of the alert. the average of all the alert life span is around 3-4 minutes.

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

- 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 click on the **Alert ID** and pivot to Wireshark. Based on the information derived from this initial alert answer the following questions:

RT	1	seconion-...	5.439	2019-03-19 01
RT	2	seconion-...	Event History	1
RT	1	seconion-...	Transcript	1
RT	2	seconion-...	Transcript (force new)	1
RT	12	seconion-...	Wireshark	1
RT	12	seconion-...	Wireshark (force new)	1

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

10.0.90.9 at port 53 is the destination address and 10.0.90.9 at port 52609 is the source ip address

What type of protocol and request or response was involved?

UDP and DNS were the protocols and they used Dynamic Update Response

What is the IDS alert and message?

alert UDP \$EXTERNAL\_NET any -> \$HOME\_NET 53, msg: "ET POLICY DNS Update from external net."

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

since the request is from internal host as a DNS update to DNS server not from external source,

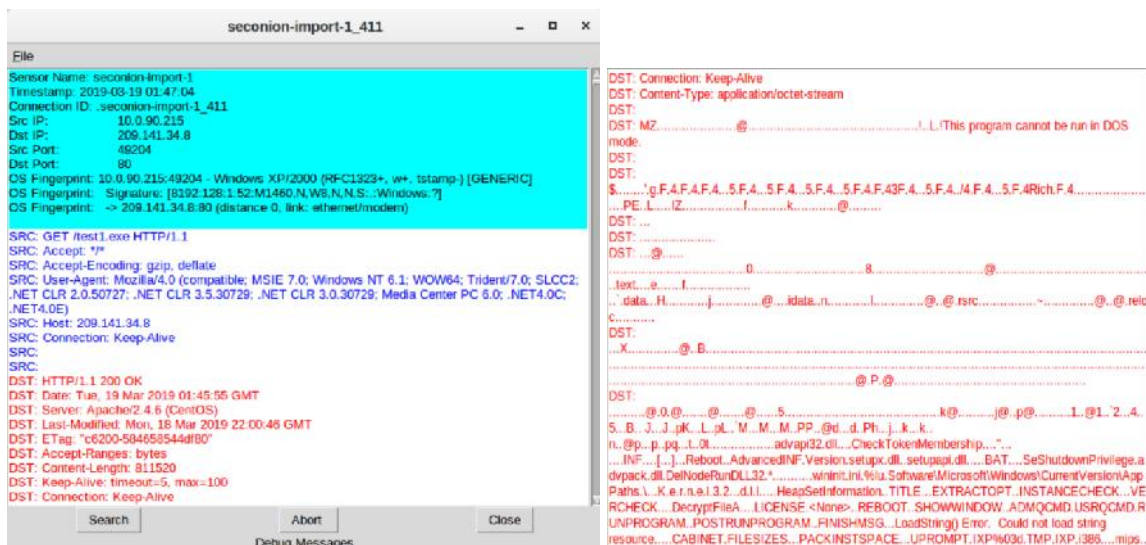
it can be concluded that this is a misconfiguration.

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

Close the Wireshark window.

- 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?

The destination IP address is 209.141.34.8:80 and the source IP address is 10.0.90.215:49204.

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

GET /test1.exe

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? Search for this file signature to find out what type of file was downloaded in the data?

The characters are "MZ." It represents a Windows executable.

- c. Close the transcript. Right-click on the Alert ID of the second event, pivot to Wireshark. Use Wireshark to export the executable file for malware analysis (**File > Export Objects > HTTP...**). Save the file to the analyst's home folder. Exit Wireshark.
- d. 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
2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbbc1c2d2b92ced3f1c85  test1.exe
```

e. **Optional:**

Now that we have a signature, we can do little more search. On your personal machine, submit the file hash value 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?  
Talos recognized it as a malware win32 trojan-spy-agent

- f. In Snort 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:



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

```
Sensor Name: seconion-import-1
Timestamp: 2019-03-19 01:49:45
Connection ID: seconion-import-1_480
Src IP: 10.0.90.215
Dst IP: 103.1184.108
Src Port: 49205
Dst Port: 2404
OS Fingerprint: 10.0.90.215:49205 - Windows XP/2000 (RFC1323+, w+, tstamp-)[GENERIC]
OS Fingerprint: Signature: [8192:128:152:M1460,N,W8,N,N,S:Windows:7]
OS Fingerprint: -> 103.1184.108:2404 (distance 0, link: ethernet/modem)

SRC: ...0...n...#3...TS...S...o
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...a7N*.1.V].C:
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...c6Kf.8.Q.F
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...a2K*.?.].E.>
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...b2L*.?.].E.1a
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...c3O*.?.].G.>c
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...d2K*.?.].E.=
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...PRx*.L.Ka.L...
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
DST: ...0...n...#3...
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...PT...h6J
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
DST: ...0...n...#3...
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...v<5.JUq.F-1.B
DST: ...0...n...#3...
SRC: ...0...n...#3...TS...S...o
DST: ...0...n...#3...
SRC: s.r6@.r.w.l.3R.u...X.H...I...T.qb@'.GO&R.j...PP&H.j.sHK...v55.SJ...[2.N)
DST: ...0...n...#3...
```

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

2404 is the Dest Port. It is not a well-known port

Is the communication readable or is it encrypted?  
it is encrypted

Do some online research on Remcos RAT Checkin 23. What does Remcos stand for?  
Remcos is Remote Control and Surveillance Software.

What type of communication do you think was being transmitted?  
Remcos generate keylogger send to this command and control server.

What type of encryption and obfuscation was used to bypass detection?  
Remcos often use base64 and RC4 encoding to bypass detection.

- h. Using Sguil and the remaining alerts from **3-19-2019**, locate the second executable file that was downloaded.

What Alert IDs alert to a second executable file being downloaded?  
5.483,5.485,5.497,5.509,5.522,5.533.

From which server IP address and port number was the file downloaded from?  
217.23.14.81:80

What is the name of the file that was downloaded?  
F4.exe

**Optional:** Create a SHA256 hash of the file as before. 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, it used the PE32 executable. AMP DETECTION NAME: 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?

they used malicious software name Dridex.

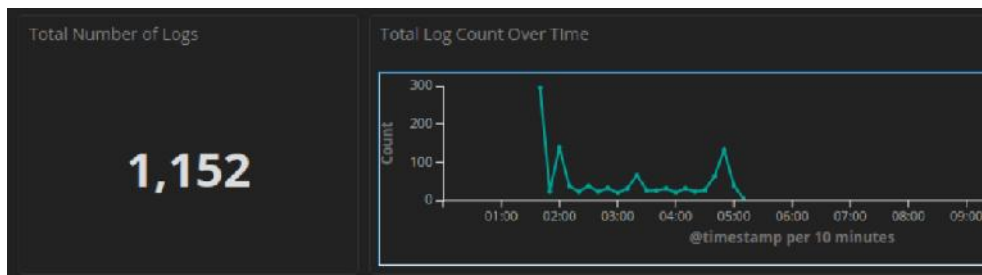
- j. Even though you have examined all the alerts in Sguil related to an attack on a Windows host on 3-19-2019, there may be additional related information available in Kibana. Close Sguil and launch Kibana from the desktop.

### 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.

- Login to Kibana with the analyst username and cyberops password.
- In the Kibana window, click **Last 24 Hours** and the **Absolute** time range tab to change the time range to March 1, 2019 to March 31, 2019.
- The **Total Log Count Over Time** timeline will show an event (a dot) 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.

- 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	

## 27.2.16 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

- 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?

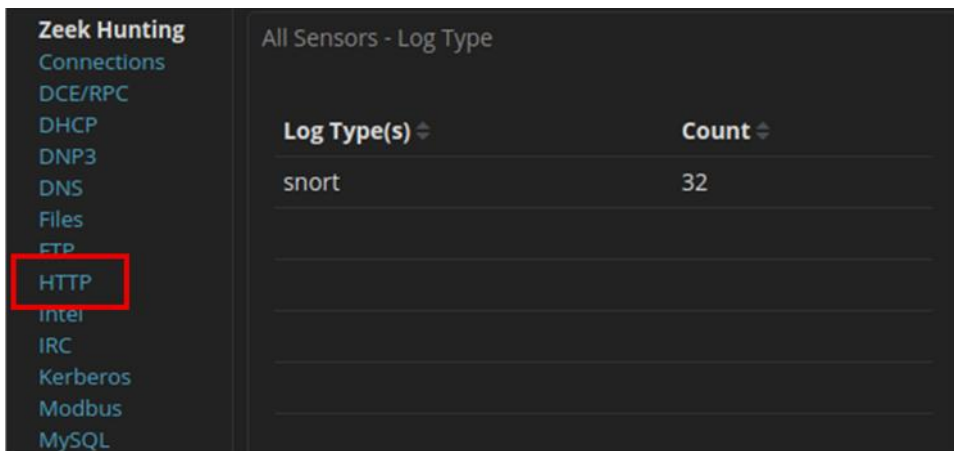
UK, New Castle

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

India, Mumbai

- d. Scroll back to the top of the page and click the Home link under Navigation.

- e. 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.



All Sensors - Log Type	
Log Type(s) ▾	Count ▾
snort	32

- f. 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?

Log Count: 4; From: United States, Netherlands

What are the URIs for the files that were downloaded?

/f4.exe, /ncsi.txt, /pki/crl/products/CSPCA.crl, and /test1.exe

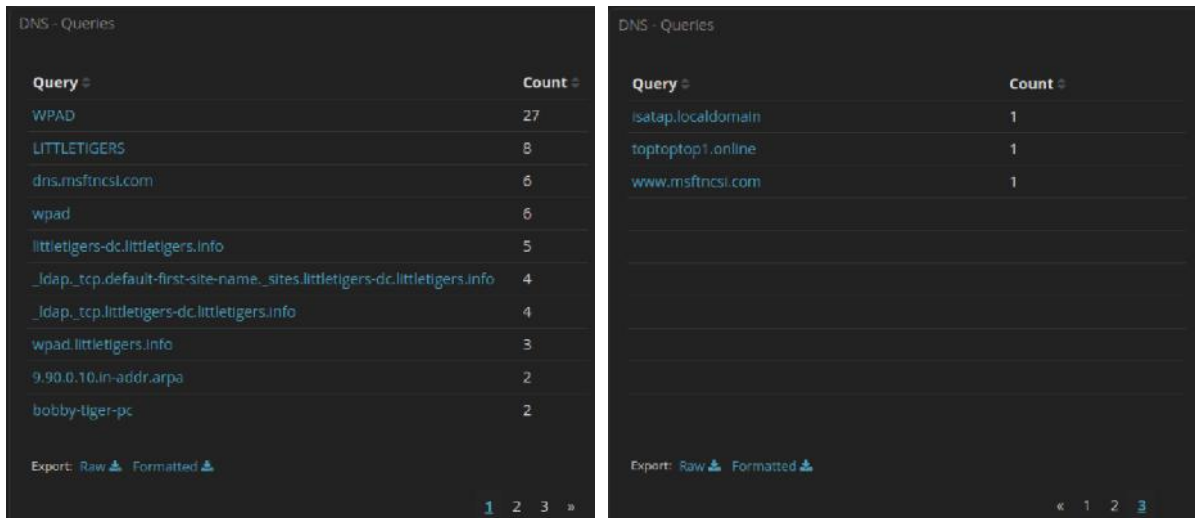
- g. Match the **HTTP - URIs** to the **HTTP - Sites** on the dashboard.

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

CSPCA.crl indicates a request for a Microsoft certificate revocation list, while ncsi.txt signifies the network connection status indicator, which Windows automatically utilizes.



- 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.



Query	Count
WPAD	27
LITTLETIGERS	8
dns.msfncsi.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

Query	Count
isatap.localdomain	1
toptoptop1.online	1
www.msfncsi.com	1

Do any of the domains seem potentially unsafe? Try submitting the URL *toptoptop1.online* to [virustotal.com](https://www.virustotal.com) on your personal computer. What is the result?

All of them seem unsafe. Virus total.com show this website is malicious, which is unsafe.

- i. 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