

Overview

|  |  |
| --- | --- |
| *Name* | Himanshu dubey |
| *Institution* | United College of Engineering and Research |
| *Course name* | Cybersecurity |
| *Supervisor’s name* | Ayush kumar |
| *Date* | 31 July 2025 |

***Abstract***

This project focuses on analyzing network traffic using Wireshark and Zeek to detect suspicious patterns and potential security threats. The purpose was to understand how network monitoring tools can be used to identify malicious activity in a controlled lab environment.

A sample PCAP file containing pre-recorded malicious activity was used for the analysis. Wireshark was first utilized to inspect the captured network packets in detail, applying filters to narrow down significant traffic patterns. Zeek was then used to process the same PCAP and generate structured logs such as connection details, DNS queries, and protocol anomalies. These logs helped highlight suspicious behaviors like repeated failed login attempts, unusual DNS lookups, and high-frequency connections to unknown IP addresses.

One of the main challenges was handling the large amount of captured network traffic and identifying what was actually relevant. This was addressed by applying focused Wireshark filters and by examining Zeek’s “weird” and “notice” logs, which flag abnormal activity.

The results showed that network traffic analysis can successfully identify security issues like brute-force login attempts, data exfiltration, and suspicious domains. These findings demonstrate the importance of continuous traffic monitoring in strengthening network security.

***Table of Contents***

* Abstract
* Introduction
* Methodology
* Results & Discussion
* Conclusion
* Recommendations
* References
* Appendices

***Introduction***

This project is about analyzing network traffic to detect potential security threats using packet analysis tools. In simple terms, it focuses on understanding how data travels across a network and spotting anything that looks suspicious, such as malware downloads or unauthorized connections.

Cybersecurity attacks are becoming more frequent and sophisticated, often hiding within normal network traffic. Many organizations struggle to detect these threats before they cause serious damage. This project was chosen because learning how to analyze network traffic is a critical skill in cybersecurity. It helps identify malicious activity early and strengthens the overall security posture of any network.

To solve this problem, the project used a real-world infected traffic sample (PCAP file) in a controlled lab environment. The sample was analyzed using two industry-standard tools: Wireshark and Zeek. Wireshark was used to visually inspect packets and filter suspicious traffic, while Zeek was used to generate detailed logs that summarize the network activity.

By combining packet-level analysis with log-based analysis, the project demonstrates how security analysts can uncover malware infections and potential Command and Control (C2) communications hidden in network traffic.

***Methodology***

This project aimed to detect malicious network activity using a sample PCAP file. The approach involved analyzing the network traffic in a structured way, first at the packet level with Wireshark and then at the log level with Zeek.

* **Approach**

The plan was to simulate the work of a network security analyst by inspecting the network traffic from a known infected system. By filtering and correlating network events, the objective was to identify suspicious behavior such as malware downloads and abnormal outbound communications.

* **Tools and Technologies**

**Wireshark**: A packet analysis tool used to capture and inspect individual network packets. It allows filtering of traffic by protocol, IP address, and domain name.

**Zeek (formerly Bro)**: A network analysis framework that processes PCAP files and generates structured logs (dns.log, http.log, conn.log) summarizing network activity.

**Sample PCAP file:** A real-world malware traffic sample (2020-10-12-traffic-analysis-exercise.pcap) was obtained from Malware-Traffic-Analysis.net for use in this project.

* **Step-by-Step Process**

**1. Traffic Inspection with Wireshark:**

1. The PCAP file was loaded into Wireshark.
2. An I/O graph was generated to visualize traffic spikes.
3. Filters were applied:
4. dns to identify suspicious domain lookups
5. http.request to find HTTP GET requests (used for malware downloads)
6. tls to identify outbound encrypted traffic (possible Command & Control activity)

Suspicious domains (mailsmilitianon.com) and the malware download request (Xehnimjgm.exe) were identified.

2. Log Analysis with Zeek:

The same PCAP file was processed with Zeek using the command:

zeek -r 2020-10-12-traffic-analysis-exercise.pcap

1. Zeek generated several log files:
2. dns.log: Confirmed suspicious domain lookups
3. http.log: Captured the malware download request
4. conn.log: Recorded outbound connections to Discord IPs (possible Command & Control communications)

* **Correlating Findings:**

Results from Wireshark and Zeek were compared to confirm the infection chain:

* Suspicious DNS queries
* Malware download via HTTP
* Subsequent connections to external servers

***Results and Discussion***

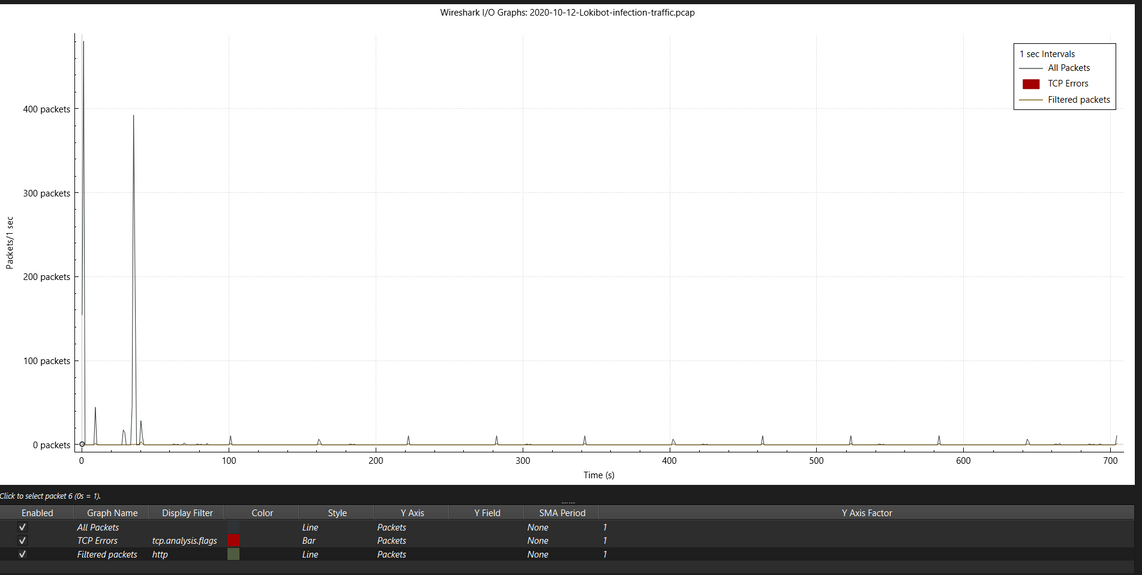
The goal of this project was to analyze a known-infected PCAP file to detect suspicious patterns and malicious activity. The analysis was carried out in two stages using Wireshark and Zeek to ensure both packet-level and log-based perspectives.

**Wireshark Analysis**

The PCAP file (2020-10-12-traffic-analysis-exercise.pcap) was first opened in Wireshark for packet inspection.

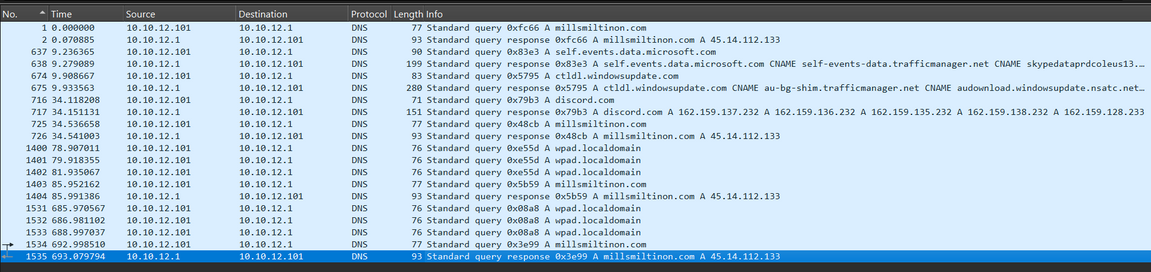
***1. Traffic Overview:***

The I/O Graph feature was used to view traffic volume over time. Spikes in network activity were identified, indicating potential malicious activity.



***2. DNS Traffic:***

Using the dns filter, several suspicious domain queries were identified, such as mailsmilitianon.com. These domains were not associated with legitimate traffic and indicated possible malware command-and-control activity.



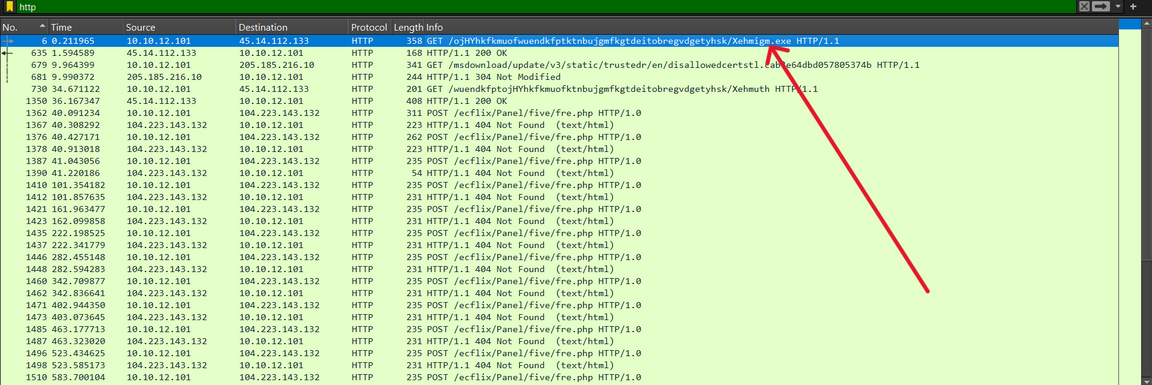
***3. HTTP Traffic:***

The http.request filter was applied to locate HTTP requests. An HTTP GET request was observed retrieving the file Xehnimjgm.exe, confirmed to be the Lokibot malware binary.

**More about Lokibot**

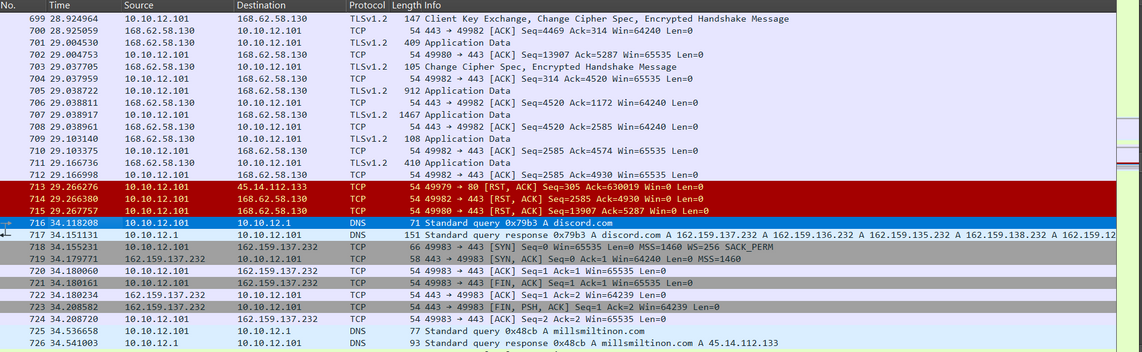
Lokibot is a well-known information-stealing (infostealer) malware that primarily targets Windows-based systems. First discovered in 2015, it is designed to harvest sensitive information such as usernames, passwords, cryptocurrency wallets, browser-stored credentials, and FTP/SSH login details from infected machines.

Lokibot is often delivered through phishing emails, malicious attachments, or drive-by downloads. Once executed, it establishes persistence on the system and immediately begins stealing stored data. The stolen information is then transmitted to the attacker’s Command and Control (C2) server, which is often hidden using encrypted communications or legitimate services such as Discord.



***4. Discord C2 Connections:***

A tls filter was applied to identify outbound encrypted traffic. Attempts to connect to discord.com were observed, likely used as a Command & Control (C2) channel by the malware after infection.

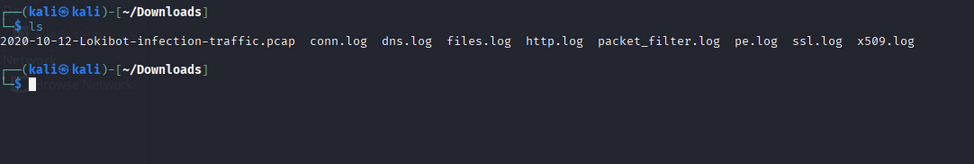


**Zeek Analysis:**

To complement Wireshark’s findings, the same PCAP file was analyzed using Zeek:

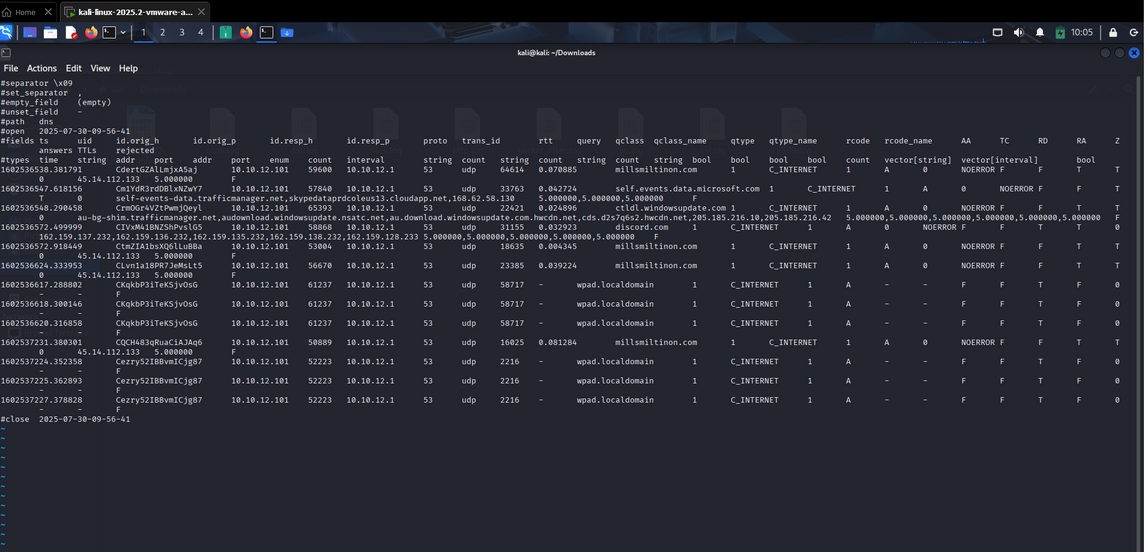
**cmd:**  zeek -r 2020-10-12-traffic-analysis-exercise.pcap

This generated structured logs (dns.log, http.log, conn.log) that summarized the network traffic.



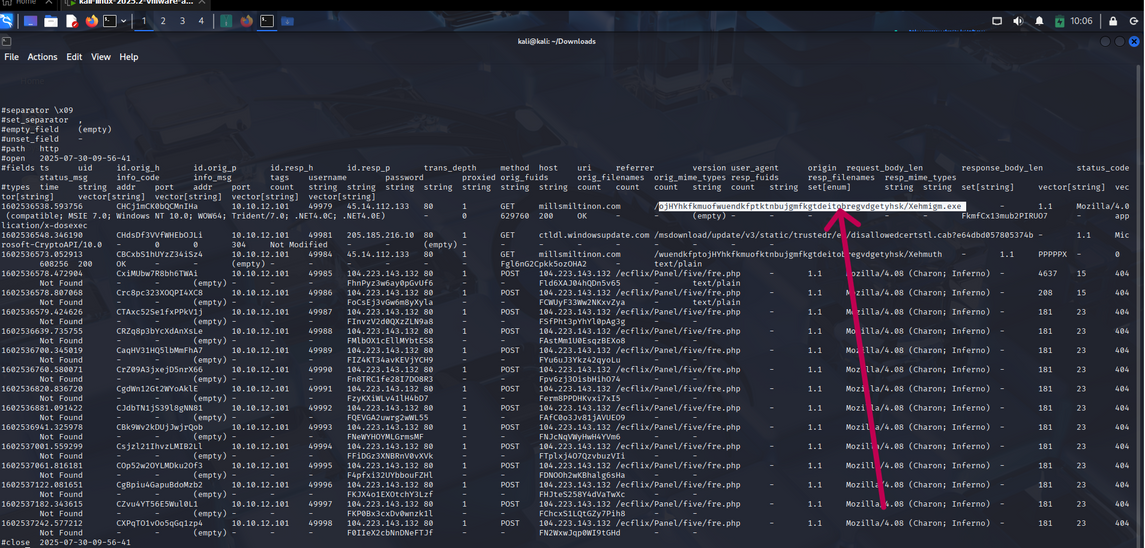
***1. dns.log:***

Confirmed suspicious domains previously seen in Wireshark, including mailsmilitianon.com.



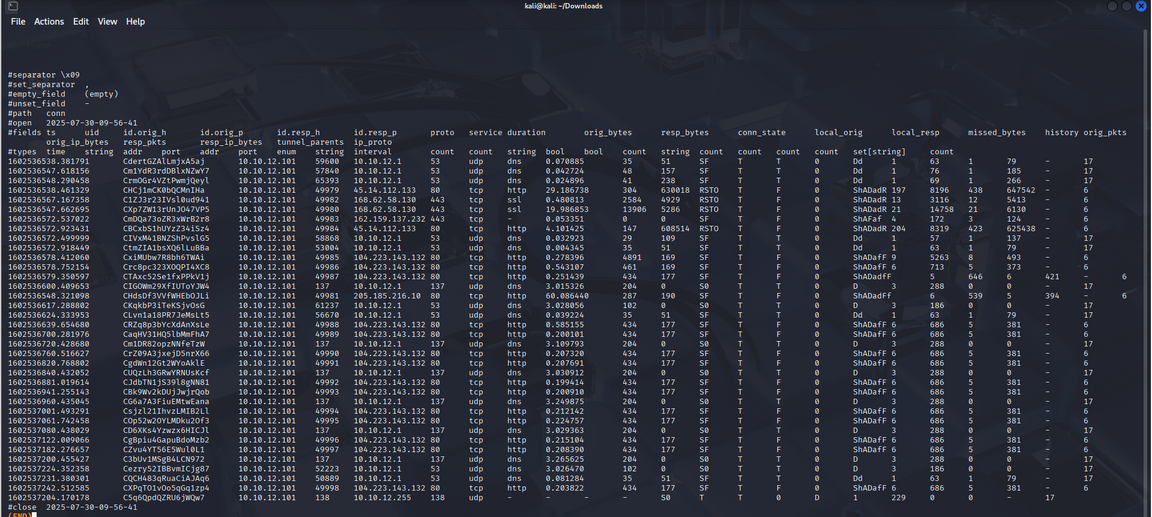
***2. http.log:***

Captured the HTTP GET request for Xehnimjgm.exe, confirming the malware download.



***3. conn.log:***

Showed two outbound connections to Discord IPs shortly after the malware was downloaded, consistent with C2 communication attempts.



***Conclusion***

This project successfully demonstrated how network traffic analysis can be used to detect malicious activity within a controlled lab environment. By examining a real-world infected PCAP file using Wireshark and Zeek, it was possible to identify a full malware infection chain.

The analysis revealed suspicious DNS queries, an HTTP GET request downloading the Lokibot malware executable (Xehnimjgm.exe), and subsequent outbound connections to Discord servers likely used for Command and Control (C2) communications. These findings confirmed the infected host was compromised and actively attempting to communicate with external infrastructure.

Through this project, it became clear that combining packet-level inspection (Wireshark) with structured log analysis (Zeek) provides a comprehensive approach to detecting and validating network-based threats. Such methods are critical for early detection and response in real-world cybersecurity operations.

Future improvements could include automating the analysis workflow and integrating intrusion detection systems (IDS) to enable real-time alerts when suspicious activity is observed.

***Recommendations***

Based on the findings from this project, the following recommendations are suggested to improve network security and detect similar threats in the future:

**1. Implement Continuous Network Monitoring:**

* Deploy packet capture and network analysis tools such as Wireshark, Zeek, or Suricata on a continuous basis.
* Monitoring network traffic in real-time will help detect unusual DNS queries, suspicious HTTP requests, and anomalous outbound connections before an infection spreads.

**2. Use Intrusion Detection/Prevention Systems (IDS/IPS):**

* Integrate tools like Snort, Suricata, or Zeek with an IDS to automatically flag malicious behavior (e.g., known malware signatures, abnormal data exfiltration patterns).
* Automated alerts reduce the response time and help analysts focus on real threats.

**3. Block Access to Known Malicious Domains:**

* Maintain updated threat intelligence feeds and block domains associated with malware C2 servers (e.g., mailsmilitianon.com) at the firewall or DNS level.
* This will prevent infected machines from reaching their Command & Control infrastructure.

**4. Educate Users and Enforce Email Security:**

* Lokibot and similar malware are often delivered via phishing emails. Conduct regular user awareness training to identify suspicious emails and attachments.
* Implement email filtering solutions to block malicious attachments and links.

**5. Log Correlation and Centralized Security Management:**

* Forward Zeek logs, firewall logs, and endpoint detection logs to a centralized SIEM (Security Information and Event Management) solution such as ELK Stack or Splunk.
* Correlating logs from multiple sources increases the ability to detect multi-stage attacks.

**6. Regular Patch Management:**

Ensure that all software and operating systems are updated with the latest patches. Malware frequently exploits known vulnerabilities in outdated software.

***References***

1. Malware-Traffic-Analysis.net. (2020). 2020-10-12 Traffic Analysis Exercise.

https://www.malware-traffic-analysis.net/2020/10/12/index.html

2. Wireshark Foundation. (2023). Wireshark: The World's Most Popular Network Protocol Analyzer.

https://www.wireshark.org/

3. Zeek Project. (2023). Zeek Network Security Monitor.

https://zeek.org/

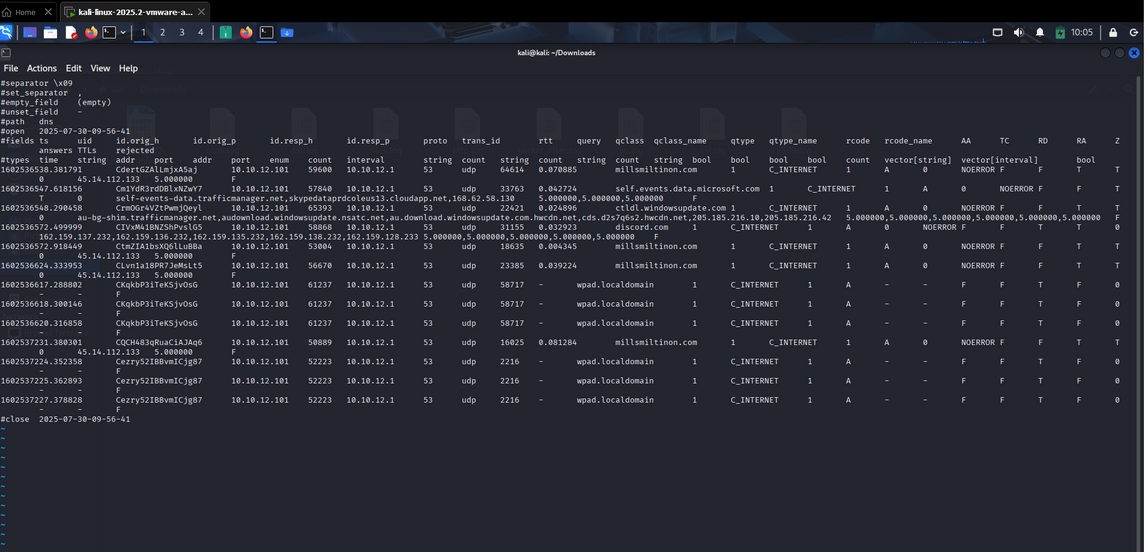
4. Rapid7. (2022). Lokibot: An Information-Stealing Trojan. https://www.rapid7.com/blog/post/2022/07/14/lokibot-overview/

5. SANS Institute. (2021). Detecting Malware with Network Traffic Analysis.

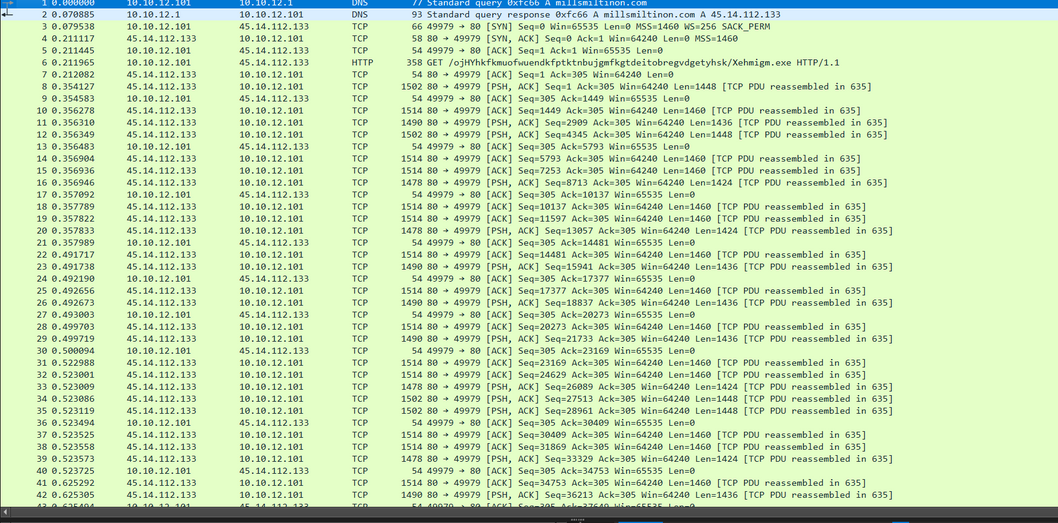
https://www.sans.org

***Appendices***

Appendix A – Zeek Log Files



Appendix B – Full Wireshark Packet Captures



**Observation**

|  |  |  |
| --- | --- | --- |
| Indicator | Type | Observation |
| mailsmilitianon.com | DNS Query | Suspicious domain used by Lokibot malware |
| Xehnimjgm.exe | HTTP GET | Malware binary download request |
| Discord.com (IP) | Outbound C2 | Command & Control connections post infection |