**Network Packet Analysis Report.**

Prince Mitchell C.E

# Introduction

In today's digital world, network security plays a crucial role in protecting sensitive data and ensuring the safe operation of digital communication. As cyber threats continue to grow, implementing robust security measures has become essential for preventing threats to our data and network infrastructure. This report displays tools like Wireshark, Nmap, Linux VM, and other open-source vulnerability scanners used to identify malware downloaded from an email received. The report further evaluates two malicious contents, one downloaded by a cleaner and the other by a teacher, by investigating what was downloaded and how it was downloaded. However, a swift investigation will be conducted using a PCAP file captured by the company network administrator and a PCAP file captured by the Forest Park School IT department. The report provides an alternative and recommendation to limit and prevent unauthorized connections to data and network infrastructure access. Through a logical and structured approach, exploring this will positively impact the protection of the company’s network over the Internet.

# Analysis of Investigative Tools

Nmap, Wireshark, TCPdump, VirusTotal, and other open-source software platforms are employed for the investigation. They all play a crucial role in gathering, analyzing, and verifying network traffic and potential threats.

Wireshark was central to the network analysis. It captured and inspected real-time packets, which helped follow up suspicious packets by examining the TCP stream with exported objects to identify downloaded malicious content. Its protocol dissection capabilities made it especially useful in reconstructing TCP sessions and examining payloads for indicators of compromise. However, Wireshark has its challenges when it comes to filtering packets; even with the filter option provided, it can be difficult without prior knowledge.

Virus Total was used in the project during the packet inspection to verify suspicious files or URLs discovered in captured traffic. It helped by verifying if the content downloaded or sent across both hosts displayed suspicious behavior. The following steps are shown by pasting the link, file, or hash code information about the virus, where it is hosted, and other necessary information from the content. However, a limitation is that it may not always detect sensitive threats (false negatives), and uploading sensitive files could raise privacy concerns.

Additionally, Kali Linux (virtual machine) was another useful tool while examining the frames; it helped in providing the SHA 256 hashing code from files suspected to have this malicious content, and when this is provided, the hashed value is passed to VirusTotal to verify the content of this file. It also provided a safe environment for such content, isolating it from the local host, to avoid any unaware system configuration. However, Kali Linux has challenges, especially when setting up the virtual machine; its lack of stability raises questions about whether it can perform advanced or scaled tasks relating to providing a SHA value.

# Report from the PCAP file

## PCAP on Wireshark

The PCAP file displays the time the packet was sent, the packet number, the source IP address, the destination address, the protocol, and other information about the packet. It also displays the hexadecimal and other valuable resources and features used to identify the malware successfully.

## Investigation conducted on the PCAP file(holiday\_agency\_evidence.zip)

Inside the PCAP file, during the examination, it was discovered that a few packets were related to malicious content with the IP address (ip,addr == 192.168.75.119) presented by the network Administrator. While going through the TCP and HTTP stream, it was discovered that the cleaner first visited a website named update.immunet.com with the IP address == 204.236.230.152. The website was examined and confirmed as virus-free, but it happens to be that there was a hidden SHA encryption, which was further analyzed and confirmed to be a virus from TrendMicro. From what was discovered through the TCP stream, it was detected that the cleaner downloaded an update in text content with the virus inside.

A screenshot of a computer

AI-generated content may be incorrect.

TCP stream of update.immunet.com



The text file was downloaded from update.immunet.com

A screenshot of a computer

AI-generated content may be incorrect.

A detected content using VirusTotal

The second packet investigated contained malicious content from a website CRL.MICROSFT.COM with the IP address == 65.54.51.253. When scheming the TCP stream, the content hosted by the website was encrypted, but with proper scheming, a link (crl.microsoft.com/pki.crl/products/microsoftrootcert.crl0t) containing malicious content from ESTsecurity was found using an open-source tool called VirusTotal. A possible outcome would be that the cleaner visited this link and tried to download the contents, because no content was downloaded from the malicious link.

A screenshot of a computer

AI-generated content may be incorrect.

A detected content using VirusTotal,(source: Bernardo Quintero, 2004)

A screenshot of a computer

AI-generated content may be incorrect.

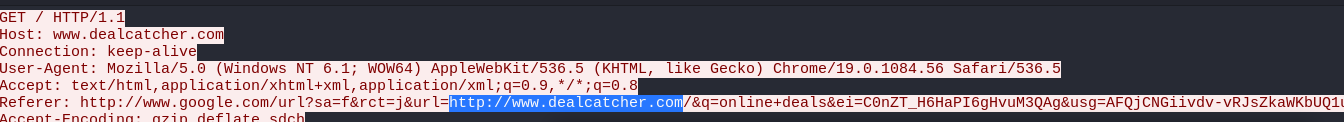
TCP stream of crl.microsoft.com

Another packet with malicious content was discovered during the investigation, which was from a website named [www.dealcatcher.com](http://www.dealcatcher.com) with the IP address 141.101.124.100. A further inspection of the TCP stream revealed that the VirusTotal software revealed a hidden detail about the website; it was discovered to have malicious content from Quttera. The inspection went further to the exported objects to know if any content was downloaded from the website, and it was discovered to have more than five different downloaded contents by the IP address = 192.168.75.119.

A screenshot of a computer

AI-generated content may be incorrect.

Contents downloaded from www.dealcatcher.com



TCP stream of www.dealcatcher.com

## Investigation conducted on the PCAP file (Forest Park School. pcap file)

It all started by going through the PCAP file, which contained different packets possibly related to phishing, malicious content, and malware in text format. With the IP address ==10.1.6.206 presented by the IT departments from which the malware got into the network, the investigation will be easy to find the malware. The first packet was investigated after discovering malicious content, phishing, and malware. The first to be seen was from a website called hangerlastilk.com with the IP address = 89.252.164.58, which was determined to be a malicious site. It happened to be that the downloaded file was from this site with the content named Ui4n (/cgi-bin/Ui4n/HTTP1.1), which the teacher downloaded. The file is a text content file, and inside the file is a link referencing another link (the document has moved”), so it happened to be that when the teacher downloaded the file, a file referencing where the virus was detected was equally downloaded by the name suspendedpage.cgi (cgi-sys/suspendedpage.cgi HTTP/1.1).

A screenshot of a computer

AI-generated content may be incorrect.

Forest Park School. PCAP containing Malware



The two downloaded text files

# Security Recommendations and Analysis

The attack on Caribex highlighted critical vulnerabilities in organizational processes and its technical infrastructure. The breach, likely from an unpatched system vulnerability or phishing-based compromise, demonstrates the need for a comprehensive and layered security approach.

**Technical measures** must begin with implementing a robust intrusion detection and prevention system (IDPS) to monitor network traffic and alert administrators to suspicious behavior in real time(Fortinet, 2023). A firewall is equally beneficial in blocking certain packets and IP addresses from accessing your network. Implementing a patch management system is equally critical, as many cyberattacks exploit unknown vulnerabilities and outdated software. Applying Local host protection, the principle of least privilege, and enforcing network segmentation can also significantly limit the scope of any intrusion.

Sensitive data should be encrypted at rest and in transit to prevent unauthorized data access and leakage. Multi-factor authentication (MFA) should be assigned to all network systems, particularly systems accessed remotely.

It is also essential to focus on **non-technical measures**. Human error is considered the easiest link to exploit, particularly through social engineering and phishing, which remains a leading cause of breaches(Verizon, 2023). A recommendation will be to conduct cybersecurity awareness and training campaigns regularly, which should be mandatory for all employees to encourage a security-conscious culture. Establishing a clear incident response plan and performing regular drills can ensure preparedness and quick recovery in future incidents.

A suggestion for Caribex will be to consider adopting frameworks such as ISO/IEC 27001, which provides a structured approach to managing sensitive information securely and aligning security efforts with business objectives(National Institute of Standards and Technology, 2024).

# Conclusion

In conclusion, the project has laid the groundwork for understanding the importance of implementing security against cyberattacks, the risk of not securing our network, taking note of the technical and non-technical aspects of security, and the open-source tools such as Wireshark, Nmap, and Linux VM used for scanning vulnerabilities and scanning for malicious content. However, a few more explanations and more scanning of PCAP files were neglected due to the project's word count format. Moreover, addressing the recent breach and preparing for similar future threats requires a holistic strategy that blends advanced technical defenses with strong governance, policy, and employee involvement. Only through this multi-layered approach can Caribex build resilience against evolving cyber threats.