Phishing Attack Simulation and Training

Team Members

1. Mostafa Helal Atia Mohamed
2. Mohamed Yasser Rabie
3. Mostafa Ahmed Abbas
4. Nofir Nasr Atta Qandil
5. Mahmoud Walid Rajab Askar

Phishing Attack Simulation and Training

1. Introduction

Phishing attacks are one of the most common cybersecurity threats facing organizations today. Implementing a phishing attack simulation and training program can help educate employees, assess vulnerabilities, and improve the organization's security posture. This documentation provides a step-by-step guide on how to implement a phishing simulation program, conduct training, and measure its effectiveness.

1.1 Purpose

The purpose of this document is to outline the procedures and best practices for conducting a phishing attack simulation and training within the organization. This simulation is intended to improve employee awareness and prepare the incident response (IR) team to handle phishing attacks effectively.

1.2 Goals and Objectives

- To test and evaluate the organization’s incident response capabilities against phishing threats.
- To identify gaps in security awareness among employees.
- To enhance the organization's ability to detect and respond to phishing attacks.
- To strengthen the overall security posture by integrating the findings into the security awareness program.

1.2 Scope

- Develop phishing email templates.

- Conduct simulated phishing campaigns.
- Provide training based on the results.
- Measure success and generate reports.

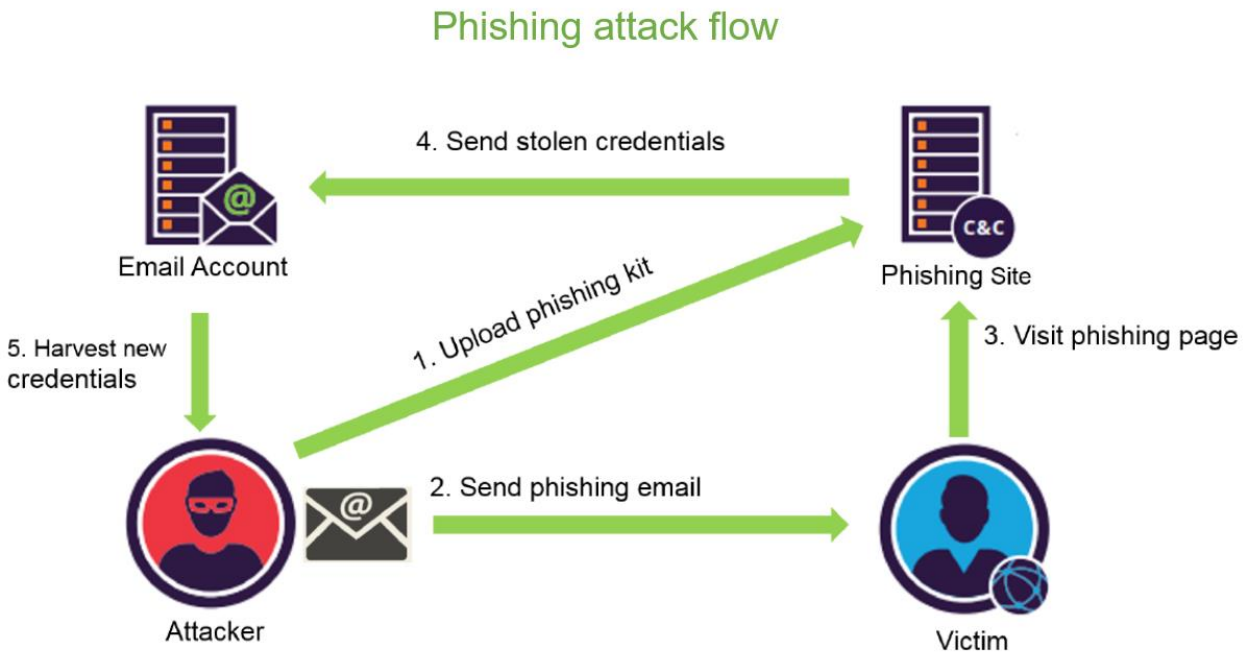
1.2 Scenario

- Your email address has been leaked and you receive an email from Paypal in German. Try to analyze the suspicious email.

2. Phishing Simulation Overview

2.1 Definition of Phishing Attack

- A phishing attack is a form of social engineering in which an attacker sends a fraudulent message (usually via email) to trick individuals into revealing sensitive information or installing malicious software.



2.2 Goals and Objectives of the Simulation

- To evaluate the organization's ability to detect and respond to phishing attempts.
- To train employees on identifying phishing red flags.
- To test and enhance the incident response procedures.
- To measure the effectiveness of security awareness programs.

2.3 Stakeholders

- **Incident Response Team**: Responsible for detecting, analyzing, and responding to the simulated phishing attack.
- **IT Security Team**: Manages infrastructure and provides technical support.
- **Training and Awareness Team**: Conducts training sessions post-simulation.
- **Employees**: Serve as test subjects for the simulation.

2.3 Tools and Machines used

- KALI LINUX Machine
- Window Victim Machine
- Software Phishing tool such as: ZPHISHER
- **Zphisher**
    - is an open-source phishing tool designed for creating and hosting fake web pages that mimic legitimate sites to capture sensitive user credentials (e.g., usernames and passwords). It is commonly used by penetration testers and cybersecurity enthusiasts to demonstrate and test the effectiveness of phishing attacks.
    - It is written in **Bash** and **Python** and comes preconfigured with various phishing page templates.
    - ***Features of Zphisher***

- **Multiple Phishing Templates**: Zphisher includes ready-to-use phishing templates for platforms like social media sites, e-commerce, and financial services.
- **No Setup Required**: It automatically sets up the server, configures tunneling services, and initiates the phishing page.
- **Support for Custom Pages**: Users can create their own custom phishing pages.
- **Tunneling Options**: Supports various tunneling methods (Ngrok, Localhost, Cloudflared, LocalXpose
- **User-Friendly Interface**: The tool is designed with a simple command-line interface for easy use.

Timeline of Events

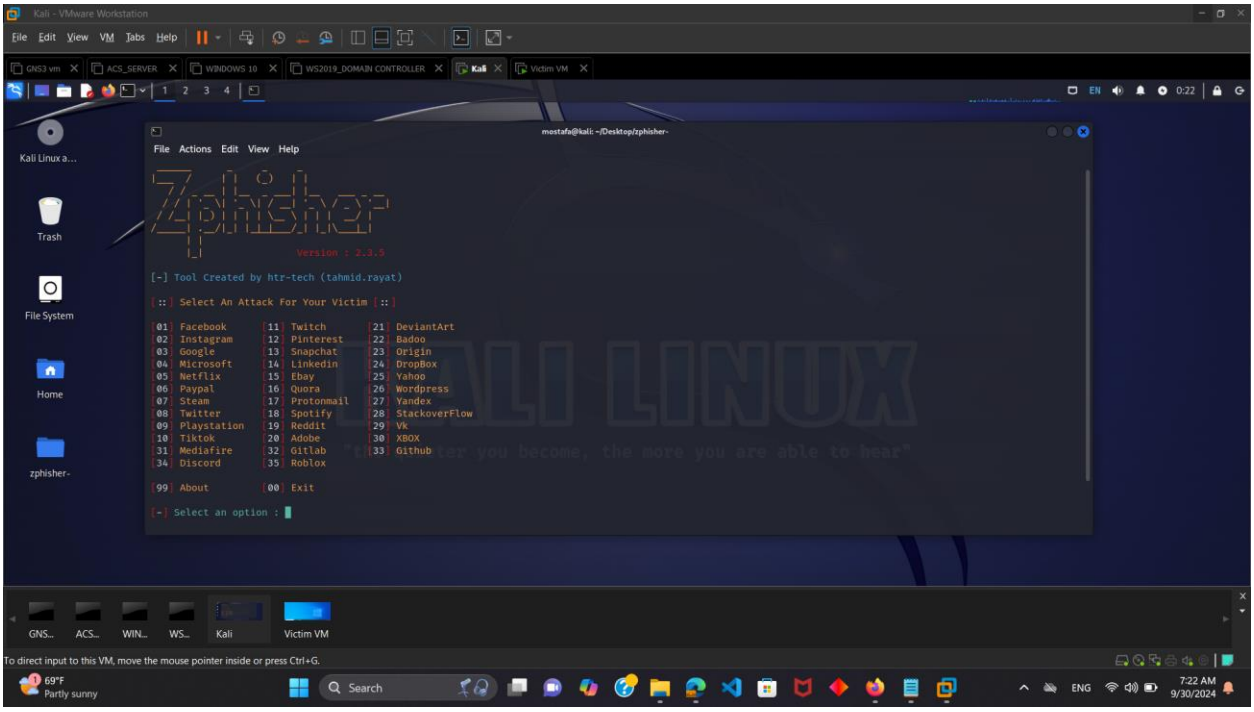
- **Preparation Phase**:
  - **Day 1**: Identify target group (e.g., employees in finance) and create the phishing simulation emails.
  - **Day 2**:
  - Configure email templates with realistic content mimicking common phishing attacks (e.g., fake PayPal alerts).
  - Set up necessary tracking mechanisms to monitor user interaction (link clicks, responses).
- **Execution Phase**:
  - **Day 3**:
    - Launch the phishing simulation and send emails to the selected users.
    - Monitor user responses, including clicks on phishing links, data entry attempts, and emails reported.
- **Analysis and Training Phase**:
  - **Day 4**: Analyze the results, document which users fell for the phishing attempt, and identify common weak points.

- **Day 5**: Conduct a detailed awareness training session for employees covering phishing indicators and safe practices.
- **Day 6**: Follow-up with users who fell for the phishing test and provide additional training.

3. Phishing Attack Simulation Planning

3.1 Phishing Scenario Design

- Create phishing scenarios using ZPhisher:
- Steps:
  1. **Start Zphisher**
     - When you run the script, you will see a menu displaying various phishing templates for different platforms (like Facebook, Instagram, Google, etc.).
     - Choose the desired platform by entering its corresponding number.



2. Choose the Tunneling Service

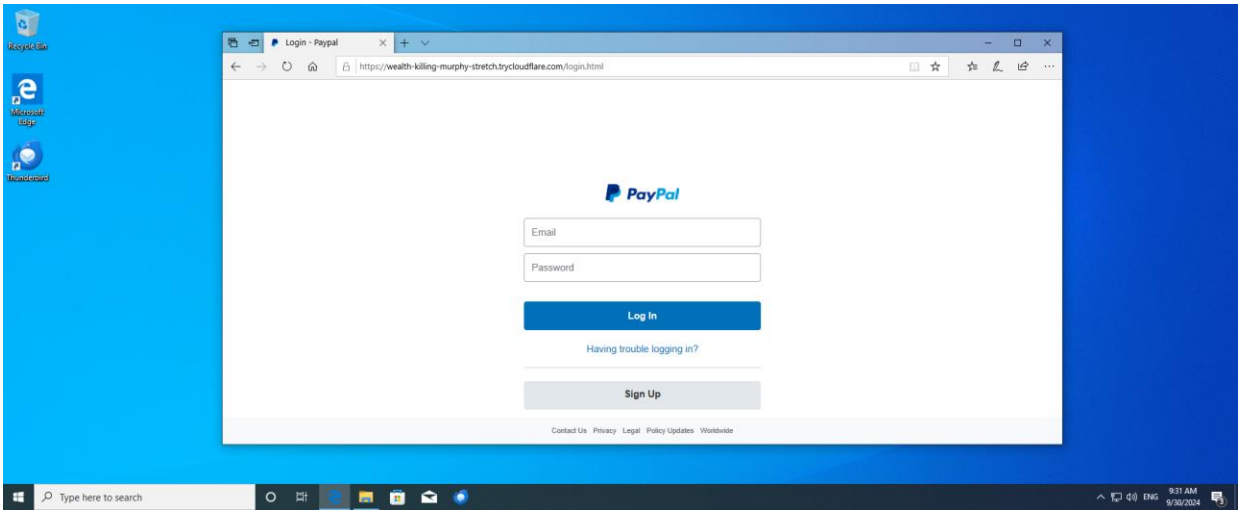
- After selecting the platform, Zphisher will present you with multiple methods, such as:
    - [01] Localhost
    - [02] Cloudflared
    - [03] LocalXpose

3. **Generate the Phishing Link**
    a. Once the server is started, Zphisher will generate a phishing link that you can use.
    b. Copy this link and send it to your target victim in an email or in an attachment.

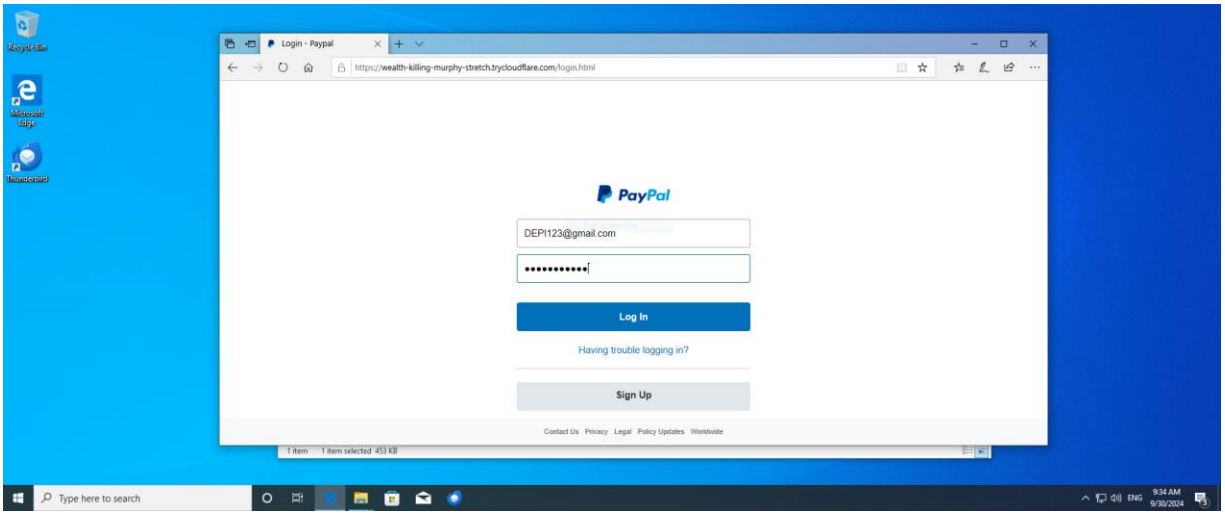
4. **Wait for the Target to Interact**

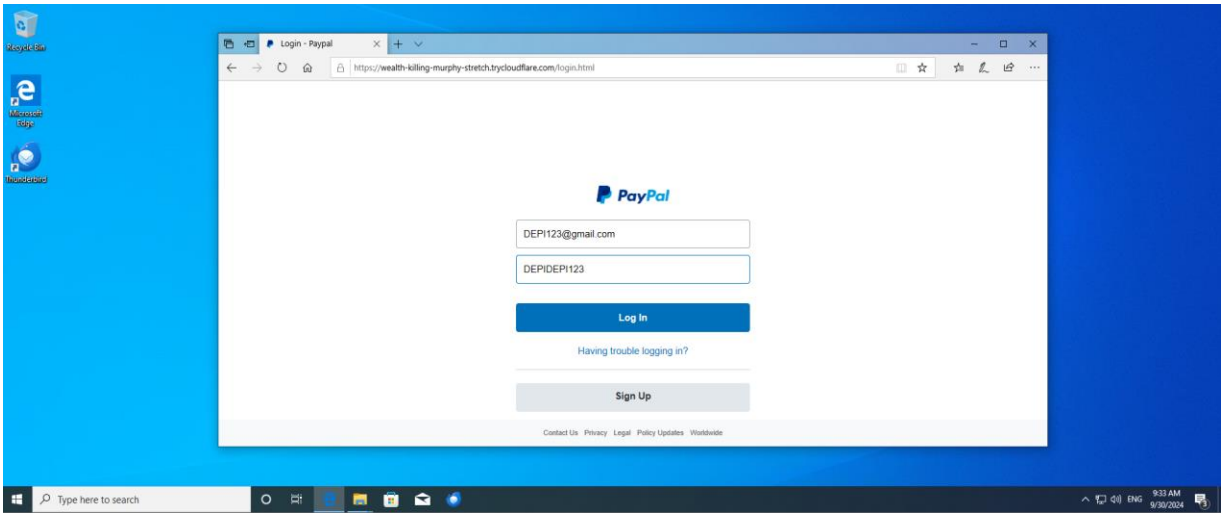
a. When the target clicks on the link on an email and inputs their credentials, Zphisher will capture the information and display it in your terminal.

1. When the target clicks on the link on an email.



2. When the target inputs their credentials





5. **Analyze the Credentials**
   - The credentials will be stored in the Zphisher directory.
   - The captured information will include:
     - **Ip address of the victim target**
     - **Username/Email**
     - **Password**

3.2 Scheduling and Execution

- Determine a schedule for the simulation without notifying employees to maintain authenticity.

- Use a secure and reputable phishing simulation platform.
- Design emails to resemble typical company communication to test user vigilance.

3.3 Email Template Design

- Subject: “Immediate Action Required: Security Alert”
- Body:
    - Include a sense of urgency.
    - Use company branding to increase legitimacy.
    - Provide a link to a mock phishing site for employees to interact with.

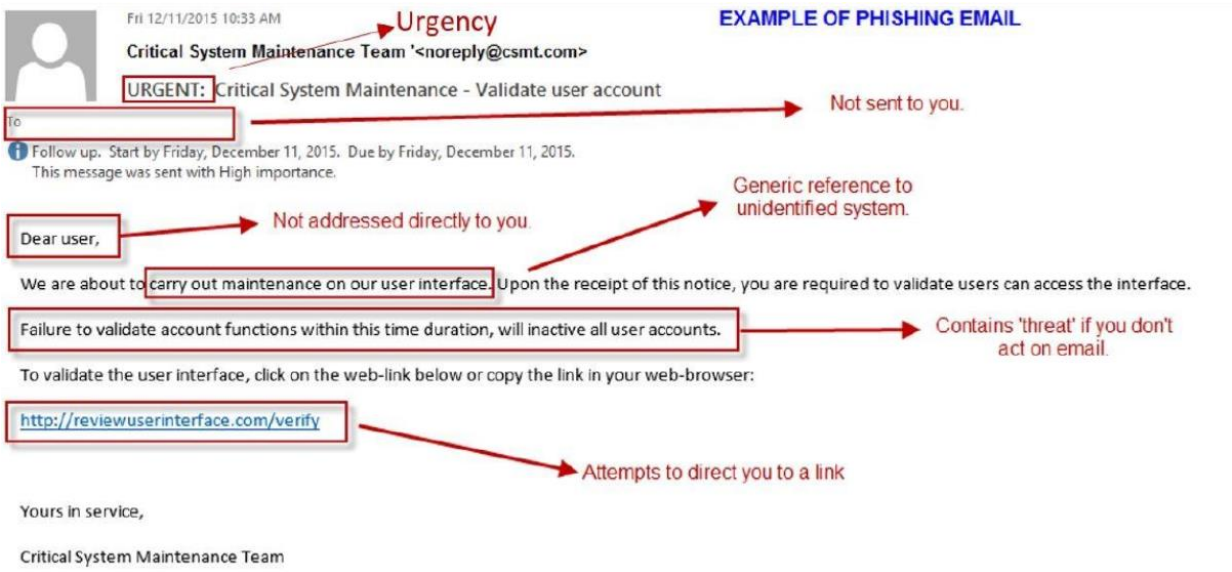
3.4 Training Setup

- Develop materials such as guides, quizzes, and video training sessions.
- Schedule a post-simulation training session to review the results.

4. Phishing Email Analysis

I. What is phishing email analysis?
    a. Phishing email analysis involves studying the content of phishing emails to ascertain the techniques the attacker used.
II. What is a common indicator of a phishing email?
    a. Common indicators of a phishing email include suspicious addresses, links, or domain names, threatening language or a sense of urgency, errors in the email, the inclusion of suspicious attachments, and emails requesting sensitive information.

III. Example of phishing email



5. Incident Response Steps

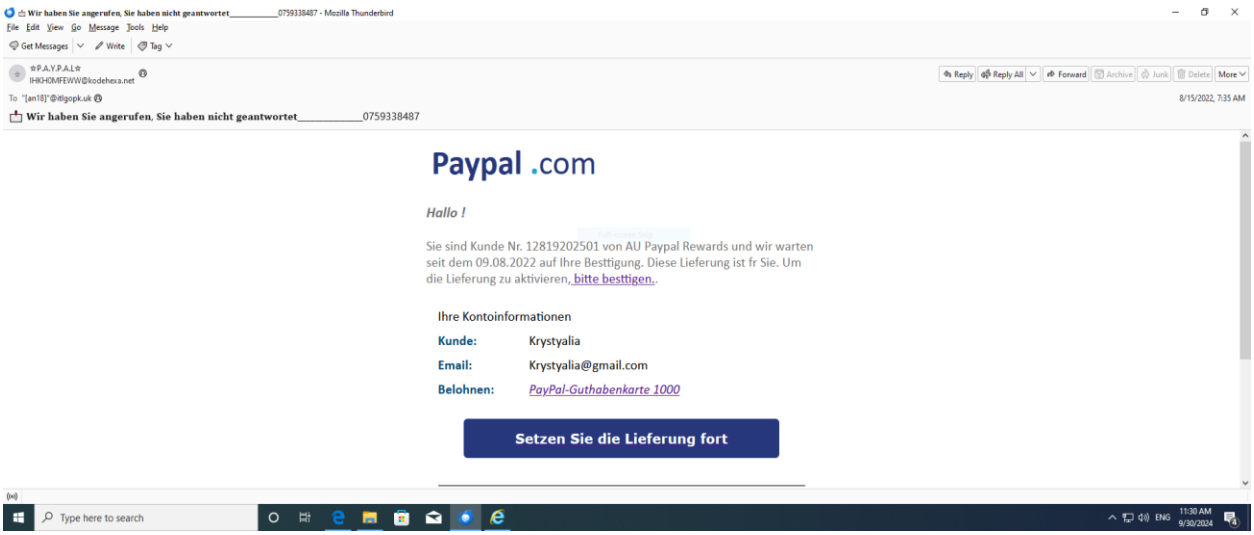
5.1 Detection and Analysis

when phishing email is detected, follow these steps:

- **Initial Analysis**
  - Identify and categorize the phishing email based on its nature (credential harvesting, malware).
  - Use automated tools (e.g., email filtering solutions, SIEM) to analyze the email's headers, sender, and content.
  - Check for Indicators of Compromise (IOCs) such as malicious links or attachments.
- **Documenting IOCs**
  - Record the sender’s email address, subject line, URLs, and file hashes for future reference.
  - Investigate if the same email was sent to multiple recipients.
- **Employee Reporting**
  - Ensure that employees know the correct procedure for reporting suspicious emails.

- Use phishing reporting buttons (if available in email clients) to streamline the process.

- **Identify employees who interacted with the phishing email.**
- **Determine if any sensitive information was submitted.**



Phishing Email Analysis:

- A phishing email designed to look like it's from PayPal. Here's a detailed analysis and steps to improve awareness around this type of phishing threat:

Sender Information:

- The sender address is `IHKH0MFEWW@kodehexa.net`, which is not a legitimate PayPal domain. Always check the sender's email address carefully.

Subject Line:

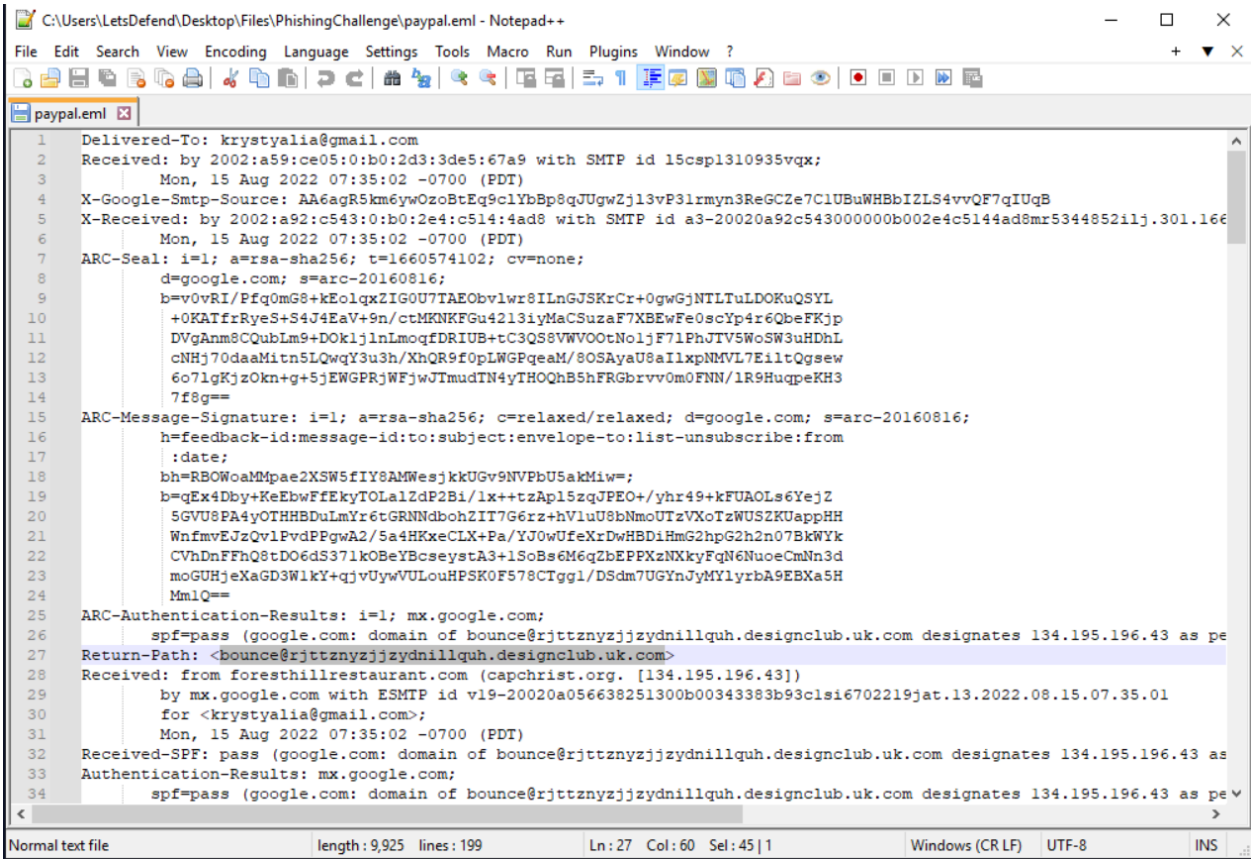
- The subject line is in German: "Wir haben Sie angerufen, Sie haben nicht geantwortet" (Translation: "We called you, you did not respond"), followed by a phone number. This is an example of a social engineering tactic to create a sense of urgency and prompt the recipient to respond without verifying.

Body Text:

- The message uses the **PayPal logo** to appear legitimate.
- Greeting is generic: "Hallo!" instead of using the recipient's name.
- The text includes phrases like "bitte bestätigen" (please confirm) with a hyperlink. Hovering over such links (without clicking) can reveal whether the URL is legitimate.

Call to Action:

- The button “Setzen Sie die Lieferung fort” (Continue with the delivery) leads to a suspicious link. This is likely an attempt to capture sensitive information such as login credentials.



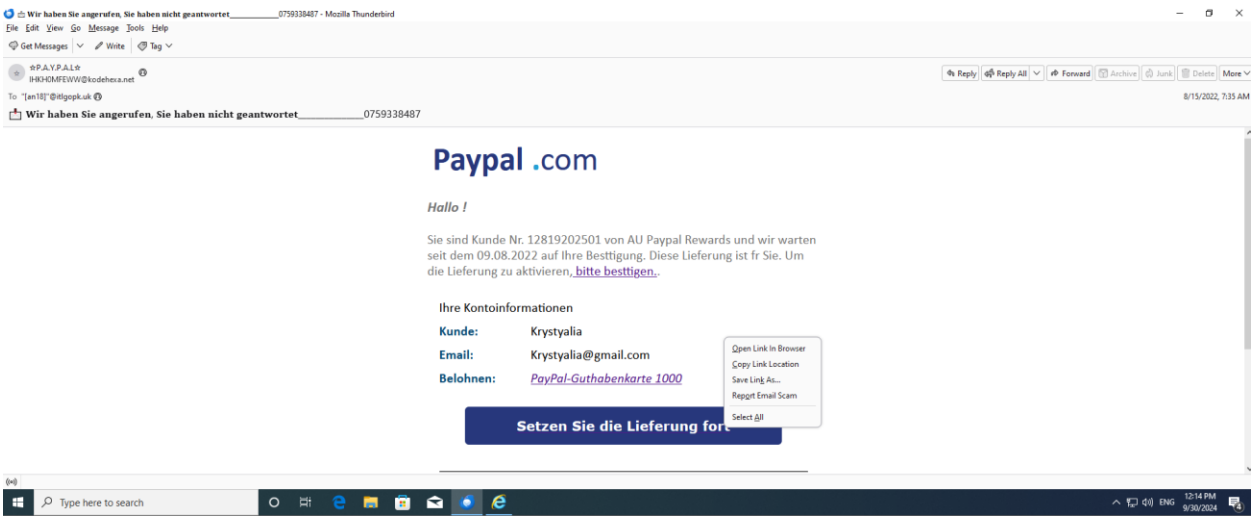
Email header extracted from a `paypal.eml` file, which is used to track the origin, authenticity, and delivery path of an email.

- **Delivered-To:** krystalia@gmail.com Indicates the recipient's email address.
- Received Fields (Multiple Entries)

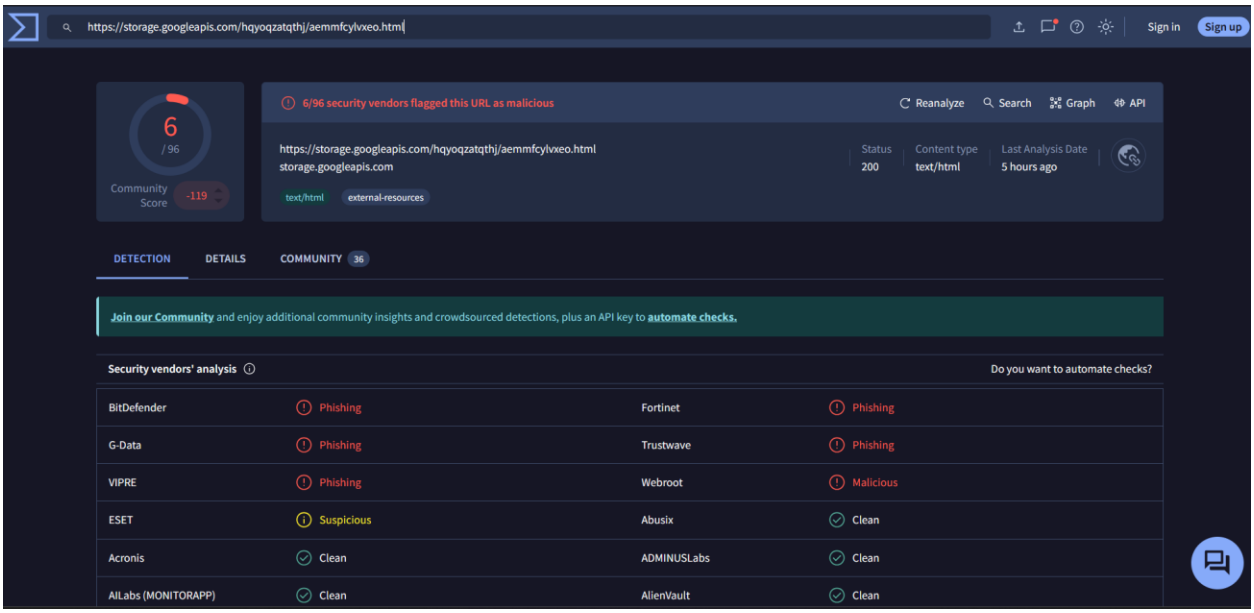
- **Purpose**: Each `Received` entry records a step in the email's journey, from the original sender to the final recipient.
- This line shows that the email was processed by Google's server ip with a timestamp indicating it was handled on August 15th, 2022, at 7:35 AM (PDT).

1. **Return-Path:** `<bounce@rjtzntyzzjjzydnillquh.designclub.uk.com>` The `Return-Path` specifies where undelivered messages should be sent back.

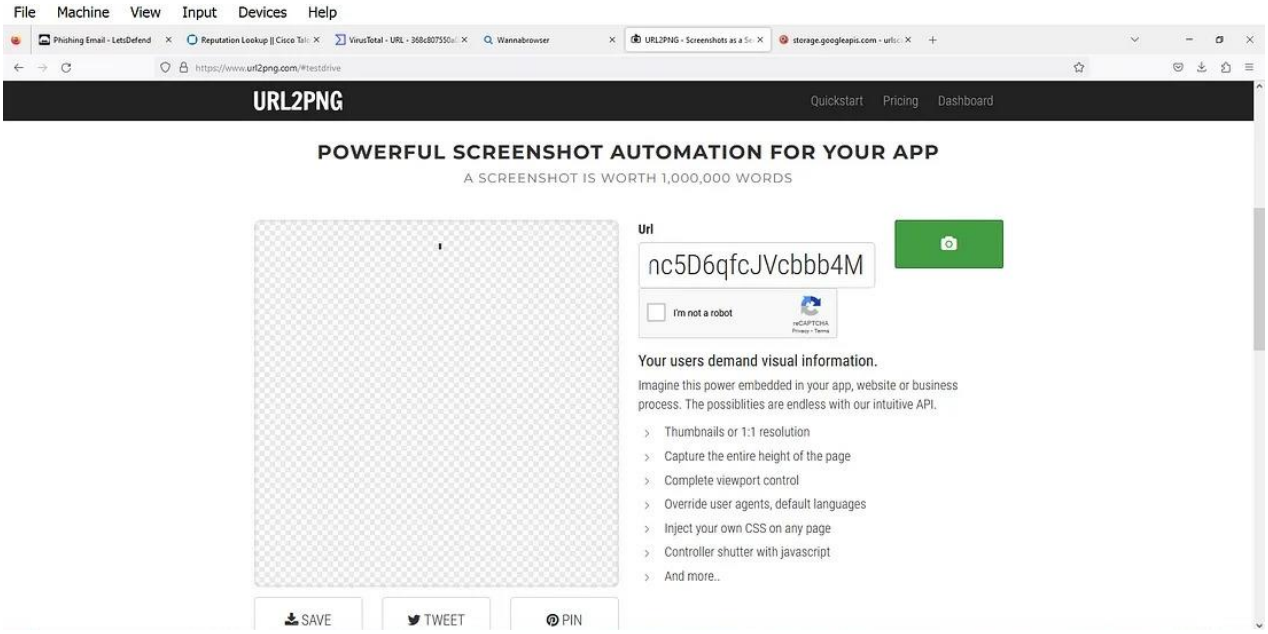
2. **Suspicious Indicator**: The domain (`designclub.uk.com`) does not match PayPal's legitimate domain, suggesting that the email may be spoofed or sent from an unauthorized server.



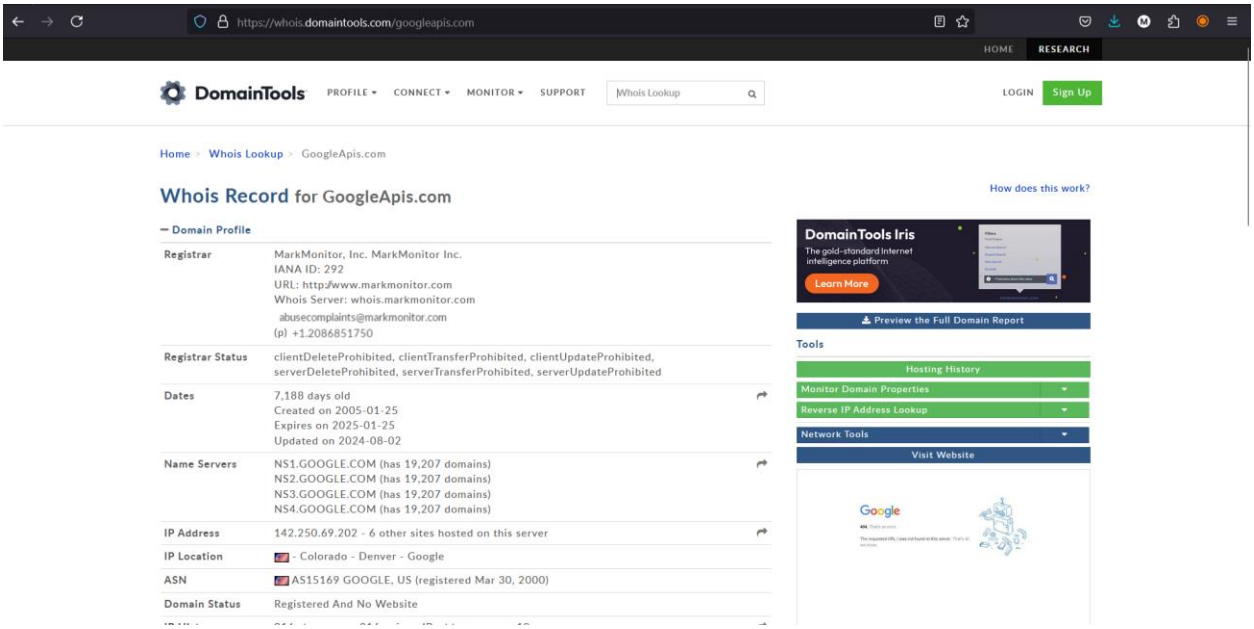
- By right-clicking on the button, copying the link, and upload the URL to VirusTotal to do some initial reputation checks. We can see that 6 out of 96 security vendors have flagged this URL as malicious.



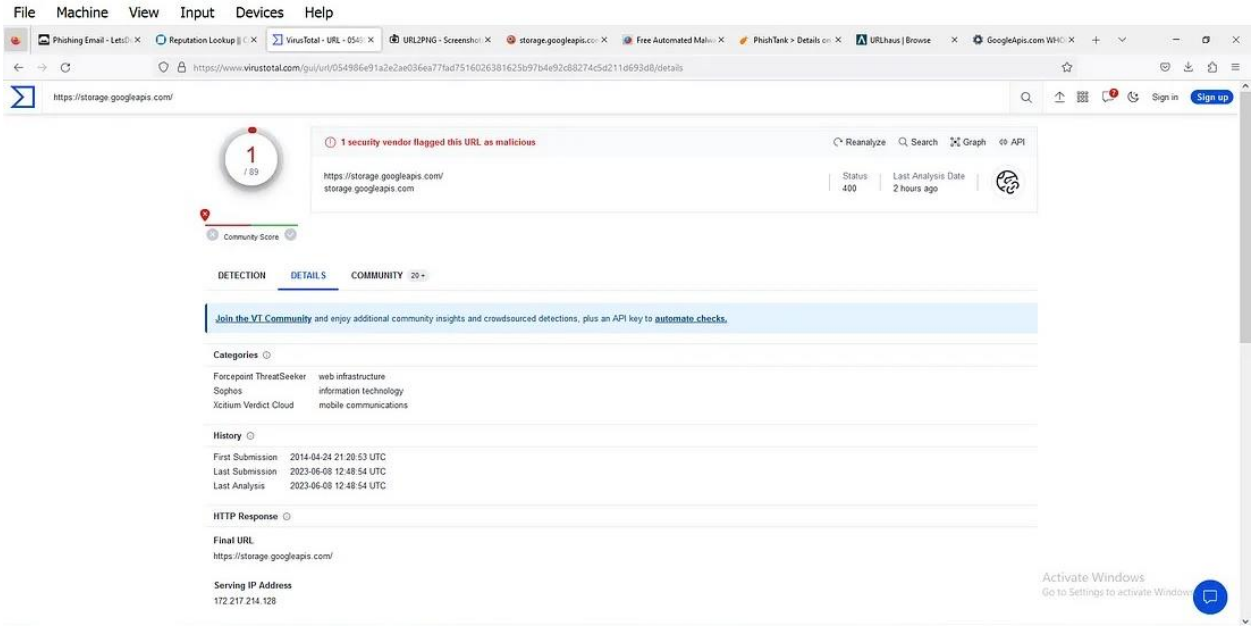
- **URL2PNG** is a tool that converts URLs to PNG images, allowing you to capture the visual representation of web pages quickly.
- When we put the URL into URL2PNG to see what the page looks like. It is not loading which means it is either not legitimate or there is no content and the site does not show any homepage.



- Check the domain <storage.googleapis.com> usign DomainTools whois lookup



- **Check the domain on virustotal** We can see that 1 out of 89 security vendors have flagged this URL as malicious.
- **Virustotal** is a tool that used to analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.



- Is this email a phishing email?
- Based on the above analysis we can see the email is actually a phishing email that has a hyperlink that is hosting a malicious URL.

5.2 Containment

- **Isolate Affected Systems**:
  - Disconnect compromised systems from the network to prevent further damage.
  - Use endpoint detection and response (EDR) tools like CrowdStrike or Carbon Black to isolate infected endpoints.
- **Quarantine Malicious Emails**:
  - Use email filtering tools (e.g., Proofpoint, Microsoft Defender) to quarantine the phishing email from all user inboxes.
  - Ensure that any internal email forwarding rules set by the attacker are removed.
- Alert the affected users immediately.
- Implement account resets if credentials were compromised.
- Isolate the affected systems if necessary.

5.3 Eradication and Recovery

- **Remove Malicious Artifacts**:
  - Delete phishing emails from users' inboxes.
  - Ensure that the phishing website and email are blocked.
  - Remove any malicious software installed by phishing attachments.
- **Patch & Update**:
  - Apply security patches if vulnerabilities were exploited.
  - Update security configurations, including email filters and spam detection rules.
  - Restore systems to a known good state.

5.4 Lessons Learned

- Conduct a post-incident review with the Incident Response team.
- Discuss what went well and areas for improvement.

- Integrate feedback into the Incident Response Plan.

6. Reporting and Metrics

6.1 Simulation Results

- Percentage of employees who:
  - Opened the email.
  - Clicked on the phishing link.
  - Submitted sensitive information.

6.2 IR Team Performance Metrics

- Time taken to detect the phishing simulation.
- Time taken to respond and mitigate the attack.
- Accuracy of the analysis and containment.

6.3 Training Effectiveness

- Improvement in user awareness before and after training.
- Reduction in the number of phishing-related incidents post-training.

The Root Cause of Phishing Attack

- **Lack of Awareness**:
  - Employees were unaware of the basic signs of phishing (e.g., mismatched email domains, urgent language).
- **Insufficient Training**:
  - Previous training sessions did not focus enough on social engineering tactics and psychological manipulation used in phishing.
- **Human Error**:
  - Many users tend to trust emails that appear visually legitimate, especially if they mimic known brands (e.g., PayPal).

- **Inadequate Technical Safeguards**:
    - Spam filters and security tools were not fully optimized, allowing simulated phishing emails to bypass safeguards.

The Impact of Phishing attack

- Phishing attacks can have severe and wide-ranging consequences on an organization or individual. Below are the primary impacts:

I. **Financial Losses**:
    a. Direct monetary losses can occur due to fraudulent transactions or unauthorized access to financial accounts.
    b. Indirect costs include recovery expenses, legal fees, and potential fines for non-compliance with data protection regulations.

II. **Data Breach and Information Theft**:
    a. Phishing can lead to unauthorized access to sensitive data such as login credentials, intellectual property, and customer information.
    b. Compromised information can result in identity theft, insider trading, or resale of data on the dark web.

III. **Reputation Damage**:
    a. Organizations that fall victim may experience a loss of trust and credibility among customers and stakeholders.
    b. Negative media coverage and the perception of poor security practices can deter future clients and impact business growth.

IV. **Business Disruption**:
    a. Phishing attacks can lead to downtime in critical systems, interrupting business operations.

V. **Legal and Compliance Issues**:
    a. Organizations may face legal action or penalties for failing to protect customer data.

VI. **Increased Security Costs**:

a. After a phishing attack, companies often need to invest heavily in security upgrades, training, and recovery processes.
b. Organizations may also have to hire external consultants to assess vulnerabilities and prevent future incidents.

Conclusion

- Implementing a phishing attack simulation and training program is a crucial step in strengthening an organization's cybersecurity posture. By simulating real-world phishing scenarios, companies can effectively measure employee awareness, identify vulnerable points, and reinforce best practices for email security. This documentation has outlined the structured approach of the simulation, the timeline of activities, and the impact analysis, providing a comprehensive understanding of the process.
- The key takeaway from this exercise is that human error is a critical factor in most successful phishing attacks, making regular training and continuous awareness essential. The simulation also highlighted the importance of robust technical safeguards, such as email filtering and incident response protocols, to complement human vigilance.

THANK YOU