Phishing Analysis Research: Deconstruction of a Live Microsoft Credential Theft Campaign

Author: Ishaan Malhotra And Aakash Anand
Date of Analysis: September 25, 2025
Analysis Subject: sample-1011.eml
Classification: **Confirmed Malicious Phishing Attempt**

---

1. Introduction

1.1. Background

Phishing remains one of the most prevalent and effective cyber attack vectors. Attackers leverage social engineering and technical deception to impersonate trusted entities, aiming to trick victims into divulging sensitive information such as login credentials, financial details, or personal data. This project analyzes a real-world phishing email to deconstruct the techniques used by attackers.

1.2. Objective

The primary objective of this investigation was to perform a comprehensive analysis of the suspected phishing email (sample-1011.eml) to:

- Verify the authenticity of the sender.
- Identify technical indicators of forgery within the email headers.
- Analyze the social engineering tactics used in the email body.
- Safely investigate the payload link to determine its threat level.

1.3. Methodology

The analysis was conducted within an isolated Kali Linux virtual environment to ensure safety. The methodology involved a multi-stage process:

1. **Static Analysis:** The raw source of the .eml file was examined using a text editor to dissect its headers and HTML structure without rendering its content.
2. **Safe Link Extraction:** The grep command-line utility was used to extract all hyperlinks from the source code for external analysis.
3. **Threat Intelligence Analysis:** The extracted URL was submitted to VirusTotal, a public aggregate of security vendor scan results, to assess its reputation and identify known threats.

---

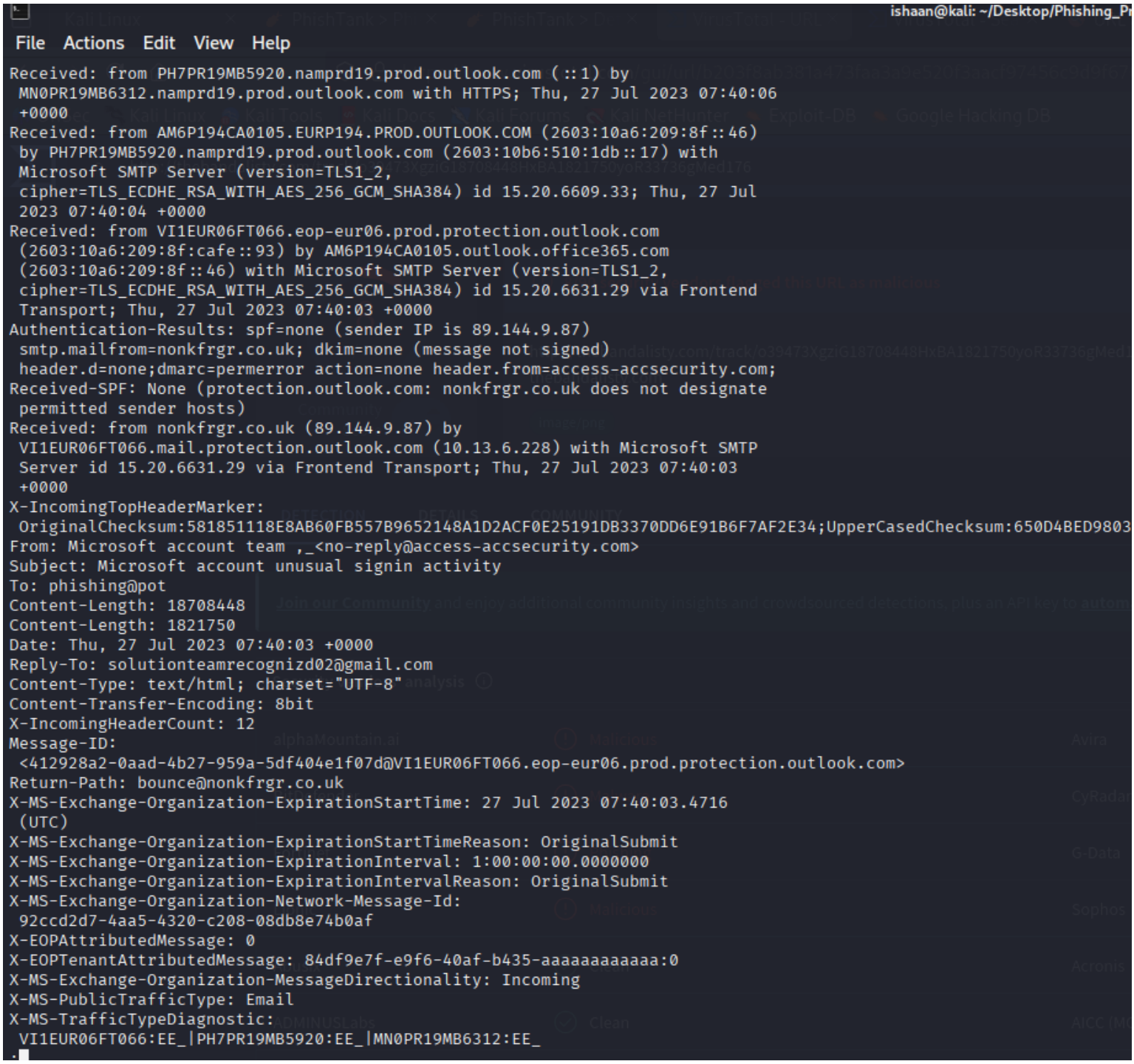
2. Detailed Analysis & Findings

2.1. Header Analysis: Proof of Forgery

The email headers provide a technical fingerprint of the message's journey and authenticity. To inspect the file safely, the raw source of the email was first opened using the less command in the terminal. This method allows for viewing the content without rendering any potentially malicious HTML or images.

The following command was used to view the file:

less sample-1011.eml



Key findings from the headers (shown in this image) include:

- **Sender Impersonation:** The From: header displayed "Microsoft account team <no-reply@access-accsecurity.com>," a domain clearly not owned by Microsoft.
- **Authentication Failure:** The Authentication-Results header reported a complete failure of standard email verification protocols:
    - **spf=none**: Sender Policy Framework (SPF) could not be verified, as the sending domain (nonkfrgr.co.uk) had no published SPF record. This means there is no policy to prevent others from sending emails on its behalf.

    - **dkim=none**: DomainKeys Identified Mail (DKIM) was not present. The email lacked a digital signature, meaning its integrity and origin could not be verified.
- **True Origin Identified:** The Received: header clearly shows the email originated from a server named **nonkfrgr.co.uk** at the IP address **89.144.9.87**. This contradicts the sender's claim of being Microsoft.

2.2. Content Analysis: Social Engineering Tactics

The email's content was crafted to exploit human psychology.

- **Subject Line:** "Microsoft account unusual signing activity"
- **Analysis:** This subject line is a classic social engineering tactic that creates a powerful sense of **fear** and **urgency**. It implies the victim's account is already compromised, pressuring them to bypass normal security caution and react immediately to the perceived threat.

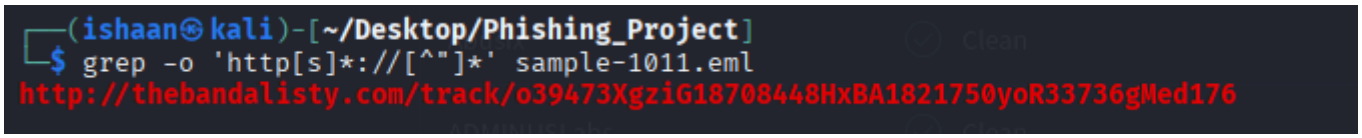
2.3. Payload Link Analysis: The Active Threat

The ultimate goal of the email was to direct the user to a malicious website.

2.3.1. Safe Extraction of URL

The link was safely extracted using the following command to avoid accidental exposure.

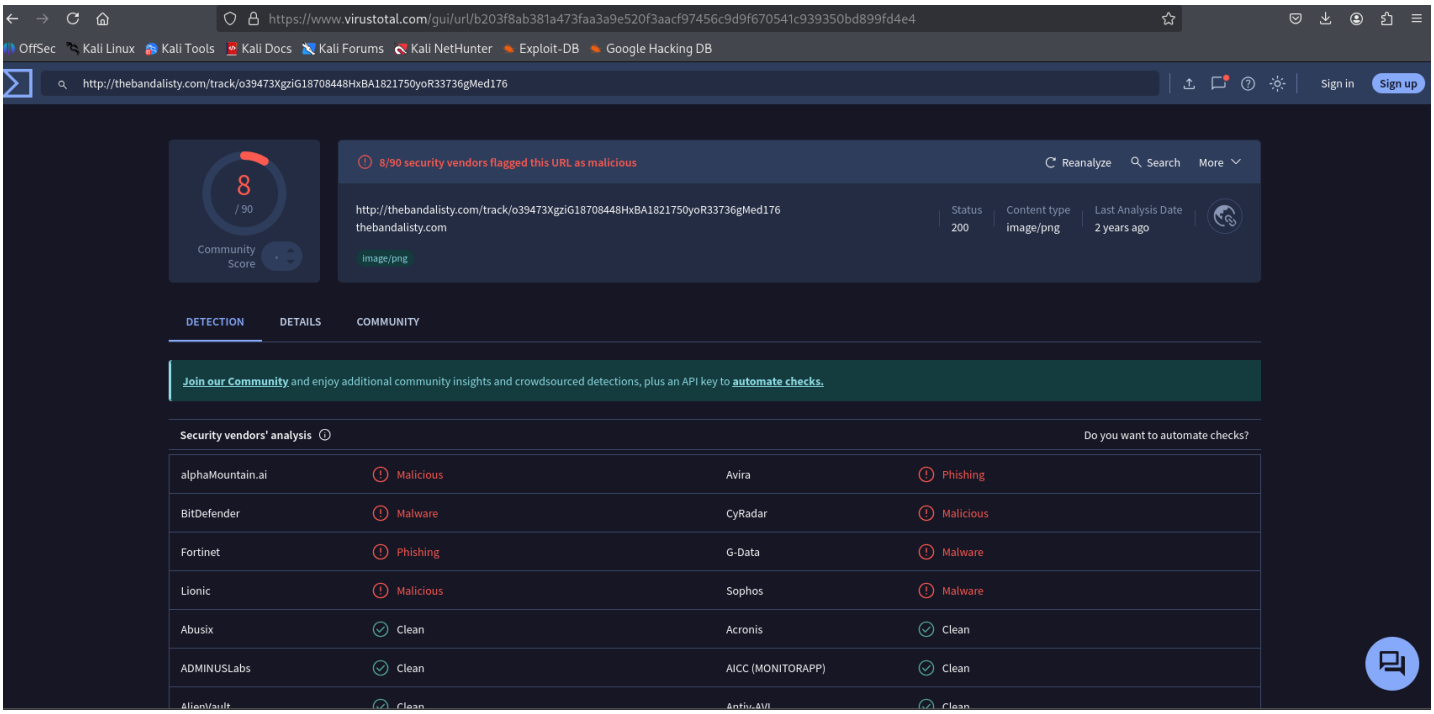
Bash
grep -o 'http[s]*://[^"]*' sample-1011.eml



The command extracted the primary payload link:
http://thebandalisty.com/track/...

2.3.2. Threat Verification

The extracted URL was submitted to VirusTotal for analysis. The scan confirmed the link is malicious.



As shown this image, the URL was flagged by **8 out of 90** security vendors. The detections explicitly classify the link as **"Malicious," "Phishing,"** and **"Malware."** This confirms that the link leads to a known-bad website, likely a credential harvesting page designed to look like a real Microsoft login form.

---

3. Conclusion

The email sample-1011.eml is definitively a **dangerous phishing attack**. The campaign combines technical forgery (spoofed sender, failed authentication) with psychological manipulation (fear, urgency) to lure victims into clicking a malicious link. The link was confirmed by threat intelligence platforms to lead to a dangerous web property. The attack's primary goal is the theft of Microsoft account credentials, which could lead to identity theft, financial loss, and further compromises.

---

4. Mitigation & Recommendations

To defend against such threats, the following security best practices are recommended:

- **Verify Sender Identity:** Always carefully inspect the sender's email address, not just the display name.

- **Never Click, Navigate Directly:** In response to unexpected security alerts, never click the provided links. Instead, open a new browser window and manually type the official URL of the service (e.g., account.microsoft.com) to check your account status.
- **Enable Multi-Factor Authentication (MFA):** MFA is the single most effective control to prevent account takeover, as it requires a second form of verification that the attacker does not have.