Phishing Email Analysis Report

Prepared By:

Emmanuel Olajoseph

Date: 26th Dec, 2025

Executive Summary

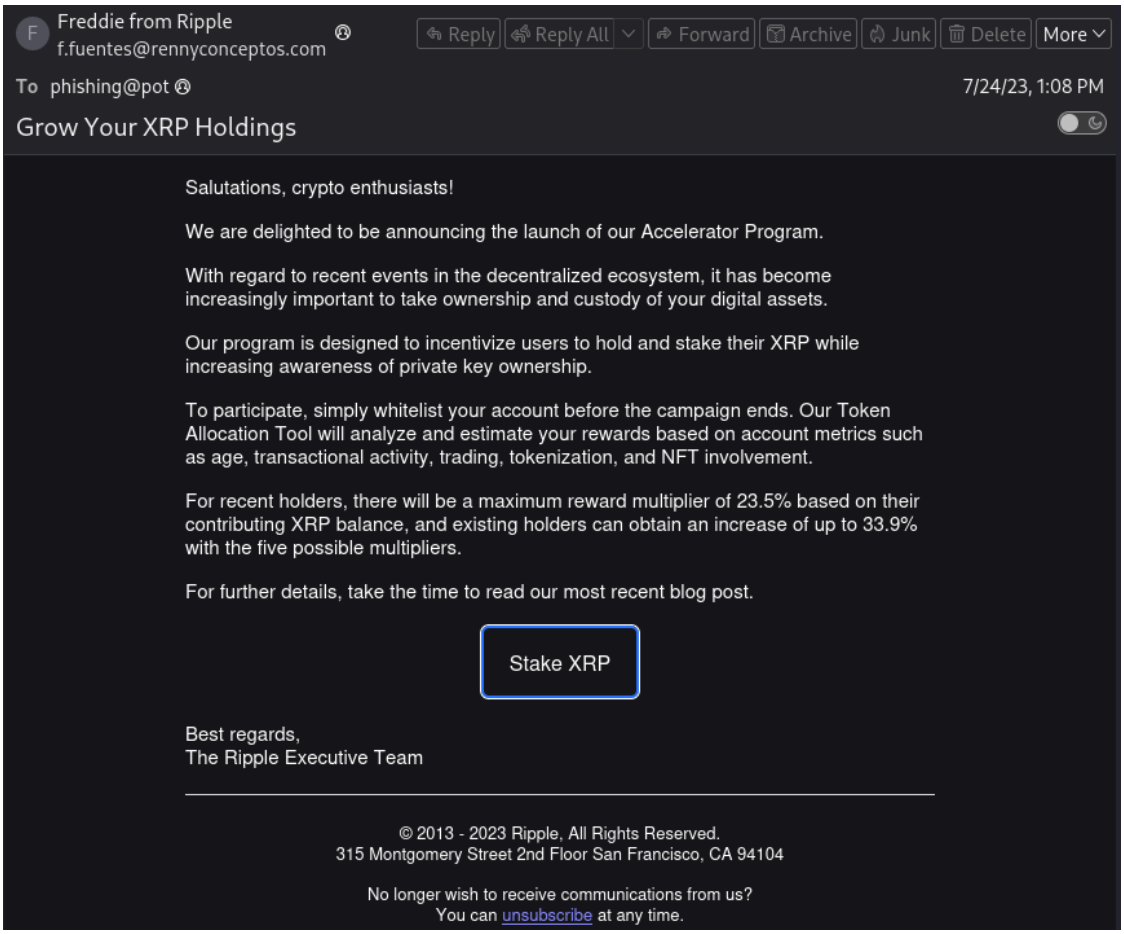
Conducted an in-depth analysis of a suspicious email received through the corporate email gateway. The email was isolated in a sandboxed virtual environment and subjected to multi-layered analysis techniques, including header inspection, URL reputation analysis, and threat intelligence gathering. Based on the results, it is concluded that the email is a phishing attempt designed to lure users into clicking a malicious link.

Tools Used

- **Symmatec Sitereview -** for checking domain categorization and reputation
- **URLScan.io -** To visualize how the link behave when accessed
- **VirusTotal -** for scanning URL across multiple antivirus engines.
- **AbuseIPDB -**To check sender IP reputation.

Email

This is the email will be Analyzed



Email Metadata Analysis

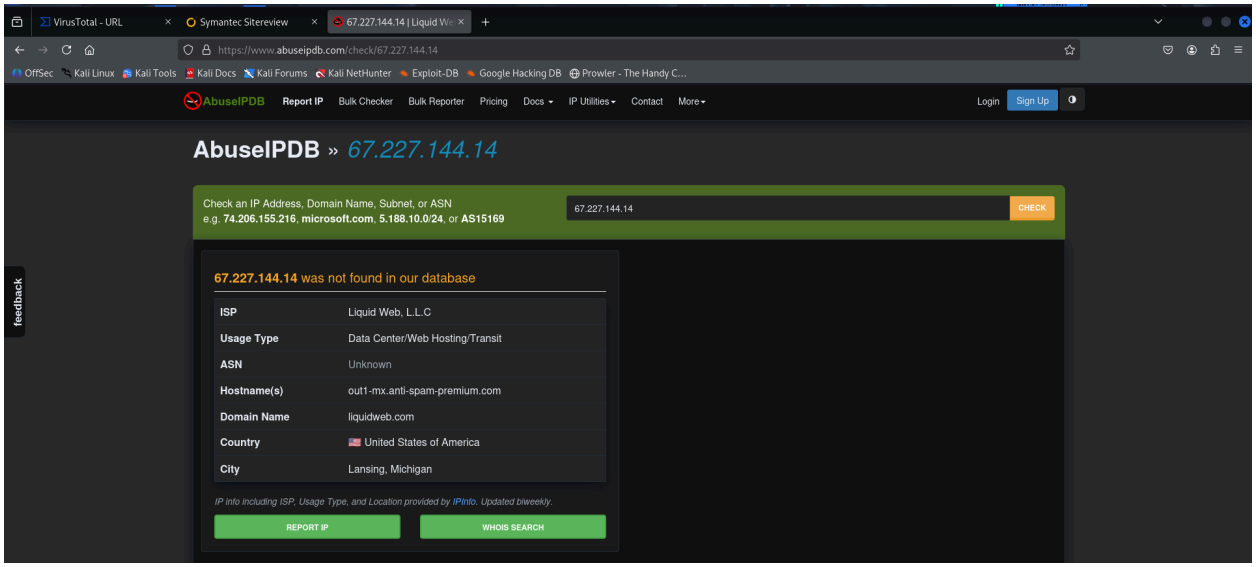
Sender Information

- **Return-Path:** f.fuentes@rennyconceptos.com
- **From- Path:** PH0PR19MB4905.namprd19.prod.outlook.com (::1)

NOTE: This is a red flag because the **from-path and return-path** does not match or does not belong to the same organization.

- **Sender IP Address**: 67.227.144.14

IP Reputation Check (AbuseIPDB): No existing reports were found for this IP address in the AbuseIPDB database. However, the lack of reports does not indicate safety, especially given the suspicious context.

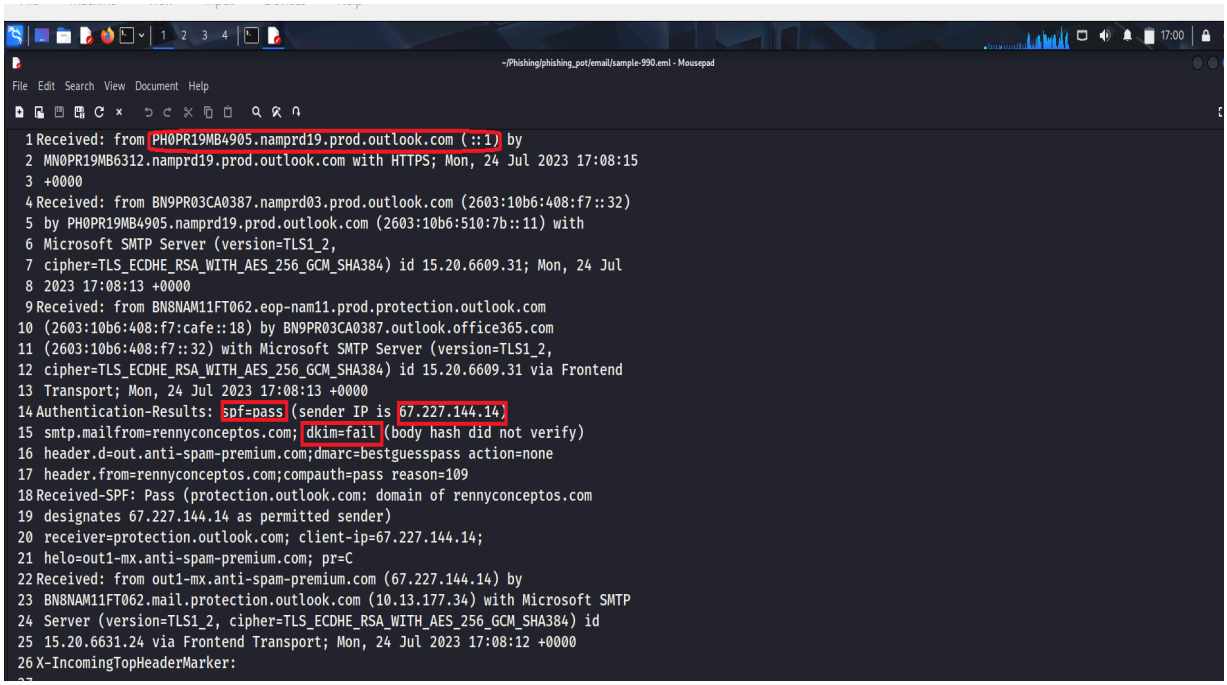


Email Authentication Results

- **SPF (Sender Policy Framework)**: PASS
  - The SPF record validated successfully, suggesting that the sending server is authorized to send mail on behalf of the domain. However, SPF alone is not a reliable indicator of legitimacy.

- **DKIM (DomainKeys Identified Mail)**: FAIL
  - No DKIM signature failed, indicating the email was not cryptographically signed. This reduces the credibility and makes the email susceptible to spoofing.

- **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**: NONE
  - The domain lacks a DMARC policy, increasing the likelihood of unauthorized use and spoofing.

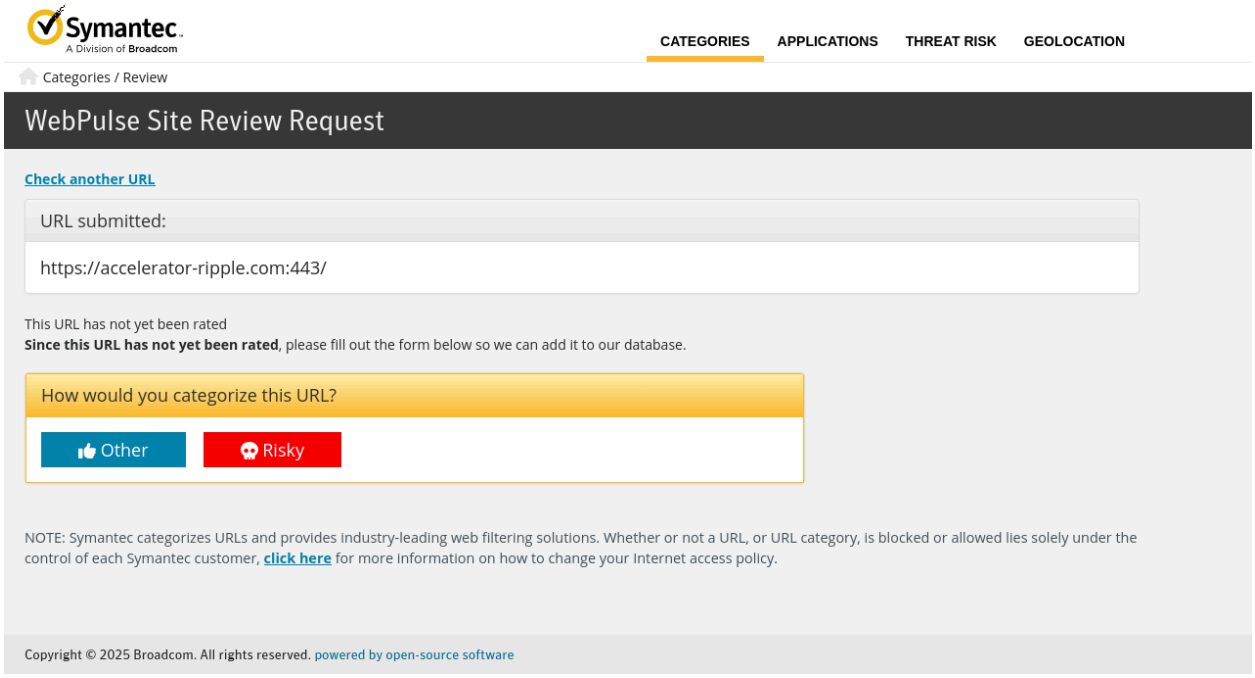



```
5  smtp.mailfrom=rennyconceptos.com; dkim=fail (body hash did not verify)
6  header.d=out.anti-spam-premium.com;dmarc=bestguesspass action=none
```

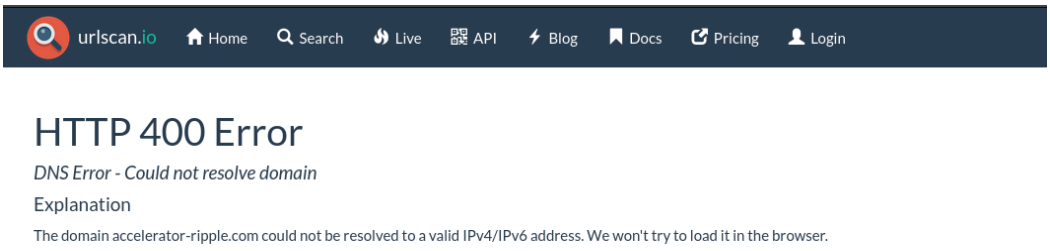
Embedded URL Analysis

Suspicious Link

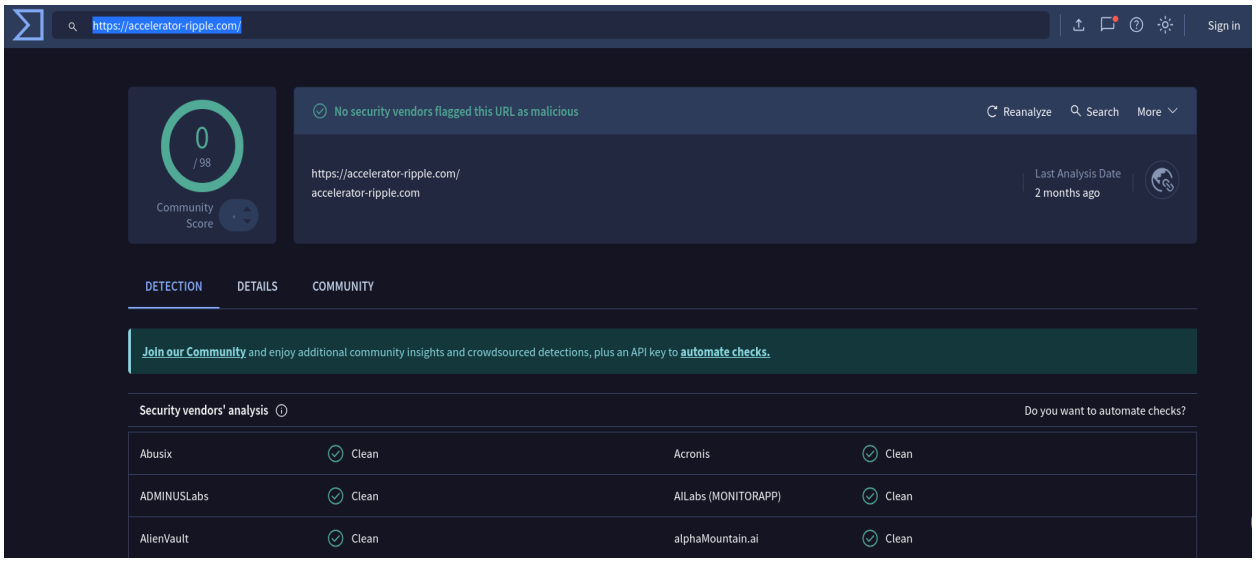
- **The embedded URL which is : https://accelerator-ripple.com/ was tested using.**



- I extracted the link and performed scans using the following tools:
  - **URLScan.io**



- **VirusTotal**



Threat Intelligence Analysis

IP Address Reputation

- **IP Address**: 67.227.144.14
- The IP address did not return any reports on AbuseIPDB. However, attackers often rotate IPs and domains, so absence of prior activity does not imply trustworthiness.

Indicators of Compromise (IoCs)

- **Email Header Anomalies**: Missing DKIM/DMARC, mismatched Return-Path and sending server.
- **Malicious URL**: The URL embedded in the email links to a suspicious domain.
- **Unusual Return-Path Domain**: f.fuentes@rennyconceptos.com is a non-standard and suspicious domain name.

Conclusion

Based on comprehensive email header inspection, authentication failures, and third-party threat intelligence scans, I assess this email to be a **confirmed phishing attempt**. The email was crafted to trick recipients into clicking a potentially malicious link. The domain and IP involved exhibit red flags consistent with phishing infrastructure.

Recommendations

- **Immediate Quarantine**: Ensure the email is removed from all user inboxes.
- **Block Indicators**: Add **https://accelerator-ripple.com/** and 67.227.144.14 to all perimeter security blocklists (firewall, proxy, email gateway).
- **Report to Authorities**: Submit indicators to APWG and Google Safe Browsing.
- **Security Awareness Campaign**: Notify users about this phishing attempt and reinforce phishing awareness training.
- **Enhance Email Filtering**: Strengthen email gateway rules to enforce strict DMARC/DKIM/SPF policies.
- **Threat Hunting**: Initiate monitoring of internal logs and endpoints for any interaction with the flagged domain/IP.