

Phishing Email Analysis Report

Prepared By:

Emmanuel Olajoseph

Date: 26th Dec, 2025

Executive Summary

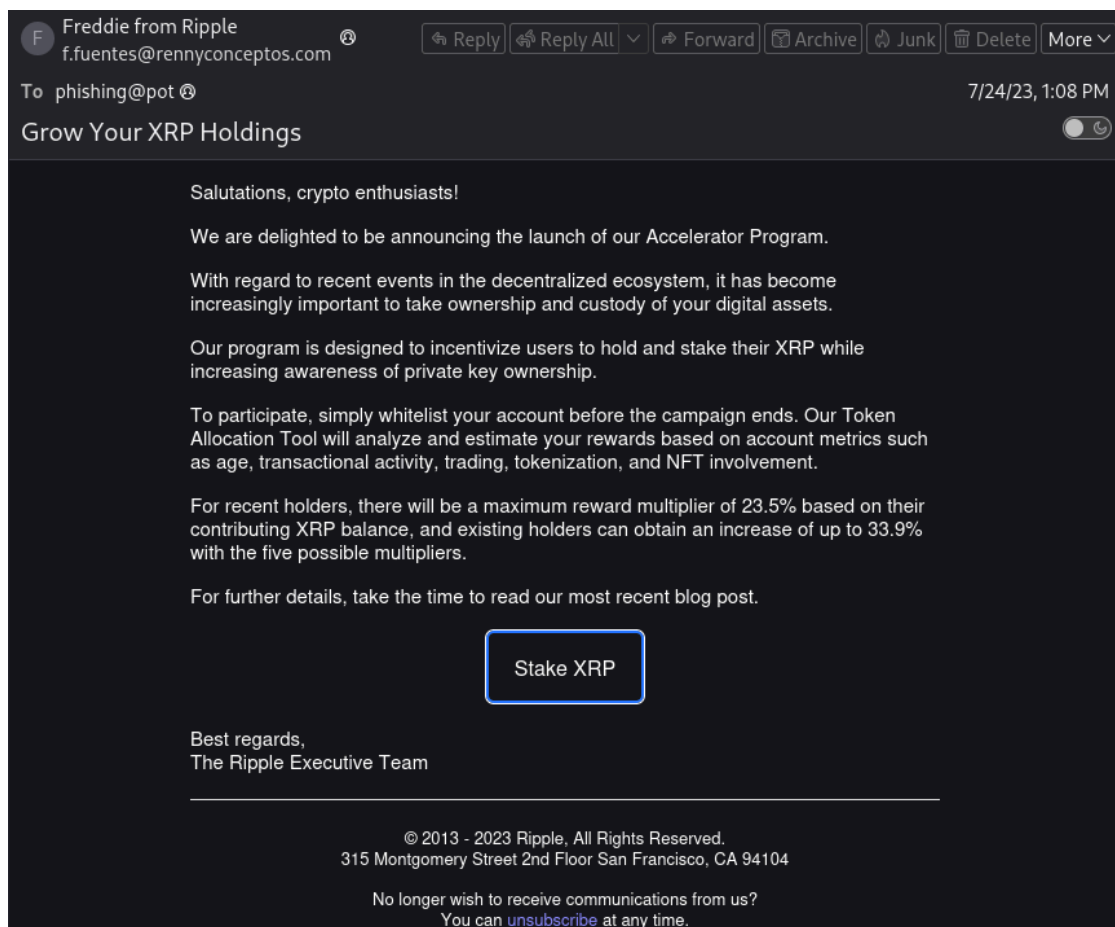
Conducted an in-depth analysis of a suspicious email received through the corporate email gateway. The email was isolated in a sandboxed virtual environment and subjected to multi-layered analysis techniques, including header inspection, URL reputation analysis, and threat intelligence gathering. Based 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**](https://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

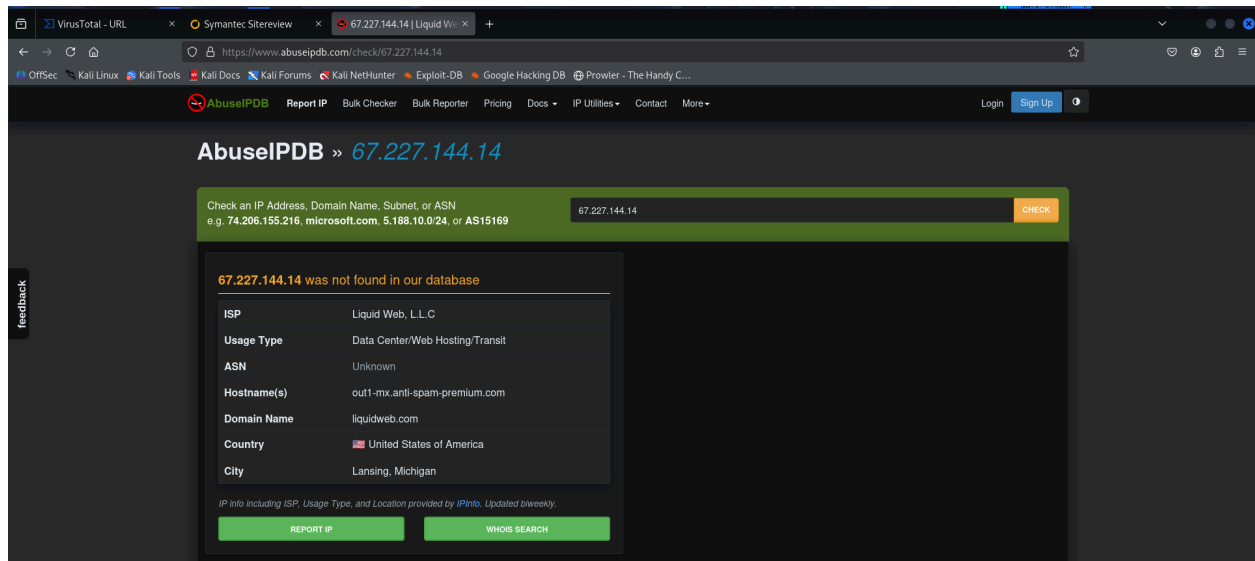
Sender Information

- **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.

```
File Edit Search View Document Help
~Phishing\phishing_pot\email\sample-950.eml - Mousepad

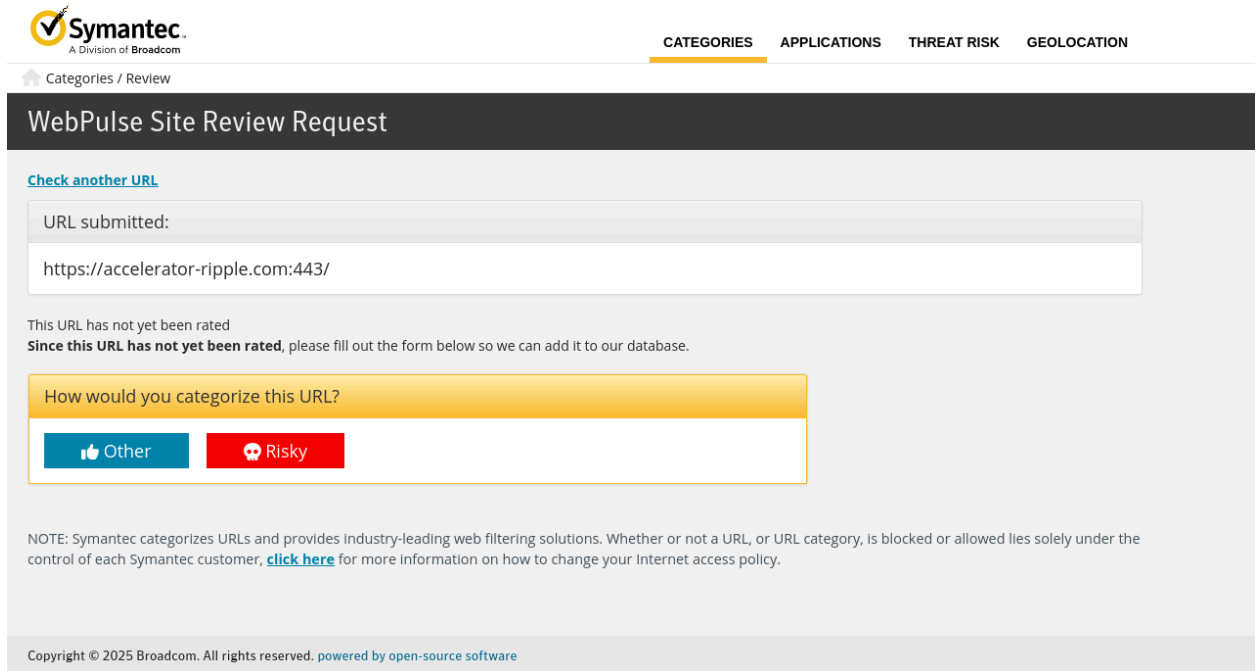
1 Received: from PH0PR19MB4905.namprd19.prod.outlook.com (::1) by
2 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Mon, 24 Jul 2023 17:08:15
3 +0000
4 Received: from BN9PR03CA0387.namprd03.prod.outlook.com (2603:10b6:408:f7::32)
5 by PH0PR19MB4905.namprd19.prod.outlook.com (2603:10b6:510:7b::11) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6609.31; Mon, 24 Jul
8 2023 17:08:13 +0000
9 Received: from BN8NAM11FT062.eop-nam11.prod.protection.outlook.com
10 (2603:10b6:408:f7:cafe::18) by BN9PR03CA0387.outlook.office365.com
11 (2603:10b6:408:f7::32) with Microsoft SMTP Server (version=TLS1_2,
12 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6609.31 via Frontend
13 Transport; Mon, 24 Jul 2023 17:08:13 +0000
14 Authentication-Results: spf=pass (sender IP is 67.227.144.14);
15 smtp.mailfrom=rennyconceptos.com; dkim=fail (body hash did not verify)
16 header.d=out.anti-spam-premium.com; dmarc=bestguesspass action=none
17 header.from=rennyconceptos.com; compauth=pass reason=109
18 Received-SPF: Pass (protection.outlook.com: domain of rennyconceptos.com
19 designates 67.227.144.14 as permitted sender)
20 receiver=protection.outlook.com; client-ip=67.227.144.14;
21 helo=out1-mx.anti-spam-premium.com; pr=C
22 Received: from out1-mx.anti-spam-premium.com (67.227.144.14) by
23 BN8NAM11FT062.mail.protection.outlook.com (10.13.177.34) with Microsoft SMTP
24 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
25 15.20.6631.24 via Frontend Transport; Mon, 24 Jul 2023 17:08:12 +0000
26 X-IncomingTopHeaderMarker:
```

```
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.



The screenshot shows the Symantec WebPulse Site Review Request interface. At the top, the Symantec logo is displayed with the tagline 'A Division of Broadcom'. Navigation tabs include 'CATEGORIES', 'APPLICATIONS', 'THREAT RISK', and 'GEOLOCATION'. Below the header, a breadcrumb trail shows 'Categories / Review'. The main heading is 'WebPulse Site Review Request'. A link 'Check another URL' is present. A form field labeled 'URL submitted:' contains the text 'https://accelerator-ripple.com:443/'. Below this, a message states: 'This URL has not yet been rated. Since this URL has not yet been rated, please fill out the form below so we can add it to our database.' A yellow box asks 'How would you categorize this URL?'. Below this are two buttons: 'Other' (blue) and 'Risky' (red). A note at the bottom explains that Symantec categorizes URLs and provides web filtering solutions, and that whether a URL is blocked or allowed is under the control of each Symantec customer, with a link to 'click here' for more information. The footer contains copyright information: 'Copyright © 2025 Broadcom. All rights reserved. powered by open-source software'.

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



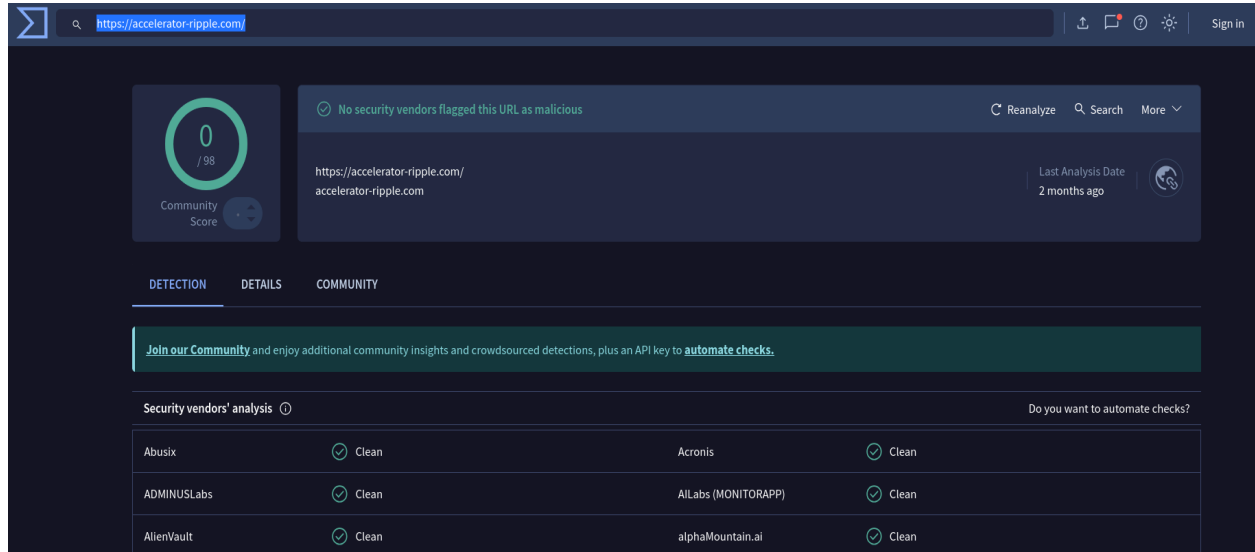
HTTP 400 Error

DNS Error - Could not resolve domain

Explanation

The domain accelerator-ripple.com could not be resolved to a valid IPv4/IPv6 address. We won't try to load it in the browser.

o 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.