Email Phishing Analysis Report

BY

Ajayi, Emmanuel Oluwagbenga

Cybersecurity Analyst

July, 2025

Table of Contents

1. INTRODUCTION

This report presents a phishing email analysis involving a suspicious message impersonating Ripple. The email contained misleading branding and a suspicious link designed to redirect recipients to a fake login page, likely for credential harvesting.

I performed a structured analysis of the email header, content, and embedded URL using a combination of automated tools (PhishTool, whois, urlscan) and manual techniques. The analysis was conducted in a safe virtual machine environment to identify possible indicators of compromise and better understand the phishing tactics used.

2. OBJECTIVES

To analyze the components of the suspicious email.

To identify phishing indicators using headers, metadata, and embedded URLs.

To document the findings in a professional format suitable for incident response and training purposes.

3. Email Metadata Overview

Headers

Date: Thu, 27 Jul 2023 15:06:03

Subject: More benefits from Ripple with the Allocation Program

To:phishing@pot

From: CoinDesk <coindesk@mg.areafellowship.com>

Reply-To: None

Return-Path: bounce+d293ba.20bffc-phishing@pot=hotmail.com@mg.areafellowship.com

Sender IP: 198.61.254.55

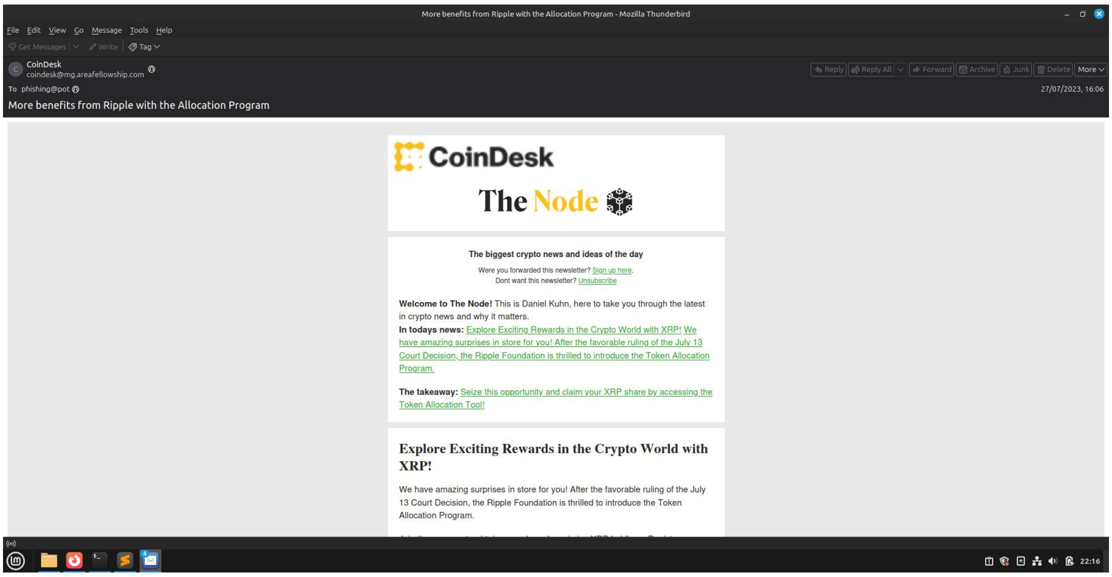
Message-ID: <20230727150603.c2011bfd5c8933f6@mg.areafellowship.com>

URLs (defanged form to avoid mistakenly clicked)

hxxps://www[.]coindesk[.]com/newsletters/

hxxps://www[.]coindesk[.]com/newsletters/unsubscribe/

hxxps://mail123ripple[.]net/726f6472696f726662d704068674d661696c2e636f6d?c_id=coindesk-27bc8277-ccf1-411d-bb5b-1281a7728da9


More benefits from Ripple with the Allocation Program - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More

CoinDesk
coindesk@mg.areafellowship.com

To phishing@pot

27/07/2023, 16:06

More benefits from Ripple with the Allocation Program

CoinDesk

The Node

The biggest crypto news and ideas of the day

Were you forwarded this newsletter? Sign up here.
Dont want this newsletter? Unsubscribe

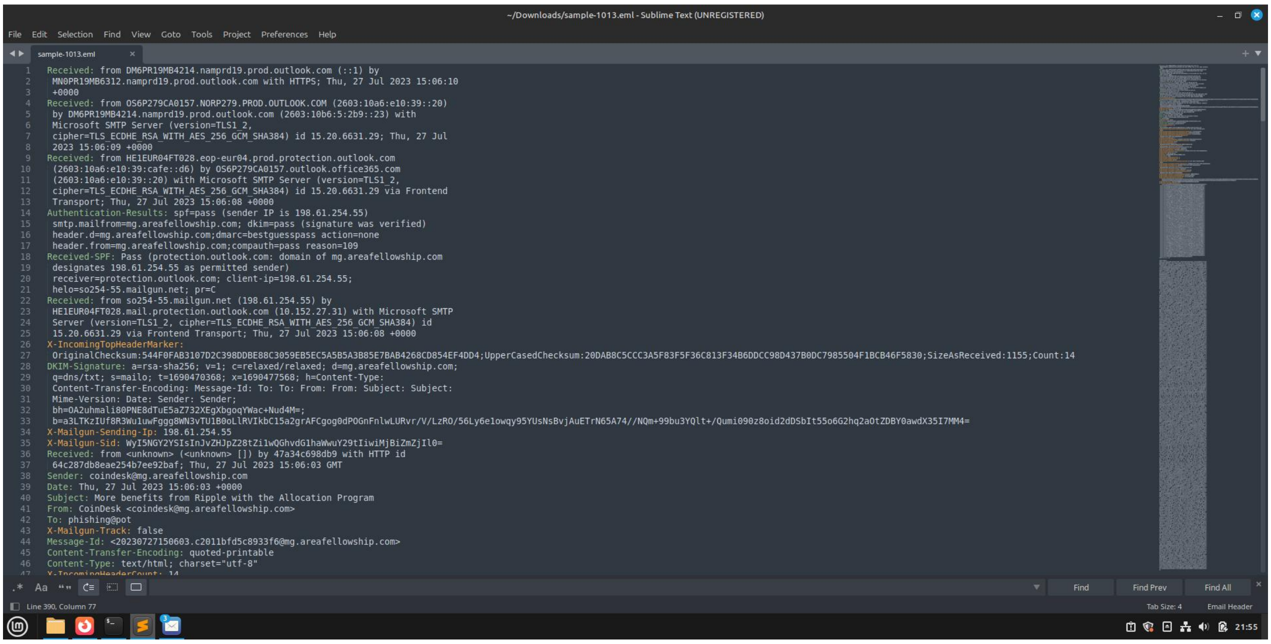
Welcome to The Node! This is Daniel Kuhn, here to take you through the latest in crypto news and why it matters.
In todays news: Explore Exciting Rewards in the Crypto World with XRP! We have amazing surprises in store for you! After the favorable ruling of the July 13 Court Decision, the Ripple Foundation is thrilled to introduce the Token Allocation Program.

The takeaway: Seize this opportunity and claim your XRP share by accessing the Token Allocation Tool!

Explore Exciting Rewards in the Crypto World with XRP!

We have amazing surprises in store for you! After the favorable ruling of the July 13 Court Decision, the Ripple Foundation is thrilled to introduce the Token Allocation Program.

Fig1: Email body preview


~/Downloads/sample-1013.eml - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
sample-1013.eml
Find
Find Prev
Find All
Line 390, Column 77
Tab Size: 4
Email Header
21:55

```
Received: from DM6PR19MB4214.namprd19.prod.outlook.com (::1) by
 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Thu, 27 Jul 2023 15:06:10
 +0000
Received: from OS6P279CA0157.NORP279.PROD.OUTLOOK.COM (2603:10a6:e10:39::20)
 by DM6PR19MB4214.namprd19.prod.outlook.com (2603:10b6:5:2b9::23) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.29; Thu, 27 Jul
 2023 15:06:09 +0000
Received: from HE1EUR04FT028.eop-eur04.prod.protection.outlook.com
 (2603:10a6:e10:39:cafe::d6) by OS6P279CA0157.outlook.office365.com
 (2603:10a6:e10:39::20) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.29 via Frontend
 Transport; Thu, 27 Jul 2023 15:06:08 +0000
Authentication-Results: spf=pass (sender IP is 198.61.254.55)
 smtp.mailfrom=mg.areafellowship.com; dkim=pass (signature was verified)
 header.d=mg.areafellowship.com;dmarc=bestguesspass action=none
 header.from=mg.areafellowship.com;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of mg.areafellowship.com
 designates 198.61.254.55 as permitted sender)
 receiver=protection.outlook.com; client-ip=198.61.254.55;
 helo=so254-55.mailgun.net; pr=C
Received: from so254-55.mailgun.net (198.61.254.55) by
 HE1EUR04FT028.mail.protection.outlook.com (10.152.27.31) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6631.29 via Frontend Transport; Thu, 27 Jul 2023 15:06:08 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:544F0FAB3107D2C398DDBE88C3059EB5EC5A5B5A3B85E7BAB4268CD854EF4DD4;UpperCasedChecksum:20DAB8C5CCC3A5F83F5F36C813F34B6DDCC98D437B0DC7985504F1BCB46F5830;SizeAsReceived:1155;Count:14
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mg.areafellowship.com;
 q=dns/txt; s=mailo; t=1690470368; x=1690477568; h=Content-Type:
 Content-Transfer-Encoding: Message-Id: To: To: From: From: Subject: Subject:
 Mime-Version: Date: Sender: Sender;
 bh=OA2uhmali80PNE8dTuE5aZ732XEgXbgoqYWac+Nud4M=;
 b=a3LTKzIUf8R3Wu1uwFggg8WN3vTU1B0oLlRVIkbC15a2grAFCgog0dPOGnFnlwLURvr/V/LzRO/56Ly6e1owqy95YUsNsBvjAuETrN65A74//NQm+99bu3YQlt+/Qumi090z8oid2dDSbIt55o6G2hq2aOtZDBY0awdX35I7MM4=
X-Mailgun-Sending-Ip: 198.61.254.55
X-Mailgun-Sid: WyI5NGY2YSIsInJvZHJpZ28tZi1wQGhvdG1haWwuY29tIiwiMjBiZmZjIl0=
Received: from <unknown> (<unknown> []) by 47a34c698db9 with HTTP id
 64c287db8eae254b7ee92baf; Thu, 27 Jul 2023 15:06:03 GMT
Sender: coindesk@mg.areafellowship.com
Date: Thu, 27 Jul 2023 15:06:03 +0000
Subject: More benefits from Ripple with the Allocation Program
From: CoinDesk <coindesk@mg.areafellowship.com>
To: phishing@pot
X-Mailgun-Track: false
Message-Id: <20230727150603.c2011bfd5c8933f6@mg.areafellowship.com>
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"
X-IncomingHeaderCount: 14
```

Fig 2: Email header view (Raw source)

4. Phishing Indicators

4.1. Sender Spoofing and Domain Mismatch

The sender address appears as “CoinDesk,” a well-known cryptocurrency news outlet. However, the actual sending domain (mg.areafellowship.com) is unrelated to CoinDesk and is likely a compromised or fraudulent mail server.

4.2. Return Path and Header Inconsistencies

The return path contains suspicious formatting with broken syntax and obfuscated elements such as phishing@pot=hotmail.com. This is a common tactic used by attackers to manipulate return emails and evade filters.

4.3. Suspicious Link (Main Phishing Indicator)

A malicious-looking link is embedded within the email body:

hxxps://mail123ripple[.]net/726f6472696f726662d704068674d661696c2e636f6d

This domain mimics Ripple branding (mail123ripple.net) but fails DNS resolution, suggesting it is not legitimate and may have been disabled or taken offline.

4.4. Lack of Reply-To Field

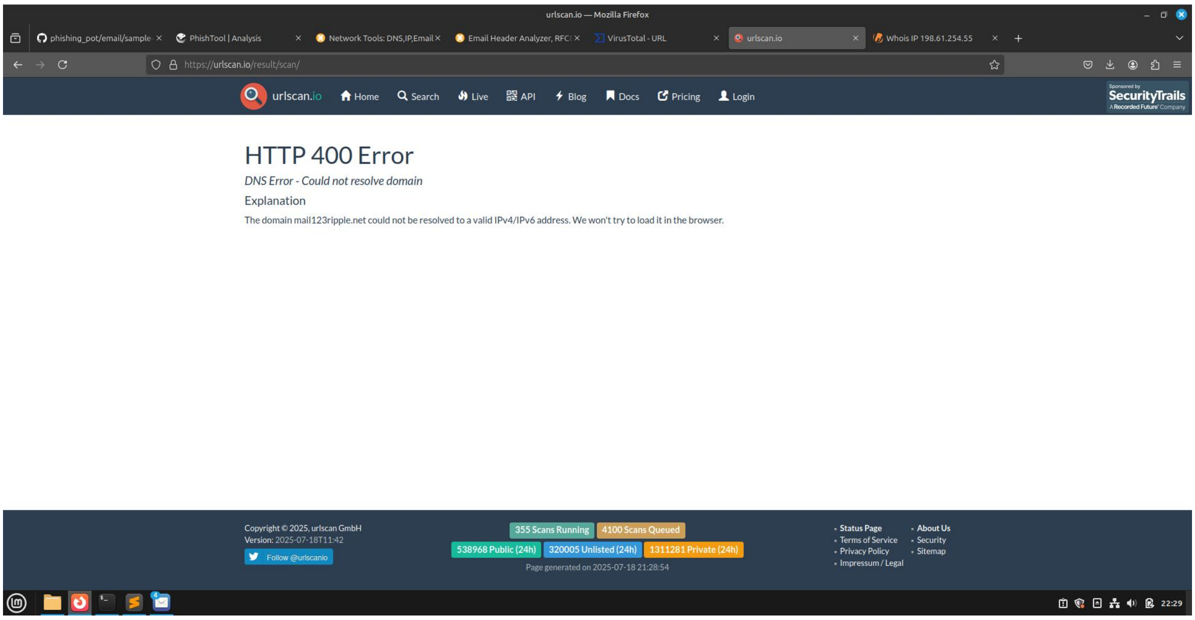
The email lacks a reply-to address, which is abnormal for legitimate promotional or transactional emails, further indicating suspicious intent.

5. Link Analysis

Embedded URLs in the Email:

URL	Status	Purpose
hxxps://www[.]coindesk[.]com/newsletters/	Legitimate	CoinDesk newsletter home
hxxps://www[.]coindesk[.]com/newsletters/unsubscribe/	Legitimate	Unsubscribe link
hxxps://mail123ripple[.]net/...	Suspicious/Malicious	Possible phishing page or malware dropper

The presence of legitimate CoinDesk links alongside the malicious domain is a blending tactic used to bypass basic security checks and to increase trustworthiness in the eyes of the recipient.



urlscan.io — Mozilla Firefox
phishing_pot/email/sample-
PhishTool | Analysis
Network Tools: DNS,IP,Email
Email Header Analyzer, RFC
VirusTotal - URL
urlscan.io
Whois IP 198.61.254.55
https://urlscan.io/result/scan/
urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
Sponsored by SecurityTrails A Recorded Future Company

HTTP 400 Error

DNS Error - Could not resolve domain

Explanation

The domain mail123ripple.net could not be resolved to a valid IPv4/IPv6 address. We won't try to load it in the browser.

Fig 3: url.io scan result for the domain

"HTTP 400 Error – DNS Error - Could not resolve domain"

means that the domain mail123ripple.net does not currently exist on the internet (or is completely unreachable). Here's what it means in simpler terms:

DNS Error:

DNS (Domain Name System) is like the internet's phonebook. When you type in a domain name (like mail123ripple.net), DNS translates it into an IP address so your computer can connect to it.

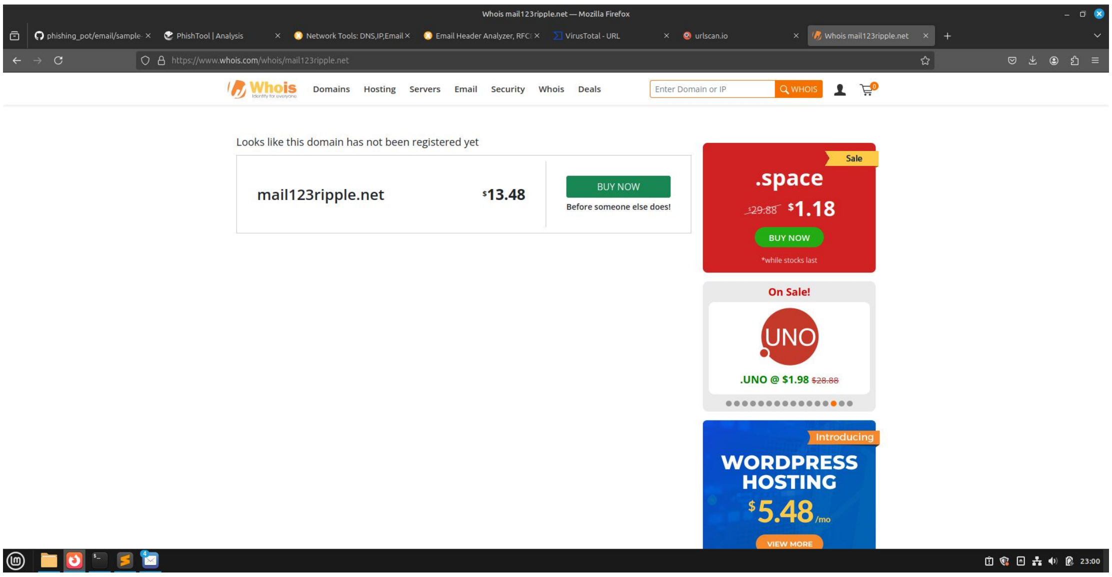
"Could not resolve" means that DNS couldn't find any IP address for that domain, it's like looking up a phone number and finding that the person isn't listed.

Could not be resolved to a valid IPv4/IPv6 address:

This means no computer/server is currently associated with that domain.

HTTP 400 Error:

This is a Bad Request error. Often, it's because the server didn’t understand the request due to a malformed URL, but in this context, it's likely a generic fallback message because the domain is unreachable.



Whois mail123ripple.net — Mozilla Firefox
phishing_pot/email/sample
PhishTool | Analysis
Network Tools: DNS,IP,Email
Email Header Analyzer, RFC
VirusTotal - URL
urlscan.io
Whois mail123ripple.net
https://www.whois.com/whois/mail123ripple.net
Whois
Identity for everyone
Domains
Hosting
Servers
Email
Security
Whois
Deals
Enter Domain or IP
WHOIS
0

Looks like this domain has not been registered yet

mail123ripple.net $13.48

BUY NOW

Before someone else does!

Fig 4: whois result for the domain

Since WHOIS.io shows:

"This domain has not been registered"

It confirms that:

The domain mail123ripple.net is unregistered, it's not currently owned by anyone.

This could mean:

The attacker used a fake or typo-ed domain and never actually registered it (possibly trying to trick users with visual similarity).

Or, the domain was registered before, used for phishing, and has since been deactivated or removed due to abuse reports.

6. Email Authentication Checks

Authentication Method	Result	Interpretation
SPF	Pass	The sending IP (198.61.254.55) is authorized by the domain areafellowship.com to send emails. This means the email came from an approved server for that domain.
DKIM	Neutral	A DKIM signature was present but not aligned or not verified successfully. This could be due to a misconfigured signing domain or replayed email.
DMARC	None	The domain areafellowship.com has no DMARC policy published, making it difficult to enforce domain alignment or prevent spoofing effectively.

While the SPF check passed, indicating that the IP was authorized to send email on behalf of the domain, the neutral DKIM result and the absence of a DMARC policy leave significant gaps in security. These results mean:

SPF pass alone is not enough: Without DKIM and DMARC enforcement, attackers could still spoof the sender or misuse the domain without detection.

Neutral DKIM may signal poor email hygiene or malicious use of weak signing practices.

No DMARC policy makes the domain vulnerable to impersonation, as there’s no instruction for receiving servers on how to handle failures.

7. Indicators of Compromise (IOCs)

The following IOCs were extracted from the phishing email and its headers. These indicators may be used for threat detection, email filtering, domain blocking, and further investigation.

Type	Indicator	Description
Sender Email	coindesk@mg.areafellowship.com	Spoofed sender impersonating CoinDesk via unauthorized domain
Return Path	bounce+d293ba.20bffc-phishing@pot=hotmail.com@mg.areafellowship.com	Obfuscated return address used to bypass email filters
Sending IP	198.61.254.55	IP address used to send the email; possibly a compromised server
Phishing URL	hxxps://mail123ripple[.]net/726f6472696f726662d704068674d661696c2e636f6d	Malicious link disguised as Ripple; may lead to phishing/malware site
Domain	mail123ripple.net	Lookalike domain impersonating Ripple; not resolving via DNS

8. Conclusion

The analyzed email is a clear phishing attempt that leverages brand impersonation, specifically CoinDesk and Ripple, combined with deceptive social engineering tactics to lure recipients into clicking a malicious link. While SPF authentication passed, the DKIM result was neutral, and the domain lacked a DMARC policy, leaving the sender domain vulnerable to spoofing and unauthenticated email delivery.

The phishing link (mail123ripple.net) mimics Ripple branding and was designed to appear legitimate, likely with the intent of stealing credentials or delivering malware. Additionally, the email included legitimate CoinDesk URLs, a common tactic known as blending, which threat actors use to increase the credibility of their messages and evade detection by filters.

If successful, this phishing campaign could result in compromised user credentials, unauthorized access to cryptocurrency platforms, or financial data breaches. These findings highlight the critical importance of layered email security, including strict SPF/DKIM/DMARC enforcement, continuous domain monitoring, and regular phishing awareness training for end users.

9. Recommendations

Do not click on any links in such emails.

Block the sender domain mg.areafellowship.com and associated IP 198.61.254.55.

Report the incident to security teams and phishing databases.

Educate users within your organization about such blended phishing techniques.

Implement strict SPF, DKIM, and DMARC policies in your organization to help prevent spoofing.