Phishing Analysis Report - 002

Case Number: 002
Report By: Rishab H Shorey
Documented on: 11/12/2025
File Name: Sample_1007.eml
File Link:

Headers

==========

Language:
English

Date of Email:
August 27, 2023

To: phishing@pot
From: xrpl@isarops.com

Subject Line:
Good news and rewards for the XRP Community

Return-Path:
bounce+5384b0.912432-phishing@pot=hotmail.com@isarops.com

Sender IP:
198.61.254.42

ASN Information
AS19994 **RACKSPACE**, **US** (registered Jan 15, 2010)

Resolve Host:

Message-ID:
<20230727082311.9d0b426cad4b843b@isarops.com>

E-Mail Authentication Details
SPF Authentication spf=pass (sender IP is 198.61.254.42)
smtp.mailfrom=isarops.com;
DKIM Authentication dkim=pass (signature was verified)
DMARC Authentication: dmarc=pass action=none
header.from=isarops.com;
Composite Authentication: compauth=pass reason=100

URLs

==========

Fanged URL:
hxxps[://]mail122-ripple[.]net/726f647269676f2d662d7040686f746d61696c2e636f6d?c_id=r25j-9d981df1-f2da-41f0-99da-41da09f42b72

Attachments

==========

Attachment Name:
N/A

Attachment Link:

MD5:
N/A

SHA1:
N/A

SHA256:
N/A

Description

==========

Starting with about the mail:
The attacker is tempting the user into download and access a tool by registering to click on a link which is more likely a phish. Kindly refer the URL artifact to understand the kind of attack.

The sender mail domain has no connection with Ripple whatsoever which shows an important IOC mentioned.

Based on header security analysis, we are able to see that it has been able to pass all the security authentication checks SPF, DKIM, DMARC all were a **clear green flag**, but the domain is unreliable as it is attempting to impersonate a legitimate financial service in India.

Tools Used For Analysis

==========

- Virus Total
- Url2png
- urlvoid
- Cisco Thalos Intelligence
- Google Safe Browsing
- Threat Cop

Artifact Analysis

==========

Sender Analysis:
The attacker is trying to impersonate Ripple, it is one of the financial services company of India. The mail is trying to trick users into **XRP Token Allocation** which based more on blockchain, it probably shall lead to NFT Mining, or trading. This is more based for investors, and hence they could potentially send it to large pool of people.

Fanged URL:
hxxps[://]mail122-ripple[.]net/726f647269676f2d662d7040686f746d61696c2e636f6d?c_id=r25j-9d981df1-f2da-41f0-99da-41da09f42b72

URL Analysis:
Link is not hashed or coded into any of hashing algorithms or operations.

The domain used by Ripple belongs to .com for the TLD but based on the customer care services it is noted that the subdomain belongs to .in which is different. Checking the customer web pages.

The body of the mail talks about registering for a tool to gain access and XRP points but, subdomain shows a link which is poorly crafted for a mail redirect. After using tools, we have also established that the first page it gets redirected to is the google which is suspicious for sure.

Refer the image for proof.

Attachment Analysis:
n/a

Verdict

==========

Considering the header analysis, URL analysis:

- **Header Analysis** suggests that the redirection of domain is nowhere related to the actual purpose of what the mail is sent from. The subdomain and domain is both misleading and doesn't show any relevance with actual company. It is an abuse of existing service to trick the user.

- **URL Analysis**: suggests that This link is a possible **malware** after confirming we have few vendors that shows pinch of positive signs score for malware, while on the other hand there are vendors that says it is safe to use, but since upon clicking the domain redirects to another webpage it is just some backend play which is taking place through the link.

E-Mail Classification (Based on Attachment, Links or Redirect)

==========

Low (Easily Managed and closed)

Defense Actions

==========

I have ensured to block out the subdomain, and sent a notification to all of the users who are having an account in Ripple to be aware.

- Also sent an abuse report to Ripple warning about potential phishing attacks it can cause it users for big losses.

- Blocked out the IP address from the mail server and ensured that the mail system doesn't receive any kind of mail from an address.

Rishab . H . Shorey

_____

Image For Reference

==========

Attachment for Site Pictures: