Phishing Email Analysis Report

By:

Dayo Sonibare, Cybersecurity Analyst

Date: 24th March, 2025.

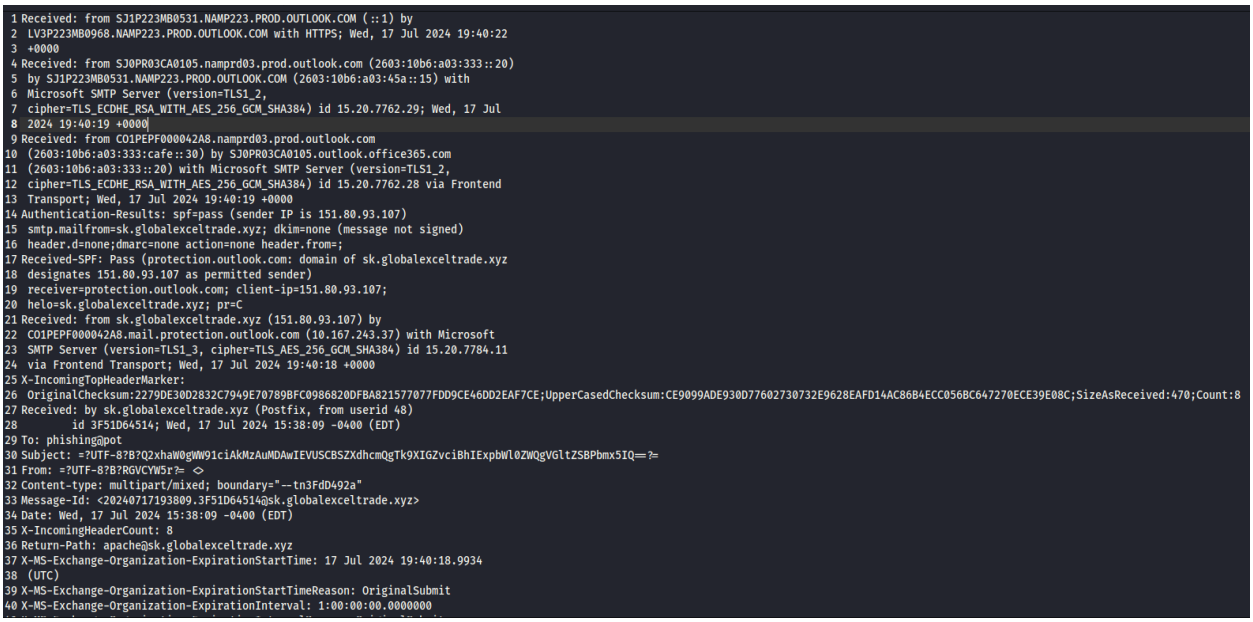
1. Executive Summary

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.

2. Email Metadata Analysis

2.1 Sender Information

- Return-Path: apache@sk.globalexceltrade.xyz
- Sending Server: SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (::1)
- Sender IP Address: 151.80.93.107
- 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.



```
Received: from SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (::1) by
 LV3P223MB0968.NAMP223.PROD.OUTLOOK.COM with HTTPS; Wed, 17 Jul 2024 19:40:22
 +0000
Received: from SJ0PR03CA0105.namprd03.prod.outlook.com (2603:10b6:a03:333::20)
 by SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:45a::15) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7762.29; Wed, 17 Jul
 2024 19:40:19 +0000
Received: from CO1PEPF000042A8.namprd03.prod.outlook.com
 (2603:10b6:a03:333:cafe::30) by SJ0PR03CA0105.outlook.office365.com
 (2603:10b6:a03:333::20) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7762.28 via Frontend
 Transport; Wed, 17 Jul 2024 19:40:19 +0000
Authentication-Results: spf=pass (sender IP is 151.80.93.107)
 smtp.mailfrom=sk.globalexceltrade.xyz; dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.from=;
Received-SPF: Pass (protection.outlook.com: domain of sk.globalexceltrade.xyz
 designates 151.80.93.107 as permitted sender)
 receiver=protection.outlook.com; client-ip=151.80.93.107;
 helo=sk.globalexceltrade.xyz; pr=C
Received: from sk.globalexceltrade.xyz (151.80.93.107) by
 CO1PEPF000042A8.mail.protection.outlook.com (10.167.243.37) with Microsoft
 SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.7784.11
 via Frontend Transport; Wed, 17 Jul 2024 19:40:18 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:2279DE30D2832C7949E70789BFC0986820DFBA821577077FDD9CE46DD2EAF7CE;UpperCasedChecksum:CE9099ADE930D77602730732E9628EAFD14AC86B4ECC056BC647270ECE39E08C;SizeAsReceived:470;Count:8
Received: by sk.globalexceltrade.xyz (Postfix, from userid 48)
        id 3F51D64514; Wed, 17 Jul 2024 15:38:09 -0400 (EDT)
To: phishing@pot
Subject: =?UTF-8?B?Q2xhaW0gWW91ciAkMzAuMDAwIEVUSCBSZXdhcmQgTk9XIGZvciBhIExpbWl0ZWQgVGltZSBPbmx5IQ==?=
From: =?UTF-8?B?RGVCYW5r?= <>
Content-type: multipart/mixed; boundary="--tn3FdD492a"
Message-Id: <20240717193809.3F51D64514@sk.globalexceltrade.xyz>
Date: Wed, 17 Jul 2024 15:38:09 -0400 (EDT)
X-IncomingHeaderCount: 8
Return-Path: apache@sk.globalexceltrade.xyz
X-MS-Exchange-Organization-ExpirationStartTime: 17 Jul 2024 19:40:18.9934
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
```

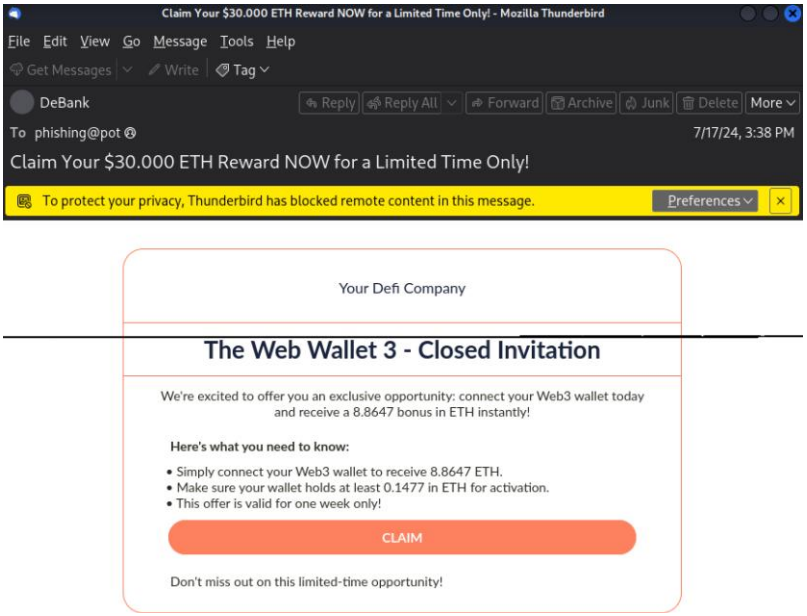
2.2 Email Authentication Results

- **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):** None
  - No DKIM signature was present, indicating the email was not cryptographically signed. This reduces 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.

3. Embedded URL Analysis

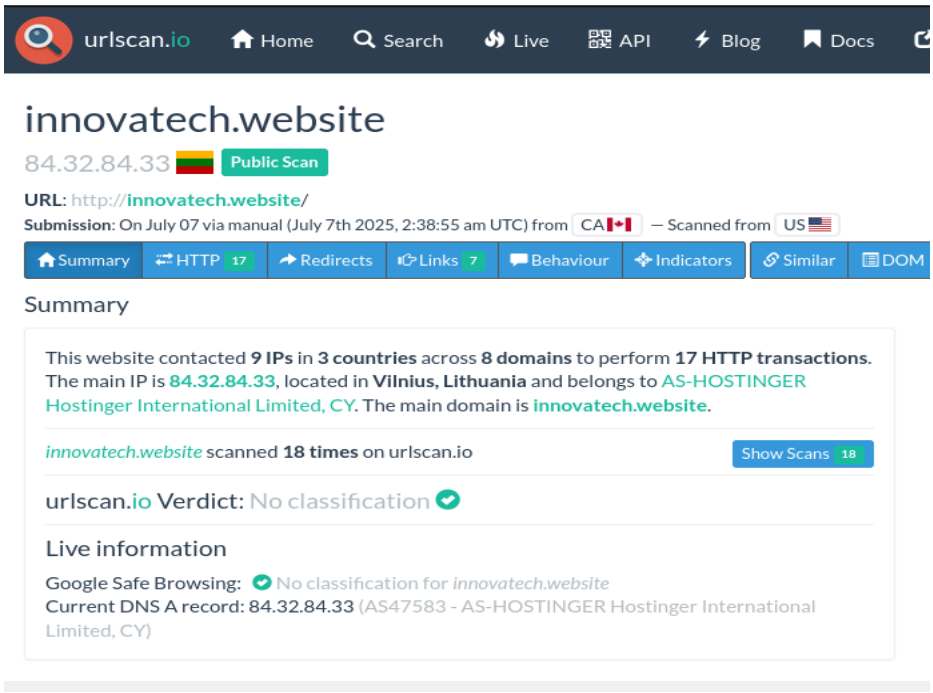
3.1 Suspicious Link

- **URL Found in Email:** https://innovatech.website

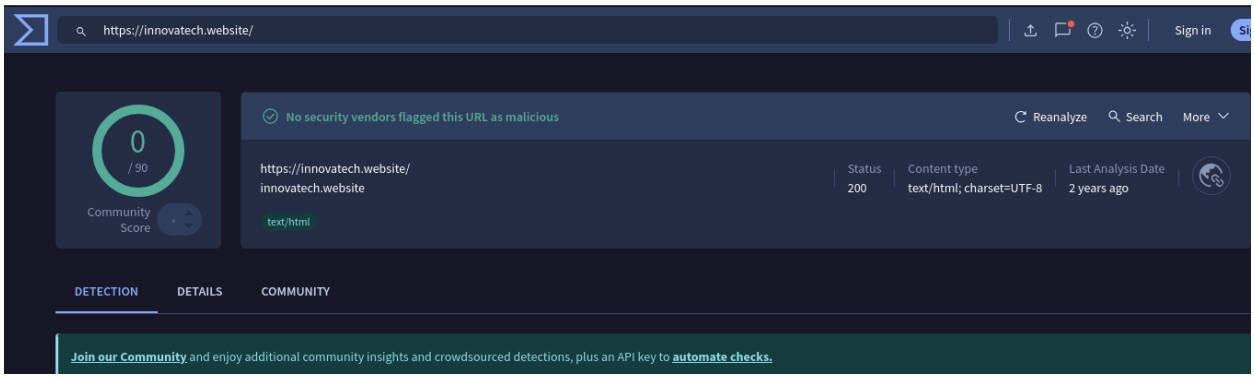


I extracted the link and performed scans using the following tools:

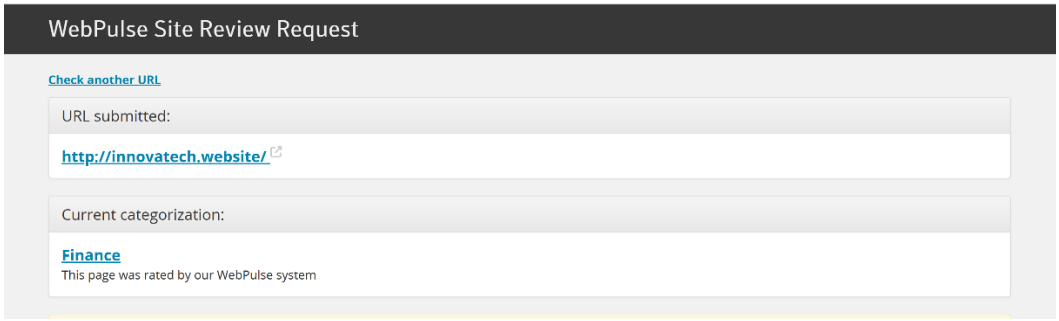
- **URLScan.io**



VirusTotal



Symantec Bluecoat Site Review



3.2 Threat Intelligence on Domain

- **Domain:** innovatech.website

A WHOIS lookup revealed:

Registrar: HOSTINGER operations, UAB

Registered On:2024-05-28

The domain appears to be newly registered and lacks a solid reputation, which is consistent with common phishing infrastructure.

4. Threat Intelligence Analysis

4.1 IP Address Reputation

- **IP Address:** 151.80.93.107
- 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.

4.2 IP Indicators of Compromises (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:** sk.globalexceltrade.xyz is a non-standard and suspicious domain name.

5. Conclusion & Recommendation

5.1 Conclusion

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

5.2 Recommendations

- **Immediate Quarantine:** Ensure the email is removed from all user inbox
- **Block Indicators:** Add innovatech.website and 151.80.93.107 to all perimeter security blocklists (firewall, proxy, email gateway).
- **Report to Authorities:**
    - Report the phishing attempt to Microsoft via the Security & Compliance Centre.
    - 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

Report Prepared by:
Dayo Sonibare
Cybersecurity Analyst