

Phishing Email Analysis Report

By:

Bolaji Bakare, Cybersecurity Analyst

Date: 24th Jan, 2026

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.

```
1 Received: from SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (::1) by
2 151P223MB0531.NAMP223.PROD.OUTLOOK.COM with HTTP(S) Wed, 17 Jul 2024 19:48:22
3 +0000
4 Received: from SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (2043:1806:a01:133::20)
5 by SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (2043:1806:a01:133::25) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.10.7762.29; Wed, 17 Jul
8 2024 19:48:22 +0000
9 Received: from C00PFP00004248-namp03.prod.outlook.com
10 (2043:1806:a01:133::cfe::10) by SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (2043:1806:a01:133::25) with Microsoft SMTP Server (version=TLS1_2,
11 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.10.7762.29 via Frontend
12 Transport; Wed, 17 Jul 2024 19:48:22 +0000
13 Authentication-Results: spfpass (sender IP is 151.80.93.107)
14 smtp.mailfrom=sk.globalexceltrade.xyz; dkim=none (message not signed)
15 header.from=sk.globalexceltrade.xyz; domain=sk.globalexceltrade.xyz
16 Received-SPF: Pass (protection.outlook.com: domain of sk.globalexceltrade.xyz
17 designates 151.80.93.107 as permitted sender)
18 receiver=protection.outlook.com; client-ip=151.80.93.107;
19 helo=sk.globalexceltrade.xyz; h=
20 Received: from sk-globalexceltrade.xyz (151.80.93.107) by
21 C00PFP00004248-namp03.prod.outlook.com (151.80.93.107) with Microsoft
22 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.10.7762.29
23 via Frontend Transport; Wed, 17 Jul 2024 19:48:22 +0000
24 X-IncomingTransportMarker:
25 OriginalChecksum:22700C180212C7F481F1998FC9806280F0A6215778777009CE40002AF7CE1cpperCaseChecksum:CE3999940E30077862732E9628AF7D54AC3684ECC9548C4727WCE39LWNC;SizeofReceived:479;Count:8
26 Received: by sk-globalexceltrade.xyz (Postfix, from user@a)
27 id 3F326A55A; Wed, 17 Jul 2024 19:48:22 -0400 (EDT)
28 To: phishlog@sk
29 Subject: <00F4781024xam000011006A00Ad1V55C32X0hcWg7N4K322v10N1Exp0W62WgV5A1258Pmc32>=h
30 From: <00F4781024xam000011006A00Ad1V55C32X0hcWg7N4K322v10N1Exp0W62WgV5A1258Pmc32>=h
31 Content-Type: multipart/mixed; boundary="=3F326A55A"
32 Message-Id: <00F4781024xam000011006A00Ad1V55C32X0hcWg7N4K322v10N1Exp0W62WgV5A1258Pmc32>=h
33 Date: Wed, 17 Jul 2024 19:48:22 -0400 (EDT)
34 X-IncomingTransportMarker:
35 Return-Path: apache@sk.globalexceltrade.xyz
36 X-MS-Exchange-Organization-ExpirationStartTime: 17 Jul 2024 19:48:16.9934
37 (UTC)
38 X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
39 X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
40 X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
41 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
42 X-MS-Exchange-Organization-AuthAs: Anonymous
43 X-MS-Exchange-Organization-AuthAs: Anonymous
44 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
45 X-MS-Exchange-Organization-AuthAs: Anonymous
46 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
47 X-MS-Exchange-Organization-AuthAs: Anonymous
48 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
49 X-MS-Exchange-Organization-AuthAs: Anonymous
50 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
51 X-MS-Exchange-Organization-AuthAs: Anonymous
52 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
53 X-MS-Exchange-Organization-AuthAs: Anonymous
54 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
55 X-MS-Exchange-Organization-AuthAs: Anonymous
56 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
57 X-MS-Exchange-Organization-AuthAs: Anonymous
58 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
59 X-MS-Exchange-Organization-AuthAs: Anonymous
60 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
61 X-MS-Exchange-Organization-AuthAs: Anonymous
62 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
63 X-MS-Exchange-Organization-AuthAs: Anonymous
64 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
65 X-MS-Exchange-Organization-AuthAs: Anonymous
66 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
67 X-MS-Exchange-Organization-AuthAs: Anonymous
68 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
69 X-MS-Exchange-Organization-AuthAs: Anonymous
70 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
71 X-MS-Exchange-Organization-AuthAs: Anonymous
72 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
73 X-MS-Exchange-Organization-AuthAs: Anonymous
74 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
75 X-MS-Exchange-Organization-AuthAs: Anonymous
76 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
77 X-MS-Exchange-Organization-AuthAs: Anonymous
78 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
79 X-MS-Exchange-Organization-AuthAs: Anonymous
80 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
81 X-MS-Exchange-Organization-AuthAs: Anonymous
82 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
83 X-MS-Exchange-Organization-AuthAs: Anonymous
84 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
85 X-MS-Exchange-Organization-AuthAs: Anonymous
86 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
87 X-MS-Exchange-Organization-AuthAs: Anonymous
88 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
89 X-MS-Exchange-Organization-AuthAs: Anonymous
90 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
91 X-MS-Exchange-Organization-AuthAs: Anonymous
92 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
93 X-MS-Exchange-Organization-AuthAs: Anonymous
94 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
95 X-MS-Exchange-Organization-AuthAs: Anonymous
96 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
97 X-MS-Exchange-Organization-AuthAs: Anonymous
98 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
99 X-MS-Exchange-Organization-AuthAs: Anonymous
100 X-MS-Exchange-Organization-AuthSource: sk-globalexceltrade.xyz
```

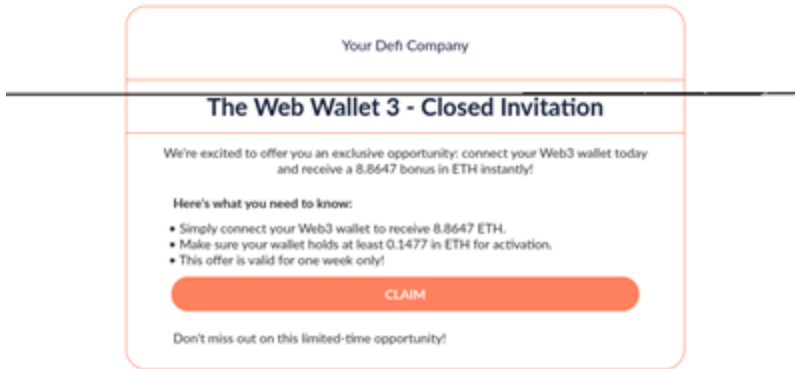
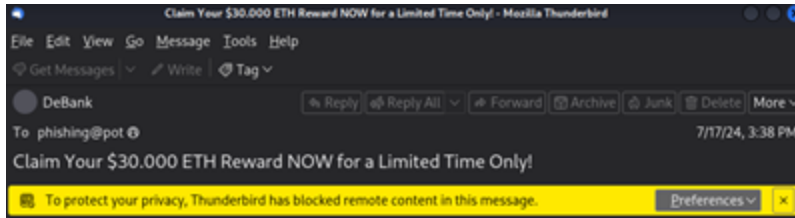
2.2 Email Authentication Results

- **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 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.

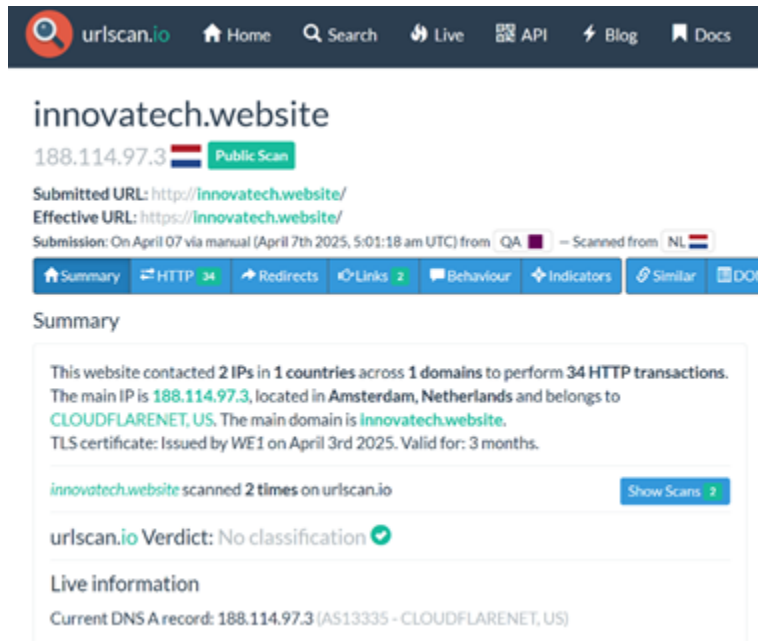
3. Embedded URL Analysis

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**



- **Bluecoat SiteReview**



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 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:** sk.globalexceltrade.xyz is a non-standard and suspicious domain name.

5. Conclusion & Recommendations

5.1 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 hosted at innovatech.website. The domain and IP involved exhibit red flags consistent with phishing infrastructure.

5.2 Recommendations

1. **Immediate Quarantine:** Ensure the email is removed from all user inboxes.
2. **Block Indicators:** Add innovatech.website and 151.80.93.107 to all perimeter security blocklists (firewall, proxy, email gateway).
3. **Report to Authorities:**
 - Report the phishing attempt to Microsoft via the Security & Compliance Center.
 - Submit indicators to APWG and Google Safe Browsing.
4. **Security Awareness Campaign:** Notify users about this phishing attempt and reinforce phishing awareness training.
5. **Enhance Email Filtering:** Strengthen email gateway rules to enforce strict DMARC/DKIM/SPF policies.
6. **Threat Hunting:** Initiate monitoring of internal logs and endpoints for any interaction with the flagged domain/IP.