

Phishing Email Analysis Report

By:

Bolaji Bakare, Cybersecurity Analyst

Date: 24th Jan, 2026

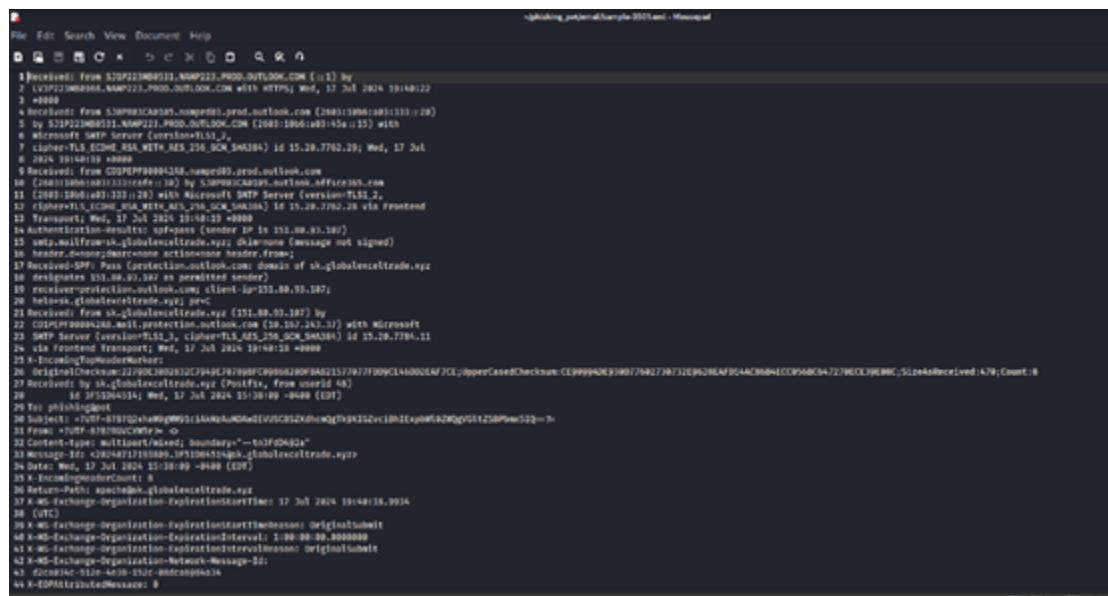
1. Executive Summary

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.



The screenshot shows a Microsoft Word document window with the title bar "C:\Users\jason\Downloads\sample3521.eml - Microsoft Word". The content area displays the raw email header information. The headers include:

```
File Edit Search View Document Help
File Open Save Print Close Find Replace Undo Redo
1 Received: from SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (::1) by
2 LXP223MB0531.NAMP223.PROD.OUTLOOK.COM with HTTPS; Wed, 17 Jul 2024 09:48:22
3 +0000
4 Received: from LXP223MB0531.NAMP223.PROD.OUTLOOK.COM (208.130.81.81:1133) by
5 via LXP223MB0531.NAMP223.PROD.OUTLOOK.COM (208.130.81.81:1133) with
6 Microsoft SMTP Server (version=TLS1_3,
7 cipher-TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7702.29; Wed, 17 Jul
8 2024 09:48:19 +0000
9 Received: from C00PEP#00000248.name@93.prod.outlook.com
10 Content-Type: multipart/signed; boundary="----=_NextPart_000_00000248"
11 Content-Transfer-Encoding: base64
12 Message-ID: <C00PEP#00000248.name@93.prod.outlook.com>
13 Date: Wed, 17 Jul 2024 09:48:19 +0000
14 Transport: smtprt
15 Authentication-Results: spf=pass (sender IP is 151.80.93.107)
16 smtp.mailfrom=xyz.globalexceltrade.xyz; dkim=none (message not signed)
17 DKIM-Signature: v=DKIM1; a=rsa-sha256; c=relaxed/relaxed; d=xyz.globalexceltrade.xyz;
18 s=dkim; t=smtptimeout; x=151.80.93.107 as permitted sender;
19 recipient=xyz.globalexceltrade.xyz; client-ip=151.80.93.107;
20 helo=xyz.globalexceltrade.xyz; pvc
21 Received: from xyz.globalexceltrade.xyz (151.80.93.107) by
22 C00PEP#00000248.name@93.prod.outlook.com (208.130.243.37) with Microsoft
23 SMTP Server (version=TLS1_3, cipher-TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 25.20.7701.11
24 via Frontend Transport; Wed, 17 Jul 2024 09:48:28 +0000
25 X-IncomingTopDomainMarker:
26 OriginalChecksum=227000100283073949779999C999862308784521577777009CE400000A7C8;UpperCaseChecksum=CE49994093807798273973289628EA954AC8684ECC956BC9472790CE39680C;Size=4aReceived:479;Count:8
27 Received: by sk.globalexceltrade.xyz (Postfix, from user@48)
28 id 3F53004034; Wed, 17 Jul 2024 09:48:19 +0400 (EAT)
29 To: xyz.globalexceltrade.xyz
30 Subject: <207F-B1B7024A40000921140A24D0d61V5C852X8hmcQfTxK252vciBhIEpxbfIAZ#qY51125P9n51Q==>
31 From: <T07F-B1B7024A40000921140A24D0d61V5C852X8hmcQfTxK252vciBhIEpxbfIAZ#qY51125P9n51Q==>
32 Content-type: multipart/mixed; boundary="----=_NextPart_00000248"
33 Message-ID: <C00PEP#00000248.name@xyz.globalexceltrade.xyz>
34 Date: Wed, 17 Jul 2024 09:48:19 +0400 (EAT)
35 X-MS-Exchange-Organization: urn:uuid:00000000-0000-0000-0000-000000000000
36 Return-Path: apache@xyz.globalexceltrade.xyz
37 X-MS-Exchange-Organization: ExpirationStartTime: 17 Jul 2024 09:48:18.9934
38 (UTC)
39 X-MS-Exchange-Organization: ExpirationStartTimeInLocal: originalSubmit
40 X-MS-Exchange-Organization: ExpirationInterval: 1:00:00:00.000000
41 X-MS-Exchange-Organization: ExpirationIntervalInLocal: originalSubmit
42 X-MS-Exchange-Organization: Network-Message-ID:
43 02e04c-size-4e36-932c-0dca502a
44 X-EDMAttributeMessages: 0
```

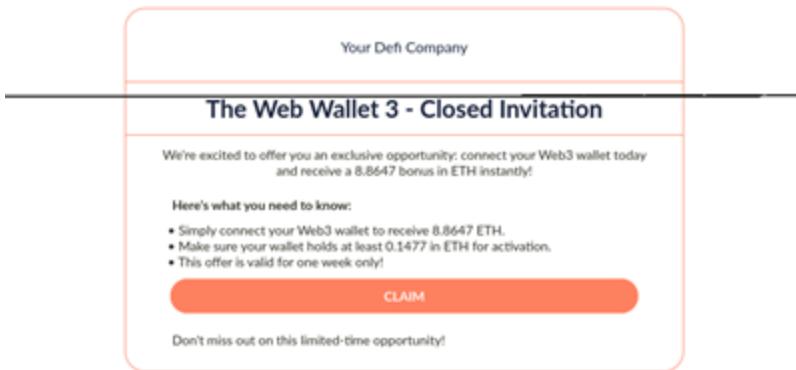
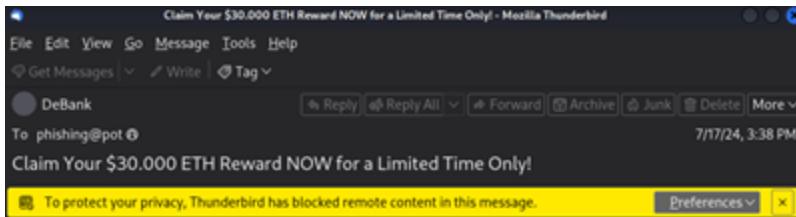
2.2 Email Authentication Results

- **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**

innovatech.website

188.114.97.3 Public Scan

Submitted URL: <http://Innovatech.website/>
 Effective URL: <https://Innovatech.website/>
 Submission: On April 07 via manual (April 7th 2025, 5:01:18 am UTC) from QA — Scanned from NL

Summary HTTP 34 Redirects Links 2 Behaviour Indicators Similar DOM

Summary

This website contacted 2 IPs in 1 countries across 1 domains to perform 34 HTTP transactions. The main IP is 188.114.97.3, located in Amsterdam, Netherlands and belongs to CLOUDFLARENET, US. The main domain is Innovatech.website. TLS certificate: Issued by WE1 on April 3rd 2025. Valid for: 3 months.

innovatech.website scanned 2 times on urlscan.io Show Scans

urlscan.io Verdict: No classification ✓

Live information

Current DNS A record: 188.114.97.3 (AS13335 - CLOUDFLARENET, US)

- VirusTotal**

The screenshot shows the Bluecoat SiteReview interface for the URL <http://innovatech.website/>. The main header indicates "No security vendors flagged this URL as malicious". Below this, there's a "Community Score" of 0/96. The "DETAILS" tab is selected, showing the URL as "innovatech.website" and its type as "Text/html; external-resources". On the right, it shows a status of 200, content type as "text/html; charset=UTF-8", and a last analysis date of "7 months ago". A "Join our Community" button is visible at the bottom.

- **Bluecoat SiteReview**

The screenshot shows the WebPulse Site Review Request interface for the URL <http://innovatech.website/>. It displays the URL submitted and its current categorization as "Finance". A note states: "This page was rated by our WebPulse system".

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.