Phishing Email Analysis Report

By:

Denis Mutwiri Gitonga, Cybersecurity Analyst

Date: 15th April, 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**: noreply@team.mobile.de
- **Sending Server**: MN2PR04CA0034.outlook.office365.com
- **Sender IP Address**: 194.169.163.160
- **IP Reputation Check (AbuseIPDB)**:
    - The IP was reported once in the AbuseIPDB database with a confidence of abuse score of 0%, indicating low suspicion of malicious activity.
    - **ISP**: MT FINANCE LLC
    - **Usage Type**: Data Center/Web Hosting/Transit
    - **ASN**: AS214822
    - **Domain**: nuvds.com
    - **Location**: Saint Petersburg, Russian Federation

- Despite the low abuse score, the IP's association with a data center in Russia raises concerns, as phishing campaigns often use such infrastructure to mask their origins.

```
Received: from MN0P223MB0416.NAMP223.PROD.OUTLOOK.COM (2603:10b6:208:3cc::16)
 by LV3P223MB0968.NAMP223.PROD.OUTLOOK.COM with HTTPS; Fri, 9 Feb 2024
 19:54:12 +0000
Received: from MN2PR04CA0034.namprd04.prod.outlook.com (2603:10b6:208:d4::47)
 by MN0P223MB0416.NAMP223.PROD.OUTLOOK.COM (2603:10b6:208:3cc::16) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7249.39; Fri, 9 Feb
 2024 19:54:11 +0000
Received: from MN1PEPF0000F0DF.namprd04.prod.outlook.com
 (2603:10b6:208:d4:cafe::6f) by MN2PR04CA0034.outlook.office365.com
 (2603:10b6:208:d4::47) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7249.38 via Frontend
 Transport; Fri, 9 Feb 2024 19:54:11 +0000
Authentication-Results: spf=fail (sender IP is 194.169.163.160)
 smtp.mailfrom=team.mobile.de; dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.from=team.mobile.de;compauth=fail
 reason=001
Received-SPF: Fail (protection.outlook.com: domain of team.mobile.de does not
 designate 194.169.163.160 as permitted sender)
 receiver=protection.outlook.com; client-ip=194.169.163.160;
 helo=hptxxt.xyvbrkqrdhgia.lek;
Received: from hptxxt.xyvbrkqrdhgia.lek (194.169.163.160) by
 MN1PEPF0000F0DF.mail.protection.outlook.com (10.167.242.37) with Microsoft
 SMTP Server id 15.20.7249.19 via Frontend Transport; Fri, 9 Feb 2024 19:54:11
 +0000
X-IncomingTopHeaderMarker:
```

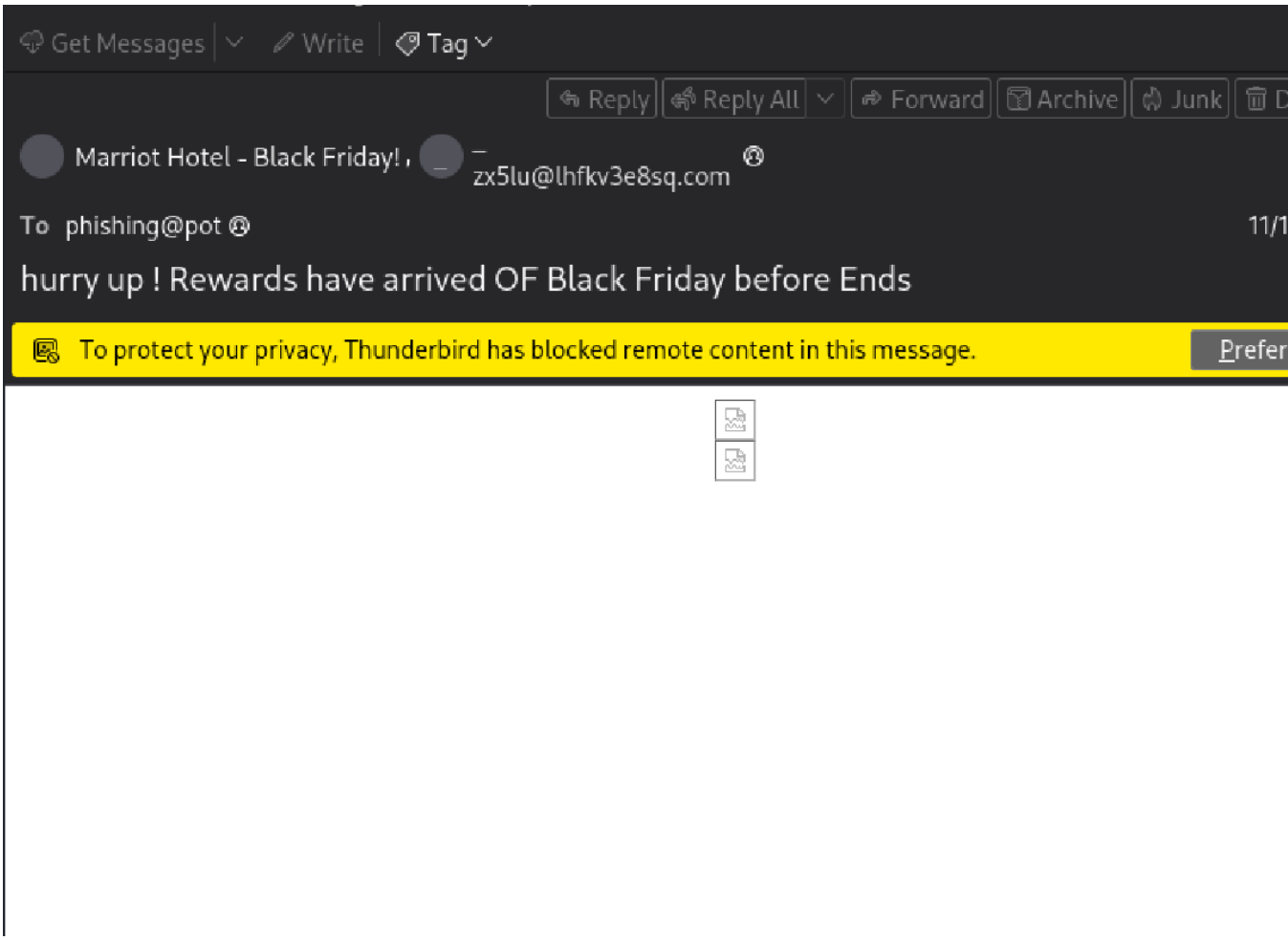
2.2 Email Authentication Results

- **SPF (Sender Policy Framework)**: FAIL
    - *protection.outlook.com* does not designate 194.169.163.160 as a permitted sender for team.mobile.de.
- **DKIM (DomainKeys Identified Mail)**, **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**: NONE
    - DKIM and DMARC checks failed, indicating the message is not signed or authenticated properly.

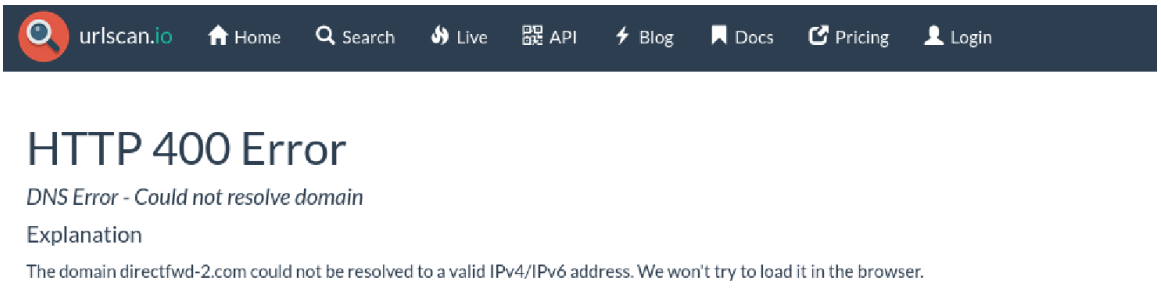
3. Embedded URL Analysis

3.1 Suspicious Link

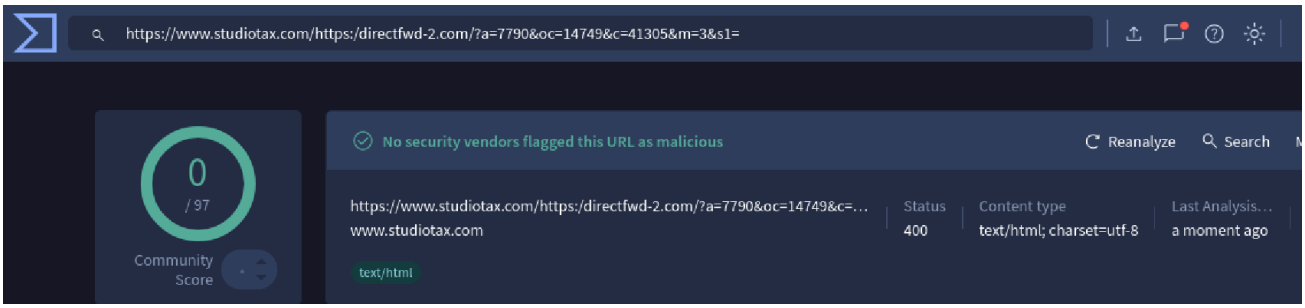
- **URL Found in Email**: https://directfwd-2.com



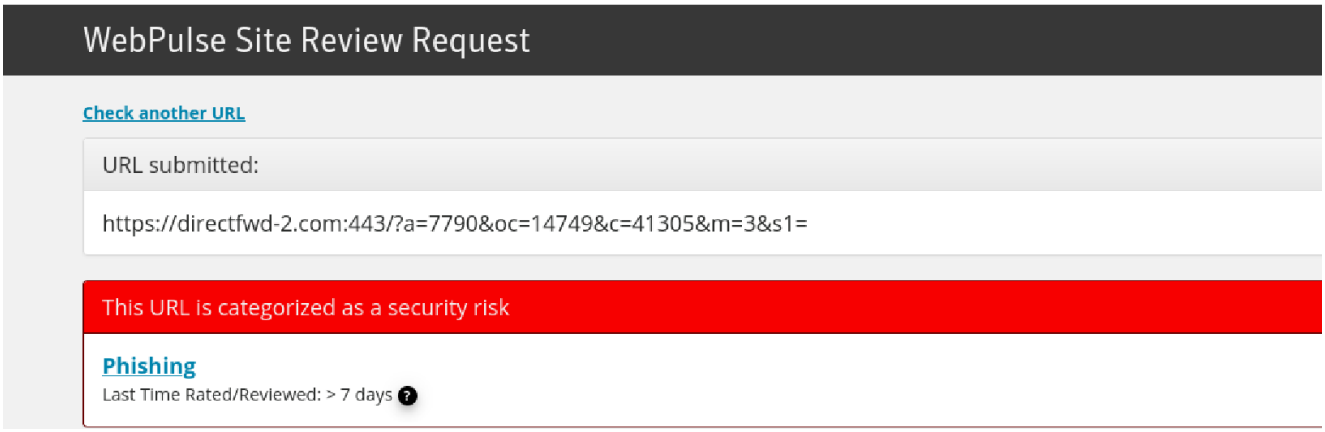
- I extracted the link and performed scans using the following tools:
  - **URLScan.io**



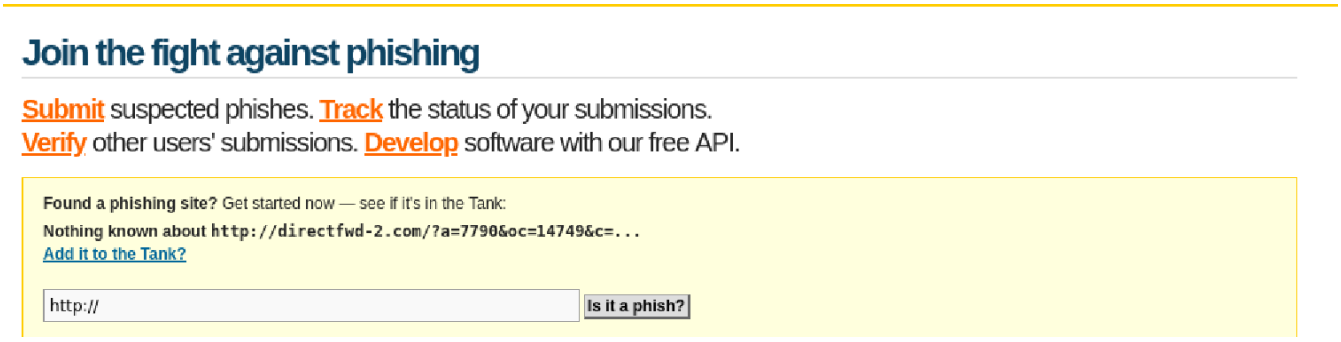
  - **VirusTotal**



- **Bluecoat SiteReview**



- **Phishing Tank**



3.2 Threat Intelligence on Domain

- **Domain**: directfwd-2.com

A WHOIS lookup revealed;

The domain appears not to have been registered, which is consistent with common phishing infrastructure.

4. Threat Intelligence Analysis

4.1 IP Address Reputation

- **IP Address**: 194.169.163.160
- The IP was reported once in the AbuseIPDB database with a confidence of abuse score of 0%, indicating low suspicion of malicious activity.

4.2 Indicators of Compromise (IoCs)

- The email passed through multiple servers, including ***protection.outlook.com*** and ***mail.protection.outlook.com***, with the sender IP identified as ***194.169.163.160.***
- SPF failure indicates potential spoofing of the ***team.mobile.de domain***.
- The email was forwarded from ***hptxtxt.xyvybrkqrdhgia.lek (194.169.163.160)*** to ***mail.protection.outlook.com (10.167.242.37),*** further indicating a potential relay through a compromised or malicious server.

5. Conclusion & Recommendations

5.1 Conclusion

The email exhibits multiple characteristics of a phishing scam:

- Authentication failures (**SPF, DKIM, DMARC**) indicate the sender domain (***team.mobile.de***) is likely spoofed.
- The IP address (***194.169.163.160***) originates from a data center in Russia, a region often associated with phishing infrastructure.
- The embedded URL (***directfwd-2.com***) is flagged as a phishing risk and fails DNS resolution, suggesting it is either defunct or deliberately misconfigured.
- The email's content uses a fake prize offer to entice the recipient into engaging with a potentially malicious survey.

5.2 Recommendations

1. **Do Not Engage**: Avoid clicking on any links or responding to the email.
2. **Report the Email**: Use the "***REPORT 194.169.163.160"*** option on AbuseIPDB to flag the IP for further investigation.
3. **Block the Sender**: Add ***noreply@team.mobile.de*** to your email blocklist.
4. **Educate Users**: Inform others about the risks of unsolicited prize offers, especially those urging immediate action.
5. **Monitor for Follow-Ups:** Be vigilant for similar emails, as phishing campaigns often target victims repeatedly.

This email should be treated as a confirmed phishing attempt and handled with caution.

Report Prepared by:
Denis Mutwiri Gitonga
Cybersecurity Analyst