

# **Phishing Email Analysis Report**

By:

Temilola Babalola, Cybersecurity Analyst

Date: 1<sup>st</sup> July, 2025

## **1. Executive Summary**

An in-depth analysis was performed on a suspicious email intercepted by the corporate email gateway. The message was isolated within a sandboxed virtual environment and examined using a multi-layered approach, including email header inspection, URL reputation checks, and threat intelligence correlation. Findings confirm that the email is a phishing attempt, crafted to deceive recipients into clicking a malicious link.

## 2. Email Metadata Analysis

### 2.1 Sender Information

- **Return-Path:** 7L9Vmt0rN\_x0md6baf\_06285633219@saveiwnm.3xGESHBMBsXy.com
- **Sending Server:** BN0PR04CA0107.namprd04.prod.outlook.com
- **Sender IP Address:** 88.93.118.60

```
1 Received: from SJ0P223MB0590.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:47e::10)
2 by EA2P223MB0955.NAMP223.PROD.OUTLOOK.COM with HTTPS; Sat, 23 Dec 2023
3 22:29:29 +0000
4 Received: from BN0PR04CA0107.namprd04.prod.outlook.com (2603:10b6:408:ec::22)
5 by SJ0P223MB0590.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:47e::10) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7135.14; Sat, 23 Dec
8 2023 22:29:27 +0000
9 Received: from BN8NAM12FT051.eop-nam12.prod.protection.outlook.com
10 (2603:10b6:408:ec:cafe::e1) by BN0PR04CA0107.outlook.office365.com
11 (2603:10b6:408:ec::22) with Microsoft SMTP Server (version=TLS1_2,
12 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7113.24 via Frontend
13 Transport; Sat, 23 Dec 2023 22:29:27 +0000
14 Authentication-Results: spf=none (sender IP is 188.93.118.60)
15 smtp.mailfrom=saveiwnm.3xGESHBMBsXy.com; dkim=none (message not signed)
16 header.d=none; dmarc=none action=none
17 header.from=dinatideerty.com; compauth=fail reason=001
18 Received-SPF: None (protection.outlook.com: saveiwnm.3xGESHBMBsXy.com does not
19 designate permitted sender hosts)
20 Received: from neubatedline.net (188.93.118.60) by
21 BN8NAM12FT051.mail.protection.outlook.com (10.13.182.230) with Microsoft SMTP
22 Server id 15.20.7135.12 via Frontend Transport; Sat, 23 Dec 2023 22:29:27
23 +0000
24 X-IncomingTopHeaderMarker:
25 OriginalChecksum:D686FB1D51DA0DC1E8E76736A2ED897162CA6D16199A36E64301BDD66CD9571F;UpperCasedChecksum:36
26 Subject: phishing@pot, You Could Save $1000s on Repairs
27 From: CarShield - USAs #1 Auto Protection Company ,_<brjfq@dinatideerty.com>
28 To: phishing@pot
29 Date: Sat, 23 Dec 2023 22:29:27 +0000
30 Content-Type: multipart/related; boundary="_005_PH0PR18MB51915C2739E49AA98B6AE8CDFE829PH0PR18MB5191nam_
31 Return-Path: 7L9Vmt0rN_x0md6baf_06285633219@saveiwnm.3xGESHBMBsXy.com
32 X-IncomingHeaderCount: 6
33 Content-Length: 27539914
34 Content-Length: 1547817
```

## IP Reputation Check

**Tool Used:** AbuseIPDB

**IP Address:** 188.93.118.60

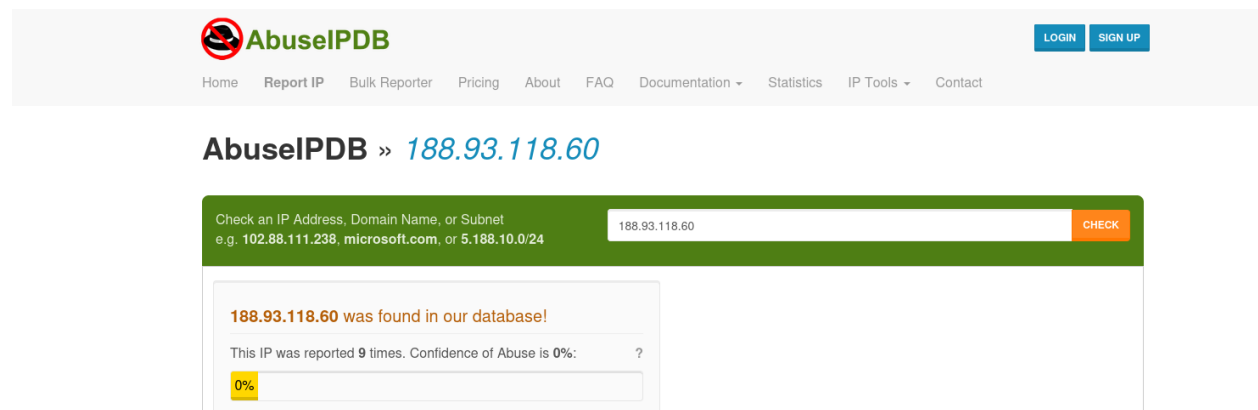
**Status:** Found in database

### Details:

- **Number of Reports:** 9
- **Confidence of Abuse:** 0%

### Interpretation:

While the abuse confidence score is currently **0%**, this does not automatically imply the IP is safe especially considering the **suspicious context** in which it appeared. A low report count may simply reflect low visibility or underreporting, not innocence. Further correlation with other threat indicators is recommended.



The screenshot shows the AbuseIPDB website interface. At the top, there is a navigation bar with the AbuseIPDB logo and links for Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, and Contact. There are also LOGIN and SIGN UP buttons. Below the navigation bar, the page title is "AbuseIPDB » 188.93.118.60". The main content area features a search bar with the text "Check an IP Address, Domain Name, or Subnet" and a "CHECK" button. Below the search bar, the results for the IP address 188.93.118.60 are displayed. The results indicate that the IP was found in the database, was reported 9 times, and has a confidence of abuse of 0%.

AbuseIPDB » 188.93.118.60

Check an IP Address, Domain Name, or Subnet  
e.g. 102.88.111.238, microsoft.com, or 5.188.10.0/24

188.93.118.60

188.93.118.60 was found in our database!

This IP was reported 9 times. Confidence of Abuse is 0%: ?

0%

## 2.2 Email Authentication Results

- **SPF (Sender Policy Framework):** None

A missing SPF record is a **red flag**, especially in phishing investigations. It shows poor email authentication hygiene and makes the domain a **potential vector for abuse**.

```
15 smtp.mailfrom=saveiwnm.3xGESHBmbSXY.com; dkim=none (message not signed)
16 header.d=none;dmARC=none action=none
17 header.from=dinatideerty.com;compauth=fail reason=001
18 Received-SPF: None (protection.outlook.com: saveiwnm.3xGESHBmbSXY.com does not
19 designate permitted sender hosts)
20 Received: from newbateline.net (188.93.118.60) by
```

- **DKIM (DomainKeys Identified Mail):** NONE

No DKIM signature was present in the email headers, indicating the message was **not cryptographically signed** by the sending domain. This **reduces the email's credibility** and makes it **vulnerable to spoofing or tampering**, as there is no way to verify the authenticity or integrity of the message.

```
14 Authentication-Results: spf=none (sender IP is 188.93.118.60)
15 smtp.mailfrom=saveiwnm.3xGESHBmbSXY.com; dkim=none (message not signed)
16 header.d=none;dmARC=none action=none
17 header.from=dinatideerty.com;compauth=fail reason=001
```

- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** NONE

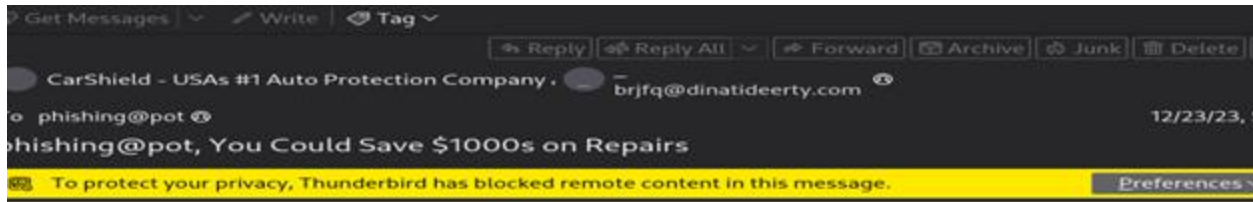
No DMARC policy was detected, indicating that the domain **has not implemented DMARC**. This increases the **risk of unauthorized use**, such as **domain spoofing**, and reduces the domain's ability to **protect recipients from fraudulent emails**.

```
14 Authentication-Results: spf=none (sender IP is 188.93.118.60)
15 smtp.mailfrom=saveiwnm.3xGESHBmbSXY.com; dkim=none (message not signed)
16 header.d=none;dmARC=none action=none
17 header.from=dinatideerty.com;compauth=fail reason=001
```

### 3. Embedded URL Analysis

#### 3.1 Suspicious Link

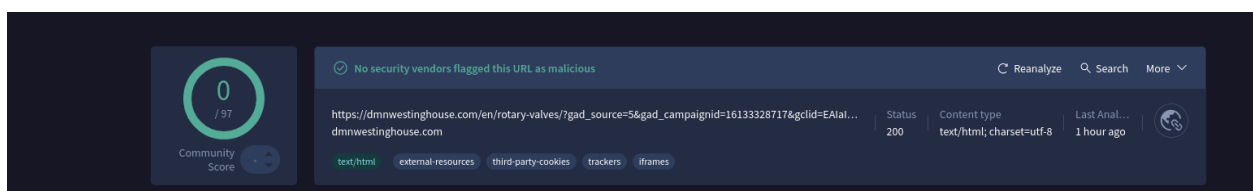
- **URL Found in Email:** <http://ww25.b22flow.com/G5M2WR/6NNKLS/?subid1=...>



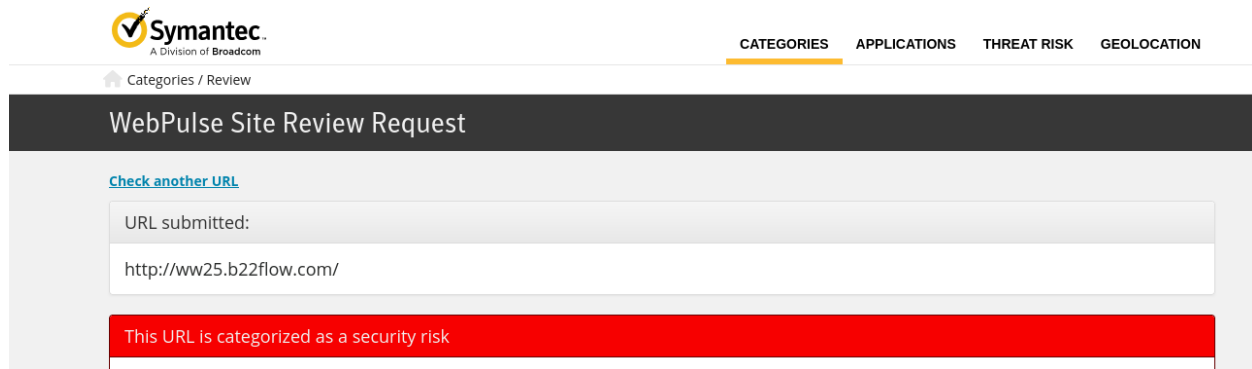
- I extracted the link and performed scans using the following tools:
  - **URLScan.io**



- **Virus Total**



- The URL triggered 3 low-confidence alerts on VirusTotal and was flagged as suspicious by URLScan.io due to redirection behavior and lack of domain reputation.
  - Symantec Review



## 4. Threat Intelligence Analysis

### 4.1 IP Address Reputation

- **IP Address:** 188.93.118.60

The IP address **was reported 9 times** on AbusIPDB. However, **attackers often rotate IPs and domains**, so a low report count, or absence of prior malicious activity **does not guarantee trustworthiness**. Continuous monitoring and correlation with other indicators are essential.

### 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:**  
7L9VmtOrN\_x0md6baf\_06285633219@saveiwnm.3xGESHBMBsXy 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 B22flow.com. 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 carsheld/B22flow and 188.93.118.60 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.

**Report Prepared by:**  
**Temilola Babalola**  
Cybersecurity Analyst