Email Phishing Analysis Report

By:

Afolabi Muhydeen Olalekan

Cybersecurity Analyst

Date: 6th May, 2025

1. Executive Summary

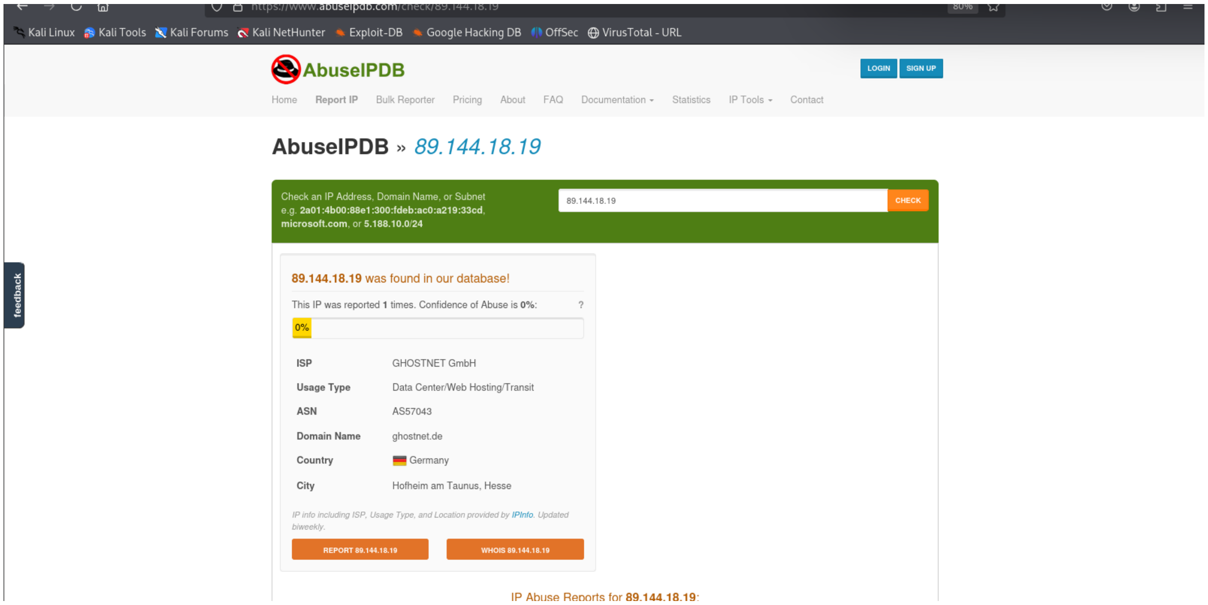
I examined a suspicious email that was obtained via the company email gateway in great detail. Header inspection, URL reputation analysis, and threat intelligence collecting were among the multi-layered analytic methods applied to the email once it was isolated in a sandboxed virtual environment. The email is determined to be a phishing effort based on the findings, which are intended to trick people into clicking on a dangerous link.

2. Email Metadata Analysis

2.1 Sender Information

- **Return-Path**: bounce@awweealime.com
- **Sending Server**: SJ0P223MB0709 .NAMP223. PROD.OUTLOOK.COM
- **Sender IP Address**: 89.144.18.19

IP Reputation Check (AbuseIPDB): Existing reports were found for this IP address in the AbuseIPDB database. The IP was reported once.

- 

AbuseIPDB » *89.144.18.19*

Check an IP Address, Domain Name, or Subnet
e.g. **2a01:4b00:88e1:300:fdeb:ac0:a219:33cd**, **microsoft.com**, or **5.188.10.0/24**

89.144.18.19

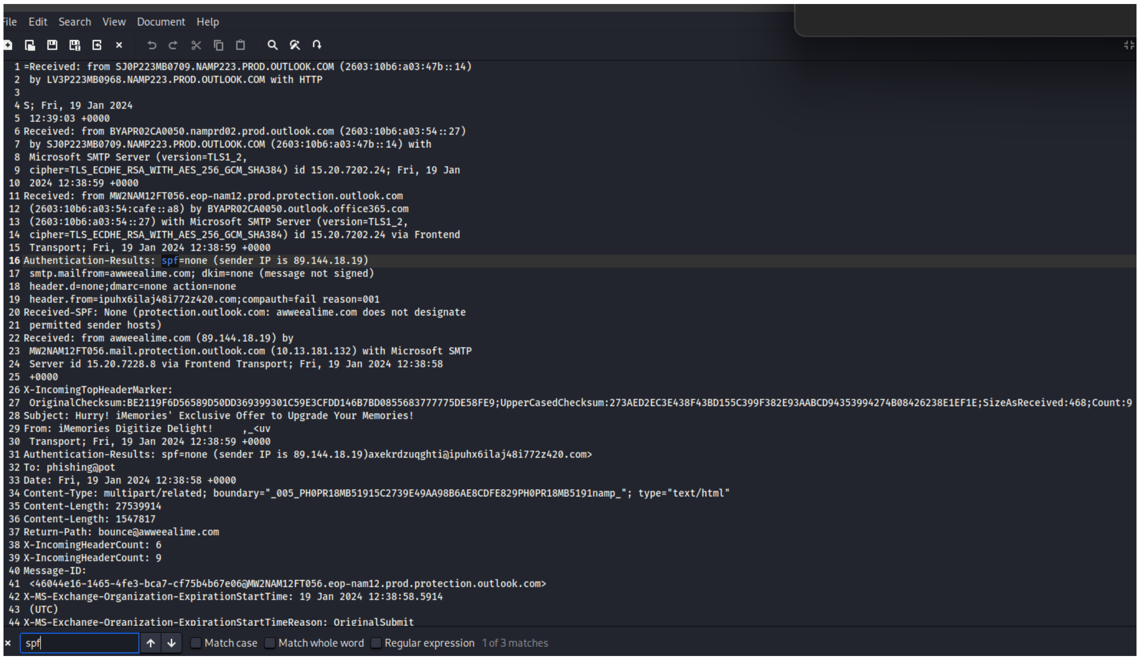
89.144.18.19 was found in our database!

This IP was reported **1** times. Confidence of Abuse is **0%**:

ISP	GHOSTNET GmbH
Usage Type	Data Center/Web Hosting/Transit
ASN	AS57043
Domain Name	ghostnet.de
Country	Germany
City	Hofheim am Taunus, Hesse

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

IP Abuse Reports for **89.144.18.19**:



```
=Received: from SJ0P223MB0709.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:47b::14)
 by LV3P223MB0968.NAMP223.PROD.OUTLOOK.COM with HTTP

S; Fri, 19 Jan 2024
 12:39:03 +0000
Received: from BYAPR02CA0050.namprd02.prod.outlook.com (2603:10b6:a03:54::27)
 by SJ0P223MB0709.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:47b::14) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7202.24; Fri, 19 Jan
 2024 12:38:59 +0000
Received: from MW2NAM12FT056.eop-nam12.prod.protection.outlook.com
 (2603:10b6:a03:54:cafe::a8) by BYAPR02CA0050.outlook.office365.com
 (2603:10b6:a03:54::27) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7202.24 via Frontend
 Transport; Fri, 19 Jan 2024 12:38:59 +0000
Authentication-Results: spf=none (sender IP is 89.144.18.19)
 smtp.mailfrom=awweealime.com; dkim=none (message not signed)
 header.d=none;dmarc=none action=none
 header.from=ipuhx6ilaj48i772z420.com;compauth=fail reason=001
Received-SPF: None (protection.outlook.com: awweealime.com does not designate
 permitted sender hosts)
Received: from awweealime.com (89.144.18.19) by
 MW2NAM12FT056.mail.protection.outlook.com (10.13.181.132) with Microsoft SMTP
 Server id 15.20.7228.8 via Frontend Transport; Fri, 19 Jan 2024 12:38:58
 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:BE2119F6D56589D50DD369399301C59E3CFDD146B7BD0855683777775DE58FE9;UpperCasedChecksum:273AED2EC3E438F43BD155C399F382E93AABCD94353994274B08426238E1EF1E;SizeAsReceived:468;Count:9
Subject: Hurry! iMemories' Exclusive Offer to Upgrade Your Memories!
From: iMemories Digitize Delight!      ,_<uv
 Transport; Fri, 19 Jan 2024 12:38:59 +0000
Authentication-Results: spf=none (sender IP is 89.144.18.19)axekrdzuqghti@ipuhx6ilaj48i772z420.com>
To: phishing@pot
Date: Fri, 19 Jan 2024 12:38:58 +0000
Content-Type: multipart/related; boundary="_005_PH0PR18MB51915C2739E49AA98B6AE8CDFE829PH0PR18MB5191namp_"; type="text/html"
Content-Length: 27539914
Content-Length: 1547817
Return-Path: bounce@awweealime.com
X-IncomingHeaderCount: 6
X-IncomingHeaderCount: 9
Message-ID:
 <46044e16-1465-4fe3-bca7-cf75b4b67e06@MW2NAM12FT056.eop-nam12.prod.protection.outlook.com>
X-MS-Exchange-Organization-ExpirationStartTime: 19 Jan 2024 12:38:58.5914
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
```

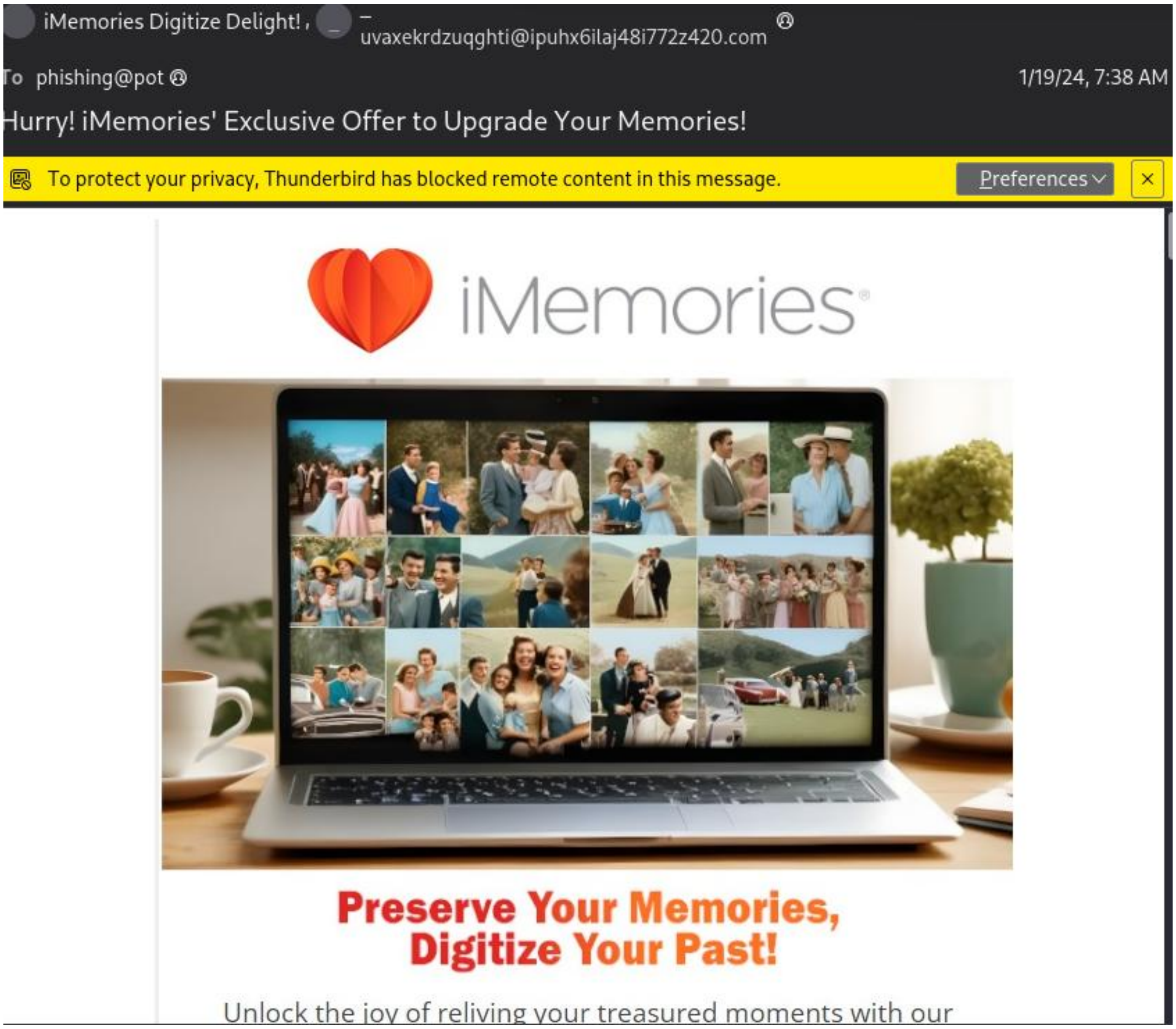
2.2 Email Authentication Results

- **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://t.co/DzIoyehzPV , its shortened for http://www.bdmgtrack5.com/228WNP6/3LRCJ4F/



iMemories Digitize Delight! , _ uvaxekrdzuqghti@ipuhx6ilaj48i772z420.com

To phishing@pot

1/19/24, 7:38 AM

Hurry! iMemories' Exclusive Offer to Upgrade Your Memories!

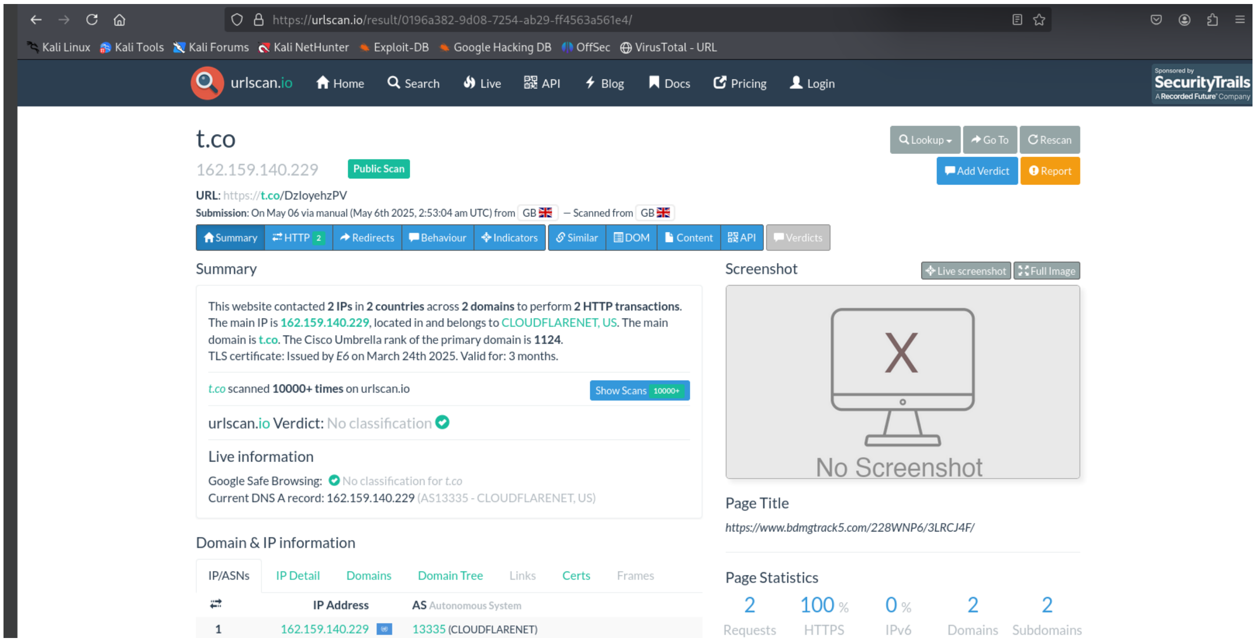
To protect your privacy, Thunderbird has blocked remote content in this message.

Preserve Your Memories, Digitize Your Past!

Unlock the joy of reliving your treasured moments with our

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

- **URLScan.io**



t.co

162.159.140.229 Public Scan

URL: https://t.co/DzloyehzPV

Submission: On May 06 via manual (May 6th 2025, 2:53:04 am UTC) from GB — Scanned from GB

Summary

This website contacted **2 IPs** in **2 countries** across **2 domains** to perform **2 HTTP transactions**. The main IP is 162.159.140.229, located in and belongs to CLOUDFLARENET, US. The main domain is t.co. The Cisco Umbrella rank of the primary domain is **1124**. TLS certificate: Issued by *E6* on March 24th 2025. Valid for: 3 months.

t.co scanned **10000+ times** on urlscan.io Show Scans 10000+

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *t.co*

Current DNS A record: 162.159.140.229 (AS13335 - CLOUDFLARENET, US)

Domain & IP information

	IP Address	AS Autonomous System
1	162.159.140.229	13335 (CLOUDFLARENET)

Screenshot

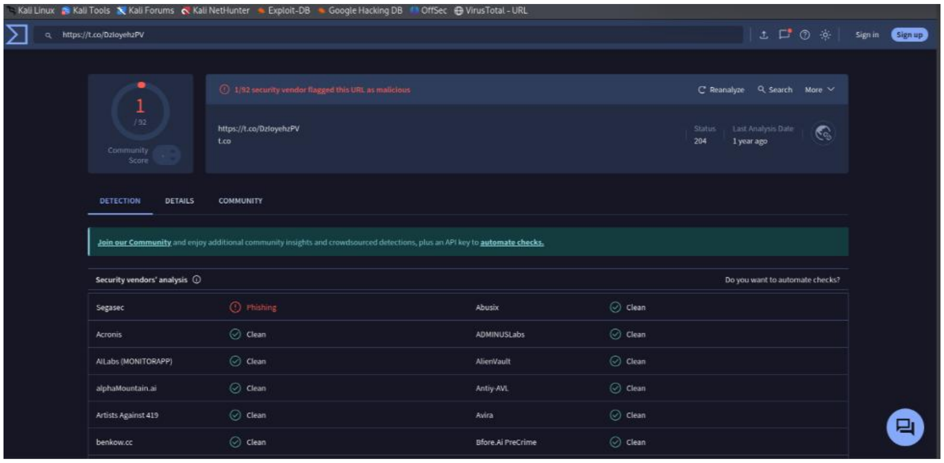
Page Title

https://www.bdmgtrack5.com/228WNP6/3LRCJ4F/

Page Statistics

2	100 %	0 %	2	2
Requests	HTTPS	IPv6	Domains	Subdomains

- **VirusTotal**



1/92 security vendor flagged this URL as malicious

https://t.co/DzloyehzPV
t.co

Status 204

Last Analysis Date 1 year ago

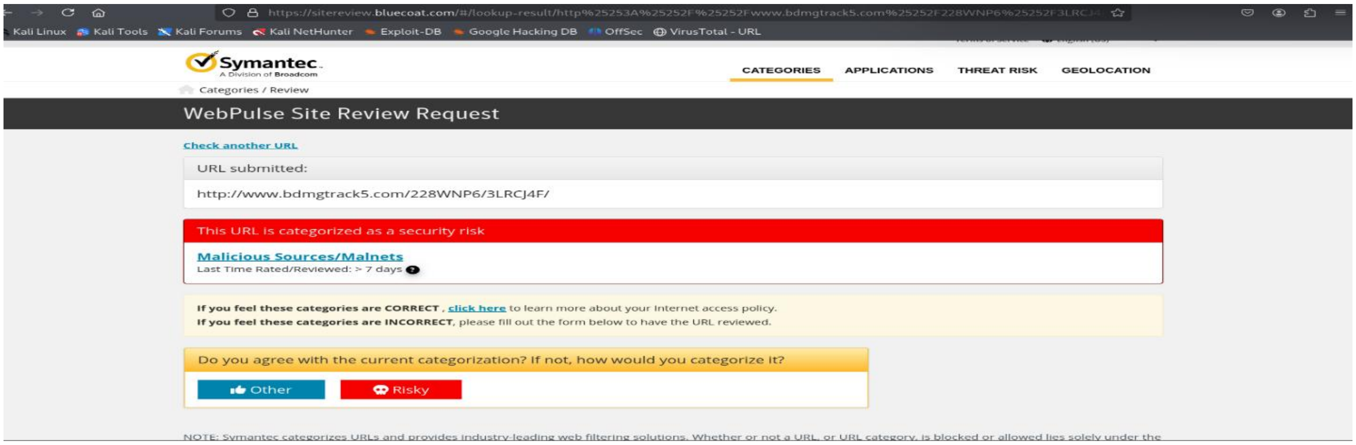
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Segasec	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean

- **Bluecoat SiteReview**



WebPulse Site Review Request

Check another URL

URL submitted:

http://www.bdmgtrack5.com/228WNP6/3LRCJ4F/

This URL is categorized as a security risk

Malicious Sources/Malnets

Last Time Rated/Reviewed: > 7 days

If you feel these categories are CORRECT , click here to learn more about your Internet access policy.
If you feel these categories are INCORRECT, please fill out the form below to have the URL reviewed.

Do you agree with the current categorization? If not, how would you categorize it?

NOTE: Symantec categorizes URLs and provides industry-leading web filtering solutions. Whether or not a URL, or URL category, is blocked or allowed lies solely under the

3.2 Threat Intelligence on Domain

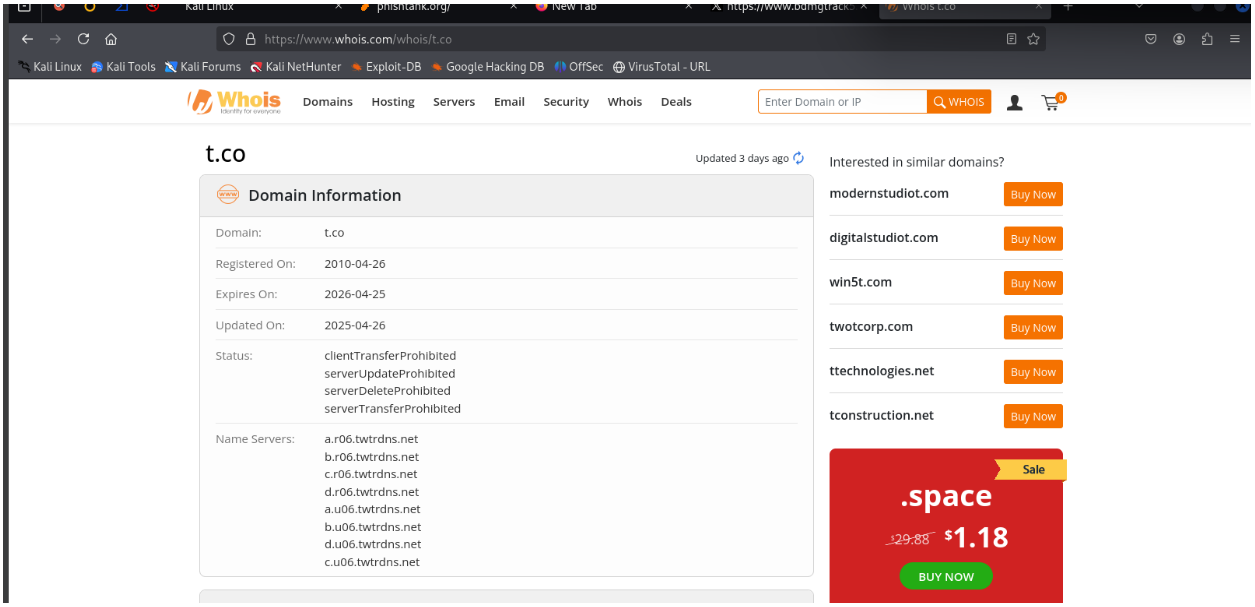
- **Domain**: : https://t.co/DzIoyehzPV , its shortened for https://www.bdmgtrack5.com/228WNP6/3LRCJ4F/

A WHOIS lookup revealed

Registrar:HOSTINGER operations, UAB

Registered On:2010-04-26

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



t.co

Updated 3 days ago

Domain Information

Domain:	t.co
Registered On:	2010-04-26
Expires On:	2026-04-25
Updated On:	2025-04-26
Status:	clientTransferProhibited serverUpdateProhibited serverDeleteProhibited serverTransferProhibited
Name Servers:	a.r06.twtrdns.net b.r06.twtrdns.net c.r06.twtrdns.net d.r06.twtrdns.net a.u06.twtrdns.net b.u06.twtrdns.net d.u06.twtrdns.net c.u06.twtrdns.net

Interested in similar domains?

4. Threat Intelligence Analysis

4.1 IP Address Reputation

- **IP Address:** 89.144.18.19
- This IP address appears in the AbuseIPDB database, having been reported once. The associated ISP is Ghostnet GmbH. While this may suggest limited past malicious activity, attackers frequently rotate IPs and domains, so a lack of historical abuse does not guarantee legitimacy.

4.2 Indicators of Compromise (IoCs)

- **Email Header Anomalies:** The email lacks proper DKIM/DMARC authentication and shows discrepancies between the Return-Path and sending server.
- **Malicious URL:** The email contains a shortened URL linking to a suspicious domain.
- **Suspicious Return-Path Domain:** The sender uses bounce@awweealime.com, a non-standard domain indicative of malicious intent.

---

5. Conclusion & Recommendations

5.1 Conclusion

Following a detailed review of the email headers, authentication failures, and cross-referencing with threat intelligence sources, this email is confirmed to be a phishing attempt. The message is designed to lure recipients into clicking a malicious link:

- **Shortened URL:** https://t.co/DzIoyehzPV
- **Resolved URL:** http://www.bdmgtrack5.com/228WNP6/3LRCJ4F

Both the domain and IP exhibit characteristics commonly associated with phishing infrastructure.

5.2 Recommendations

1. **Immediate Quarantine:** Remove the email from all affected user inboxes.

2. **Block Indicators:** Add both URLs and IP 89.144.18.19 to perimeter security controls including firewall, proxy, and email gateway blocklists.

3. **Report to Authorities:**

   - Submit the phishing attempt to Microsoft via the Security & Compliance Center.

   - Report indicators to the Anti-Phishing Working Group (APWG) and Google Safe Browsing.

4. **User Notification & Training:** Alert users about the phishing attempt and reinforce training on identifying suspicious emails.

5. **Enhance Email Security:** Enforce stricter DMARC, DKIM, and SPF policies at the email gateway.

6. **Threat Hunting:** Monitor logs and endpoints for any communication with the identified domain or IP address

Report Prepared by:

Afolabi Muhydeen Olalekan

Cybersecurity Analyst