Task - 2

Phishing Email Analysis

Objective: Identify phishing characteristics in a suspicious email sample

Source Email: sample-1039.eml

Analysis Tools: VirusTotal, eml-analyzer.herokuapp.com/#/ , https://mxtoolbox.com/

Senders Email: no-reply@access-accsecurity.com

Receiver Email: phishing@pot

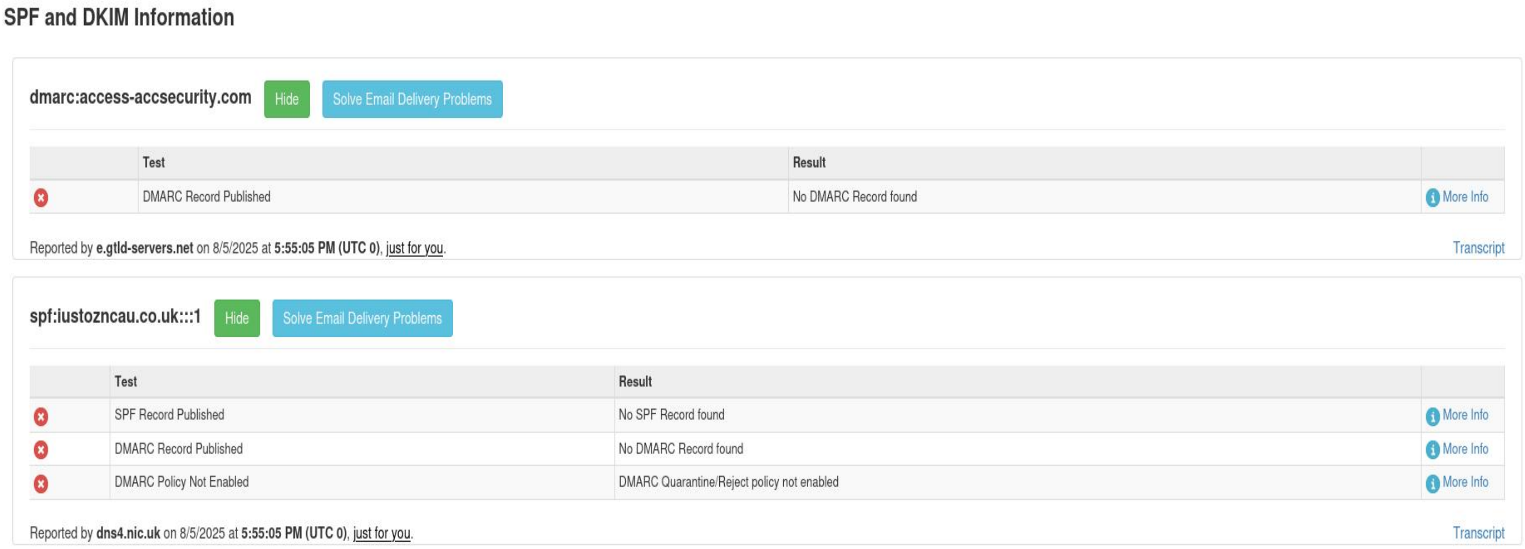
Reply to Email: solutionteamrecognizd02@gmail.com

Analysis:

SPF & DKIM:

For the email analysis we mainly check the Header analysis, the email contains much more headers to check with but there are most common headers like, SPF (Sender Policy Framework) and DKIM (Domainkeys identified mail)which are used for the authenticity of the email , and next the Message-ID, and the Domain names of the receiver and experimental headers or "x- " headers which is most commonly used by the vendors for the spam prevention and authentication results and tracking.

Here are the Results of the authentication headers



SPF and DKIM Information

dmarc:access-accsecurity.com

	Test	Result	
☒	DMARC Record Published	No DMARC Record found	ℹ More Info

Reported by **e.gtld-servers.net** on 8/5/2025 at **5:55:05 PM (UTC 0)**, just for you.

spf:iustozncau.co.uk:::1

	Test	Result	
☒	SPF Record Published	No SPF Record found	ℹ More Info
☒	DMARC Record Published	No DMARC Record found	ℹ More Info
☒	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ℹ More Info

Reported by **dns4.nic.uk** on 8/5/2025 at **5:55:05 PM (UTC 0)**, just for you.

Based on the above result, we clearly say that there is no authentication from the respective domain of the sender sending email, that means it **high chance of being a spam mail**

Message ID:

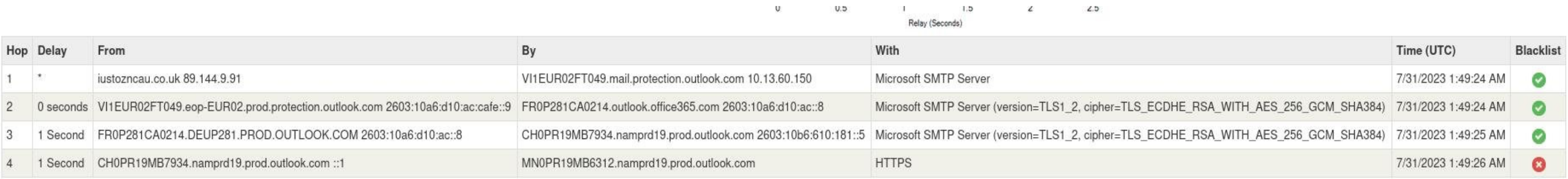
The Message-ID is a unique identifier assigned to every email message. It appears in the email header and looks something like this

Note: the below Message-ID from the sample-mail

<2f661a40-f9bc-43ee-a7a8-7fc67e7b8128@VI1EUR02FT049.eop-EUR02.prod.protection.outlook.com>

- Ensures each email is uniquely identifiable across the internet.
- Helps email clients track conversations (e.g., threading replies).
- Used in spam detection and deduplication systems

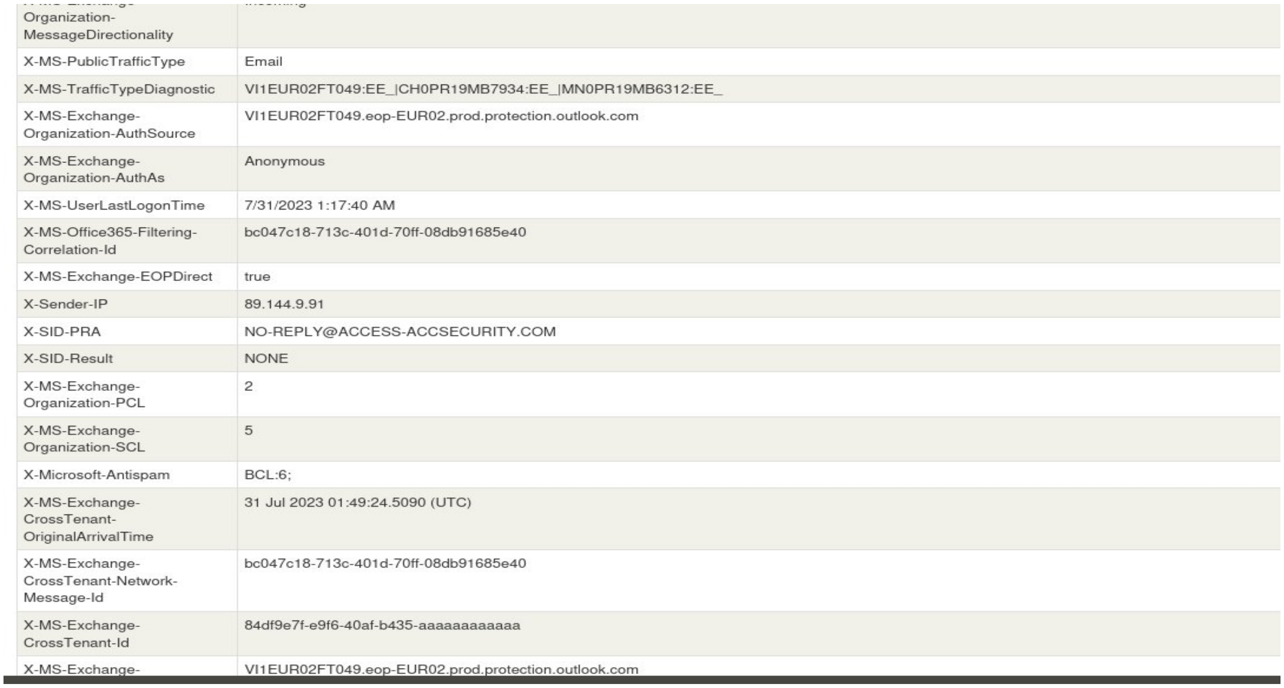
But in our analysis the above Message-ID is Blacklisted



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	iustozncau.co.uk 89.144.9.91	VI1EUR02FT049.mail.protection.outlook.com 10.13.60.150	Microsoft SMTP Server	7/31/2023 1:49:24 AM	✓
2	0 seconds	VI1EUR02FT049.eop-EUR02.prod.protection.outlook.com 2603:10a6:d10:ac:cafe::9	FR0P281CA0214.outlook.office365.com 2603:10a6:d10:ac::8	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	7/31/2023 1:49:24 AM	✓
3	1 Second	FR0P281CA0214.DEUP281.PROD.OUTLOOK.COM 2603:10a6:d10:ac::8	CH0PR19MB7934.namprd19.prod.outlook.com 2603:10b6:610:181::5	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	7/31/2023 1:49:25 AM	✓
4	1 Second	CH0PR19MB7934.namprd19.prod.outlook.com ::1	MN0PR19MB6312.namprd19.prod.outlook.com	HTTPS	7/31/2023 1:49:26 AM	✗

X-Headers:

X-Headers are custom email headers that start with X-, like:



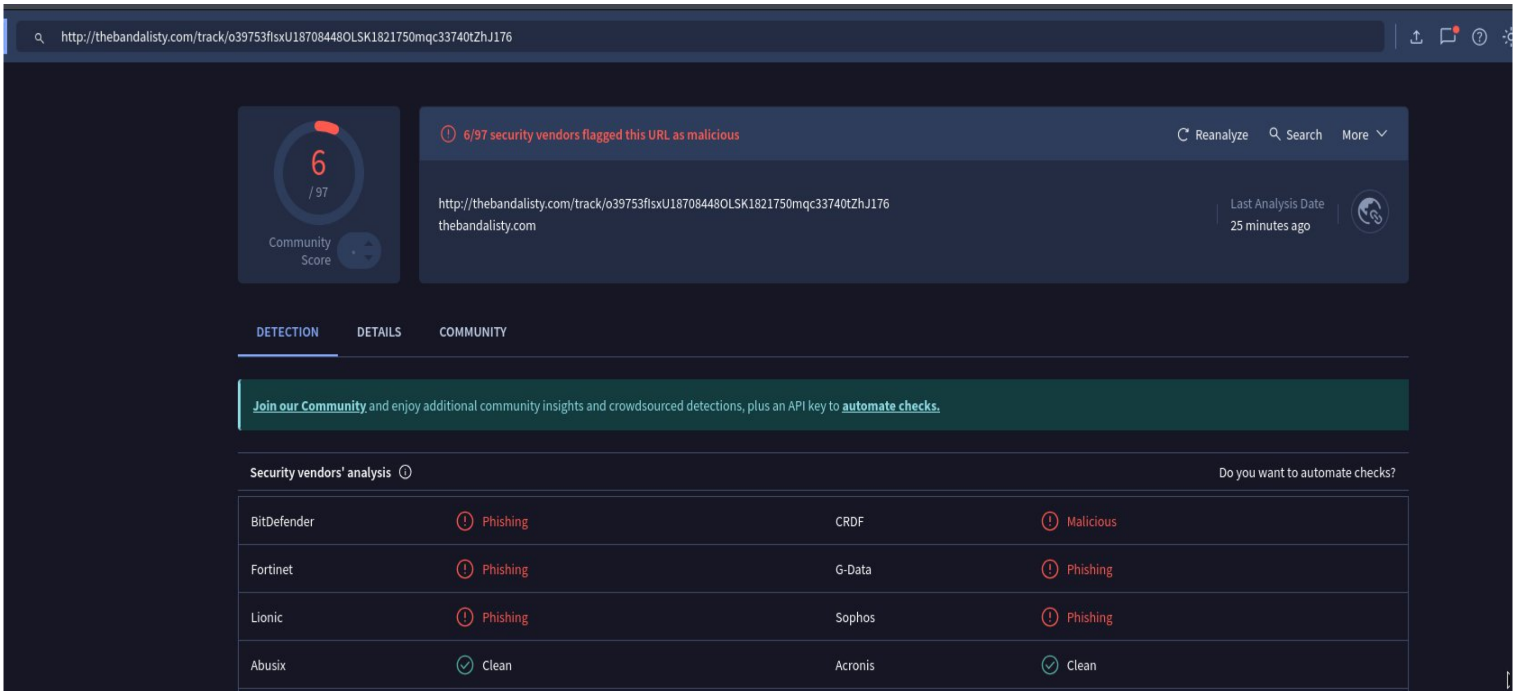
X-MS-Exchange-Organization-MessageDirectionality	Incoming
X-MS-PublicTrafficType	Email
X-MS-TrafficTypeDiagnostic	VI1EUR02FT049:EE_|CH0PR19MB7934:EE_|MN0PR19MB6312:EE_
X-MS-Exchange-Organization-AuthSource	VI1EUR02FT049.eop-EUR02.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs	Anonymous
X-MS-UserLastLogonTime	7/31/2023 1:17:40 AM
X-MS-Office365-Filtering-Correlation-Id	bc047c18-713c-401d-70ff-08db91685e40
X-MS-Exchange-EOPDirect	true
X-Sender-IP	89.144.9.91
X-SID-PRA	NO-REPLY@ACCESS-ACCSECURITY.COM
X-SID-Result	NONE
X-MS-Exchange-Organization-PCL	2
X-MS-Exchange-Organization-SCL	5
X-Microsoft-Antispam	BCL:6;
X-MS-Exchange-CrossTenant-OriginalArrivalTime	31 Jul 2023 01:49:24.5090 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id	bc047c18-713c-401d-70ff-08db91685e40
X-MS-Exchange-CrossTenant-Id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
X-MS-Exchange-	VI1EUR02FT049.eop-EUR02.prod.protection.outlook.com

We need this extra headers for multiple reasons like these:

- Add non-standard, extra info to emails.
- Used by mail clients, servers, or security tools for:
- Debugging
- Tracking
- Spam filtering
- Internal processing

Extracted URL’s and Domains with the VirusTotal Results:

URL: http://thebandalisty.com/track/o39753fIsxU18708448OLSK1821750mqc33740tZhJ176


http://thebandalisty.com/track/o39753fIsxU18708448OLSK1821750mqc33740tZhJ176
6
/ 97
Community Score
Reanalyze
Search
More
DETECTION
DETAILS
COMMUNITY

6/97 security vendors flagged this URL as malicious

http://thebandalisty.com/track/o39753fIsxU18708448OLSK1821750mqc33740tZhJ176
thebandalisty.com

Last Analysis Date
25 minutes ago

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

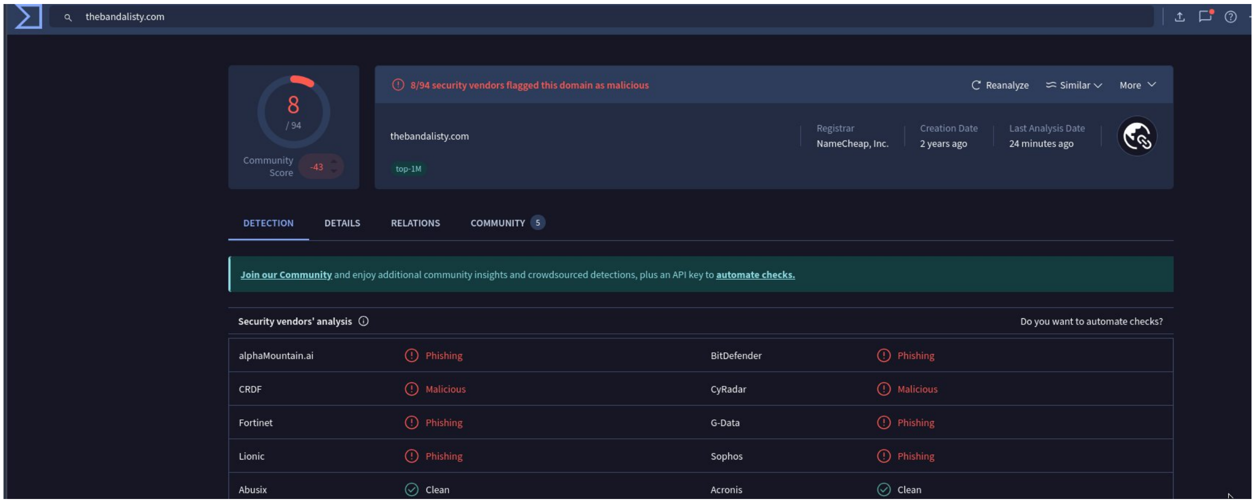
Security vendors' analysis

Do you want to automate checks?

BitDefender	Phishing	CRDF	Malicious
Fortinet	Phishing	G-Data	Phishing
Lionic	Phishing	Sophos	Phishing
Abusix	Clean	Acronis	Clean

This Results form the VirusTotal shows that the Link extracted from the Email is detected as phishing in 6 out of 97

Extracted Domains :thebandalisty.com



thebandalisty.com

8 / 94

Community Score -43

8/94 security vendors flagged this domain as malicious

thebandalisty.com

top-1M

Registrar NameCheap, Inc.

Creation Date 2 years ago

Last Analysis Date 24 minutes ago

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

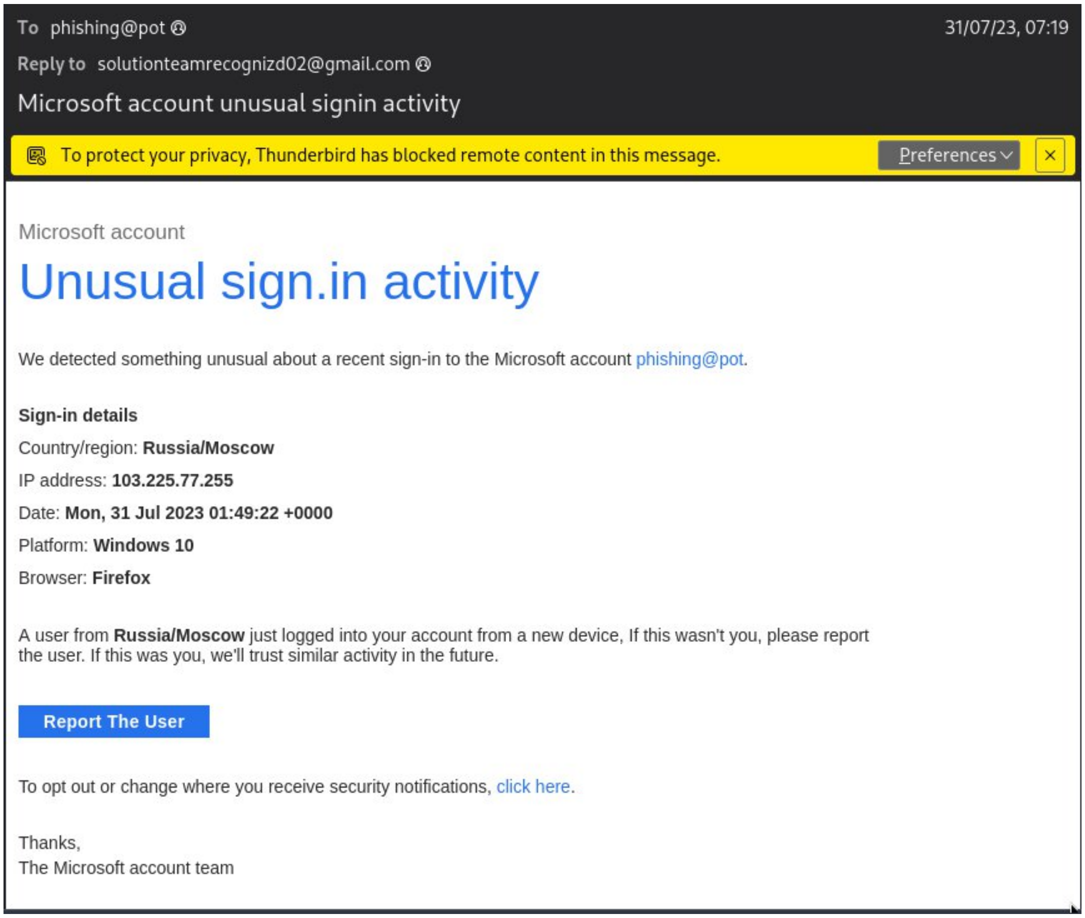
Security vendors' analysis ⓘ

Do you want to automate checks?

alphaMountain.ai	Phishing	BitDefender	Phishing
CRDF	Malicious	CyRadar	Malicious
Fortinet	Phishing	G-Data	Phishing
Lionic	Phishing	Sophos	Phishing
Abusix	✓ Clean	Acronis	✓ Clean

This is the similar to the above virustotal screenshot, that the Domain the link redirects is a phishing website detected.

Message used by the Attacker:



To phishing@pot

31/07/23, 07:19

Reply to solutionteamrecognizd02@gmail.com

Microsoft account unusual signin activity

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

Microsoft account

Unusual sign.in activity

We detected something unusual about a recent sign-in to the Microsoft account phishing@pot.

Sign-in details

Country/region: **Russia/Moscow**

IP address: **103.225.77.255**

Date: **Mon, 31 Jul 2023 01:49:22 +0000**

Platform: **Windows 10**

Browser: **Firefox**

A user from **Russia/Moscow** just logged into your account from a new device, If this wasn't you, please report the user. If this was you, we'll trust similar activity in the future.

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

The scammer used , the unknown user login for the particular location and there is a button of report user and subscription link below.

This makes the user panic that an unknown person logged in to his account and may steal information this kind of mails more likely attacked to the corporate based employees because , for attackers the employs email is a gold mine to enter in to the company’s network.

And there is another sign where , there is a grammatical mistake **sign in** as **sign.in**

Summary:

The email displays clear indicators of a phishing attempt, combining both technical and psychological tactics. It lacks essential authentication headers such as SPF, DKIM, and DMARC, making it easier for attackers to spoof the sender’s identity without detection. The domain associated with the email is listed on known blacklists, and the Message-ID appears suspicious, further undermining its legitimacy. Additionally, VirusTotal analysis flagged eight embedded links with high phishing scores, indicating a strong likelihood of malicious intent. The content of the email uses social engineering by warning the recipient of an “unknown login” from a foreign country, yet the IP address mentioned does not match the claimed location — a common scare tactic used to provoke immediate action. These combined traits strongly suggest the email is part of a phishing campaign and should not be trusted.