Phishing Email Analysis Report Template

1. Case Overview

- Case ID: CASE-001
- Date of Analysis: 2025-06-04
- Analyst: Nizar Aderbaz
- Classification: Internal
- Case Type: Phishing Email (Microsoft Spoof)
- Detection Source: Manual Analysis / Reported to phishing@pot

2. Email Metadata

Field	Value
Subject	“Microsoft account unusual signin activity”
From	Microsoft account team <no-reply@access-accsecurity.com>
To	phishing@pot
Date	Fri, 8 Sep 2023 05:47:04 +0000
Return-Path	bounce@thcultarfdes.co.uk
Message-ID	<032672b4-77ca-42f8-a036-9711e91bd1f3@DB8EUR06FT032.eop-eur06.prod.protection.outlook.com>
IP Address	89.144.44.2
Attachments	None

3. Email Header Analysis

- SPF: Fail (Sender not authorized)
- DKIM: Fail (No signature or invalid)
- DMARC: Fail (because both SPF and DKIM failed)

Received Path:
Received: from “thcultarfdes.co.uk” (89.144.44.2) by DB8EUR06FT032.mail.protection.outlook.com (10.233.253.34) with Microsoft SMTP Server id 15.20.6768.30 via Frontend Transport; Fri, 8 Sep 2023 05:47:04 +0000

Observation:
The sender used a spoofed domain and failed all major authentication checks (SPF, DKIM), confirming impersonation.

4. Email Body Analysis

- Display Name Spoofing: "Microsoft Security Team"

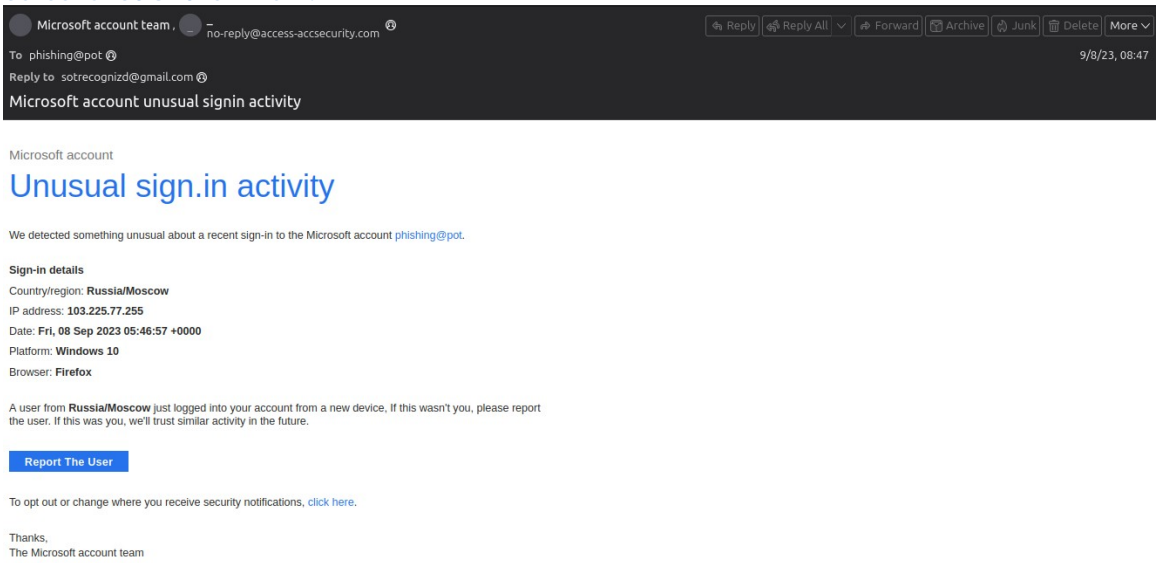
- Claims unusual sign-in from Russia/Moscow.

- Uses fear-based language.

- Phishing Link:
hxxp[://]thebandalisty[.]com/track/o43062rdzGz18708448Gdrw1821750fYo33632dSjh176

- CTA (Call to Action): "Report The User."

Screenshot Of the Email :



5. Link/Attachment Analysis

Type	Value	Result
URL	hxxp[://]thebandalisty[.]com/track/o43062rdzGz18708448Gdrw1821750fYo33632dSjh176	Malicious (VT: 4/72)
IP	89.144.44.2	Known malicious (abuseipdb)
Resolved Domain	thebandalisty.com	Used for

		tracking pixel

6. IOCs (Indicators of Compromise)

Domains
thebandalisty.com

thcultarfdes.co.uk

IPs
89.144.44.2

URLs
hxxp[://]thebandalisty[.]com/track/o43062rdzGz18708448Gdrw1821750fYo33632dSjh176

Emails
no-reply@access-accsecurity.com

sotrecognizd@gmail.com

bounce@thcultarfdes.co.uk

Hashes (if any)
N/A

7. Tools Used

=> VirusTotal – For URL scanning
=> Manual Header Analysis
=> Abuseipdb – For IP scanning

8. Analysis Summary

The email was a clear spoofing attempt pretending to be Microsoft. The use of a fake domain, failed authentication headers, and malicious tracking pixel all confirm phishing intent. The embedded link was confirmed malicious.

9. Recommendations

To Users:
- Never click unknown links in unsolicited emails.
- Verify sender addresses manually.

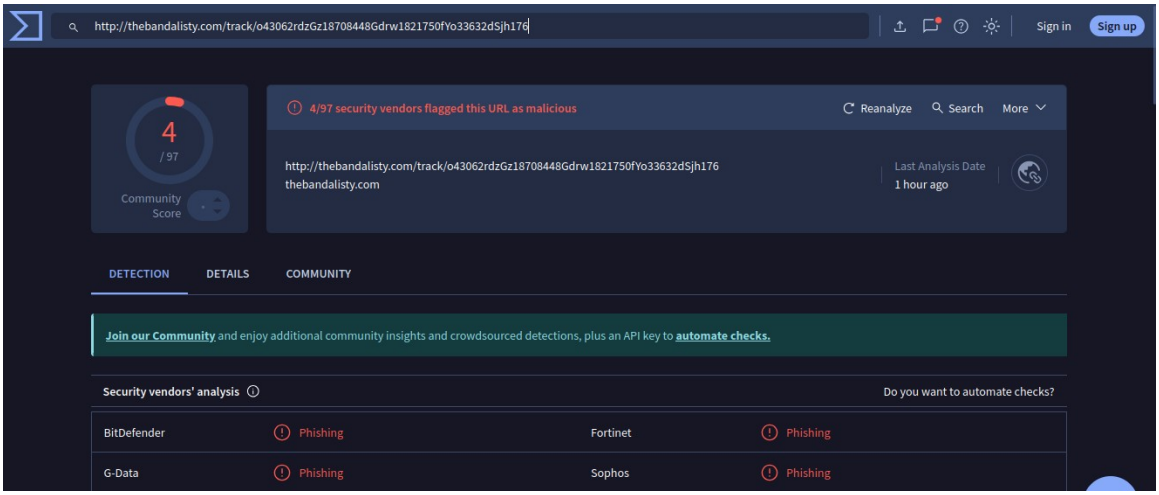
To SOC:

- Block bounce@thcultarfdes.co.uk at the gateway level
- Monitor for other traffic from 89.144.44.2

To Management:
- Consider internal phishing awareness campaigns.

10. Appendix

https://www.virustotal.com/gui/url/d0f0b1d739b21ea0f1d2cdfd1df92e20ce9311965af46b2a0ca7b29e518ee83f



https://www.abuseipdb.com/check/89.144.44.2