# *Phishing Email Analysis Report*

## 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"*

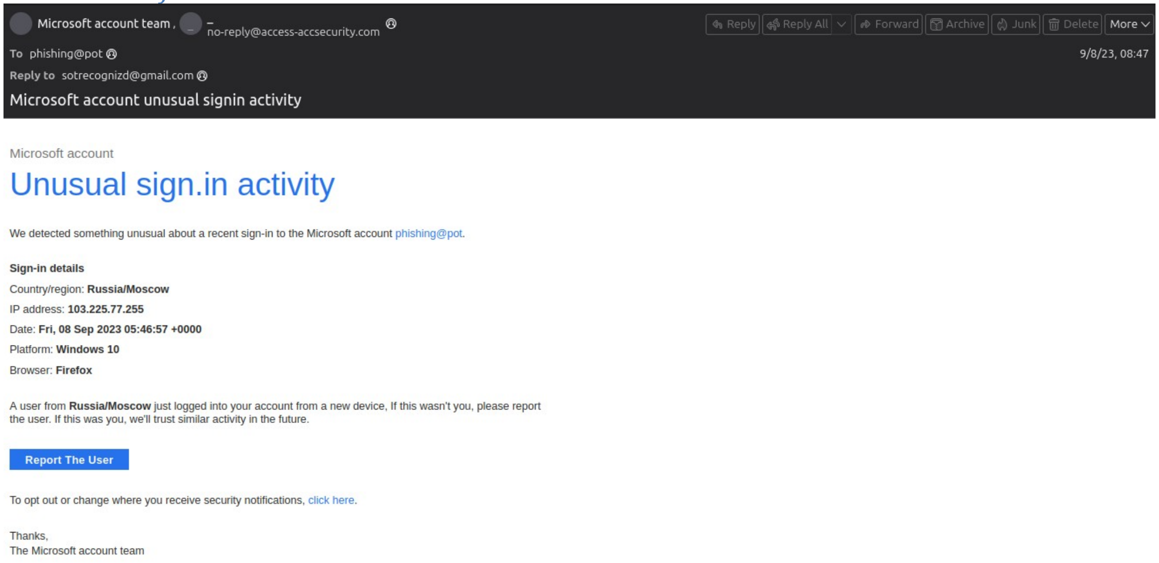
*- Claims unusual sign-in from Russia/Moscow.*

*- Uses fear-based language.*

*- Phishing Link:*
*hxxp[://]thebandalisty[.]com/track/o043062rdzGz18708448Gdrw1821750fYo33632dSjh176*

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

*# Screenshot Of the Email :*



Microsoft account team , – no-reply@access-accsecurity.com

To phishing@pot

Reply to sotrecognizd@gmail.com

9/8/23, 08:47

Microsoft account unusual signin activity

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: **Fri, 08 Sep 2023 05:46:57 +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.

Report The User

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

Thanks,
The Microsoft account team

## 5. Link/Attachment Analysis

| *Type* | *Value* | *Result* |
|---|---|---|
| *URL* | *hxxp[://]thebandalisty[.]com/track/o043062rdzGz18708448Gdrw1821750fYo33632dSjh176* | *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.*

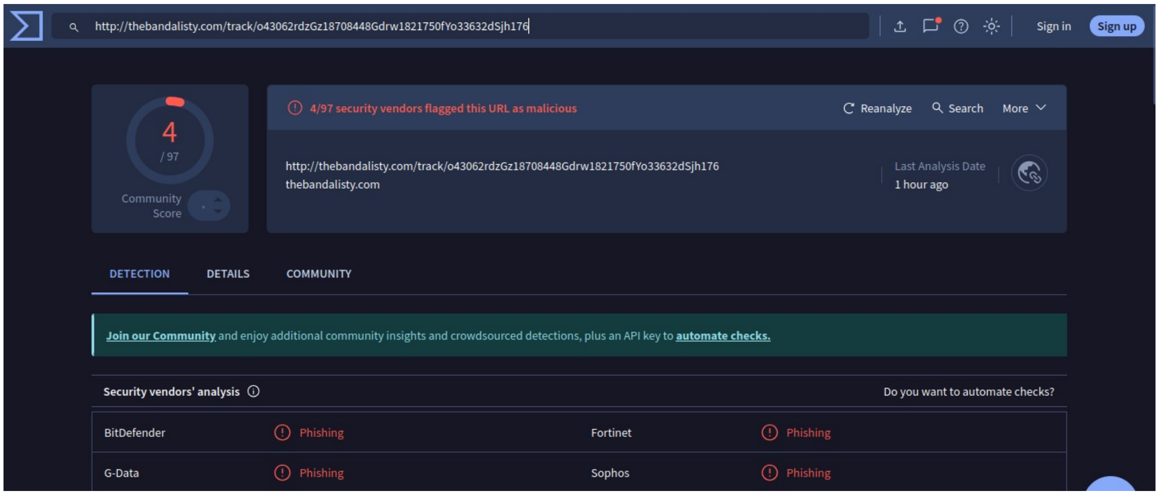
*To SOC:*

*- 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*



4/97 security vendors flagged this URL as malicious

http://thebandalisty.com/track/o43062rdzGz18708448Gdrw1821750fYo33632dSjh176
thebandalisty.com

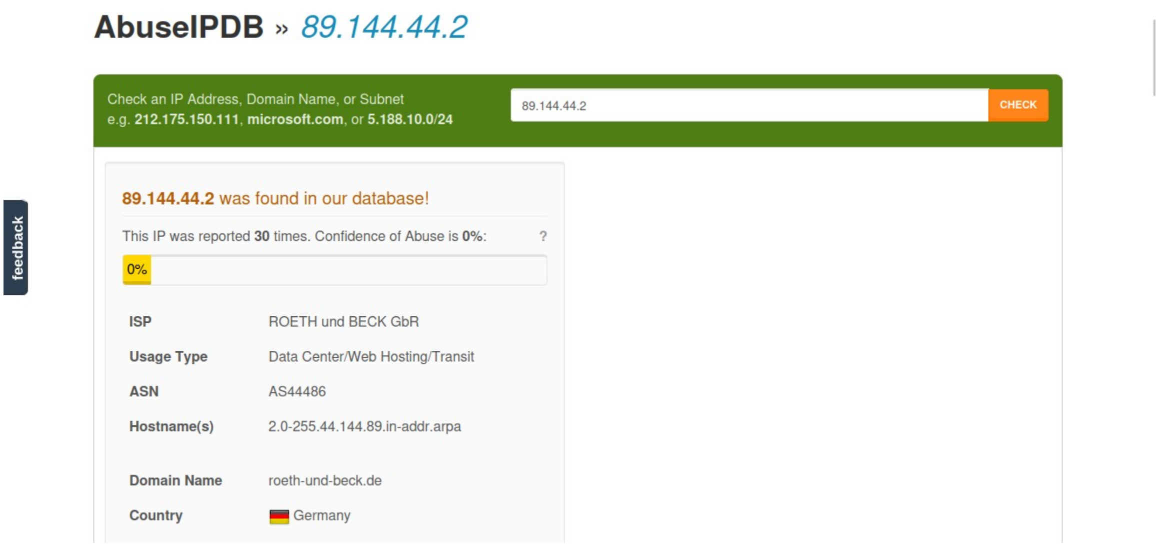
Last Analysis Date
1 hour ago

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 | Fortinet | Phishing |
| G-Data | Phishing | Sophos | Phishing |

*# [https://www.abuseipdb.com/check/89.144.44.2](https://www.abuseipdb.com/check/89.144.44.2)*



Check an IP Address, Domain Name, or Subnet
e.g. **212.175.150.111**, **microsoft.com**, or **5.188.10.0/24**

**89.144.44.2** was found in our database!

This IP was reported **30** times. Confidence of Abuse is **0%**:

| | |
|---|---|
| **ISP** | ROETH und BECK GbR |
| **Usage Type** | Data Center/Web Hosting/Transit |
| **ASN** | AS44486 |
| **Hostname(s)** | 2.0-255.44.144.89.in-addr.arpa |
| **Domain Name** | roeth-und-beck.de |
| **Country** | Germany |