HEADERS
==

Date: Fri, 8 Sep 2023 05:47:04 +0000
Subject: Microsoft account unusual signin activity

To: phishing@pot
From: Microsoft account team ,_<no-reply@access-accsecurity.com>

Reply-To: sotrecognizd@gmail.com
Return-Path: bounce@thcultarfdes.co.uk

Sender IP: 89.144.44.2
Resolve Host: NULL

Message-ID: <032672b4-77ca-42f8-a036-9711e91bd1f3@DB8EUR06FT032.eop-eur06.prod.protection.outlook.com>

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

URL'S
==

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

ATTACHMENTS
==

Attachment Name: NULL
MD5: NULL
SHA1: NULL
SHA256: NULL

DESCRIPTION
==

Received a suspicious email claiming to be from Microsoft Support.

It claims that the account has been placed on hold due to a suspicious login

The email claims an unusual "sign-in" activity from a user located in Russia/Moscow

ARTIFACT ANALYSIS
==

1. SENDER ANALYSIS:

+ The email claims that its from "The Microsoft account team" but we detect that "From" header contains an email address doesnt belong to Microsoft Domain

+ "Reply-To" Header contains an email from Google "sotrecognizd@gmail.com" doesn't belong to Microsoft which is suspicious.

+ "Return-Path" header contains an email "bounce@thcultarfdes.co.uk" doesn't belong to Microsoft, which is suspicious

+ Authentication checks such as SPF and DKIM failed, confirming that the email is suspicious

2. URL ANALYSIS:

+ While analyzing the HTML body of the email, a hidden image (1x1 pixel) was identified:

```
  <img
src="http://thebandalisty.com/track/o43062rdzGz18708448Gdrw1821750fYo33632dSjh17
6" width="1px" height="1px" style="visibility:hidden">
```

+ This image is a **tracking pixel**, typically used to detect when the email is opened. The presence of such a pixel indicates that the sender is attempting to collect metadata such as IP address, location, and email client.

+ The use of a suspicious domain (`thebandalisty.com`) and the use of plain `http` (unencrypted) reinforces the likelihood that this email is malicious and not sent by a legitimate service.

+ This is a common technique used by attackers to confirm active victims and monitor engagement with phishing emails.

+ After scanning the URL using "Virustotal" , Four security vendors show that the URL is malicious (Phishing).

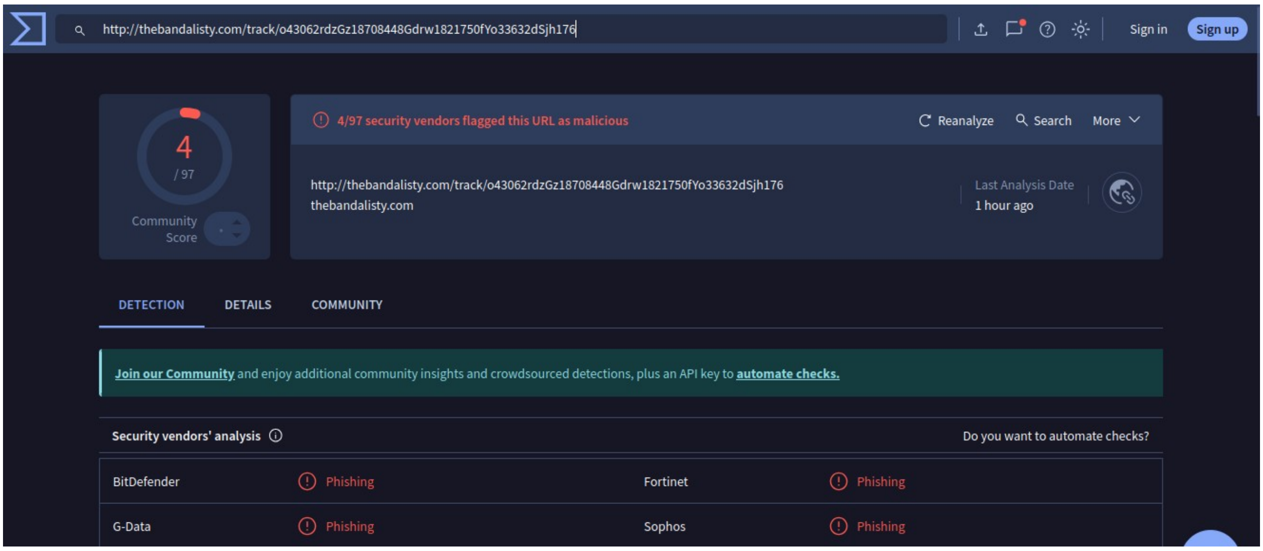
3. ATTACHMENTS ANALYSIS: NULL

VERDICT:

==

+ The email shows himself as a legitimate email from Microsoft, but after analysis we confirm that it is a impersonation and spoofing attempt.

+ Additionally, after analyzing the URL contained in the email's call to action. It was flagged on Virustotal to be malicious.



http://thebandalisty.com/track/o43062rdzGz18708448Gdrw1821750fYo33632dSjh176

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

DEFENCE ACTIONS (in a organization):

==

+ After performing a message trace, no other users within the organization received an email from this sender or with this subject line.

+ To prevent the malicious sender from sending any other email to the organization, I have blocked the “bounce@thcultarfdes.co.uk”
email address on the email gateway