4/26/2025

PHISHING EMAIL FORENSIC ANALYSIS

SPRINT 3

CYBLACK SOC ACADEMY
GROUP 4

This Report is a collective work compiled by all of the members of the CyBlack SOC Academy 3rd cohort, group 4

GROUP MEMBERS

- Adebisi Mololuwa
- Aderinola Kehinde
- Comfort Ukangwobia
- Victoria Simon
- Oghenetejiri Love Brume
- Gyekye Micaiah Ampofo
- Nwobodo Chigozie
- Odunayo Balogun
- Aleka Moses Ogamodey

Email Forensic Analysis Report

Executive Summary:

On August 16, 2023, a suspicious email purporting to be a Microsoft account security notification was received and subjected to forensic analysis. The email, titled "Microsoft account unusual sign-in activity," was crafted to imitate legitimate Microsoft communications but failed critical authentication checks, indicating it was a phishing attempt.

Analysis of the email headers revealed that the message originated from an IP address in Germany (89[.]144[.]44[.]41) associated with a hosting provider known for abuse and malicious activity. The domain used to send the email, access-accsecurity.com, is unaffiliated with Microsoft and showed no valid SPF, DKIM, or DMARC authentication, allowing for easy spoofing. Moreover, the "Reply-To" address directed responses to a free Gmail account, further highlighting the malicious intent behind the communication.

The email's structure included social engineering tactics designed to create urgency, including claims of a suspicious login from Russia, and embedded an invisible tracking pixel hosted on a non-Microsoft domain (thebandalisty[.]com). These elements indicate a high level of threat aimed at compromising user credentials or gathering reconnaissance information.

Based on the findings, the email has been classified as phishing and spoofed. Immediate action has been recommended, including blocking the sender domain and IP address, alerting internal users, submitting the phishing email to Microsoft, enhancing email authentication checks, and monitoring for similar threats. These proactive measures will help mitigate risk, prevent further exposure, and strengthen the organization's resilience against future phishing campaigns.

Methodology

The email forensic analysis involved the following steps:

1. **Email Metadata Extraction:** Retrieving and examining the email's metadata, including subject, sender, recipient, date, and reply-to information.
2. **IP Address Analysis and Mail Flow Tracing:** Identifying the originating IP address, its geolocation and tracing the path of the email through various servers (received headers).
3. **Authentication Results Verification:** Checking the email's SPF, DKIM, and DMARC records to determine its legitimacy and security.
4. **Exchange Authentication Headers Examination:** Analyzing specific Exchange headers (e.g., X-MS-Exchange-Organization-AuthAs, X-MS-Exchange-Organization-AuthSource) to understand how the email was authenticated within the Exchange environment.

5. **Sender and Domain Validation:** Comparing the stated sender and reply-to addresses with official Microsoft domains and verifying A and MX records.
6. **Timestamp and Delivery Path Analysis:** Examining timestamps within the email headers for inconsistencies and analyzing the delivery path for anomalies or manipulation.
7. **Extracted URL/Domain Analysis:** Identifying and dissecting any embedded URLs or Domains within the email body.
8. **Overall Assessment and Recommendation:** Consolidating the findings to determine the nature of the email (legitimate or phishing) and providing recommendations for mitigating future similar threats.

Tools Used:

Below is the list of tools used in the analysis:

- **Phishtool**: used to reverse engineer the email for analysis.
- **EML Analyzer**: used to understand the details within the email, including attachments and links, to potentially identify malicious content or signs of a phishing attempt.
- **MXToolbox**: used for checking domain records (MX/A)
- **Talos Intelligence**: used for IP address and domain lookups
- **VirusTotal**: used it to analyze URLs, domains, and IP addresses to identify potential threats.

The image below shows the email received about an unusual sign-in activity on a Microsoft account [phishing@pot]. The sign-in occurred on August 16, 2023, from a Windows device in Moscow, Russia, with the IP address 103.225.77.255.

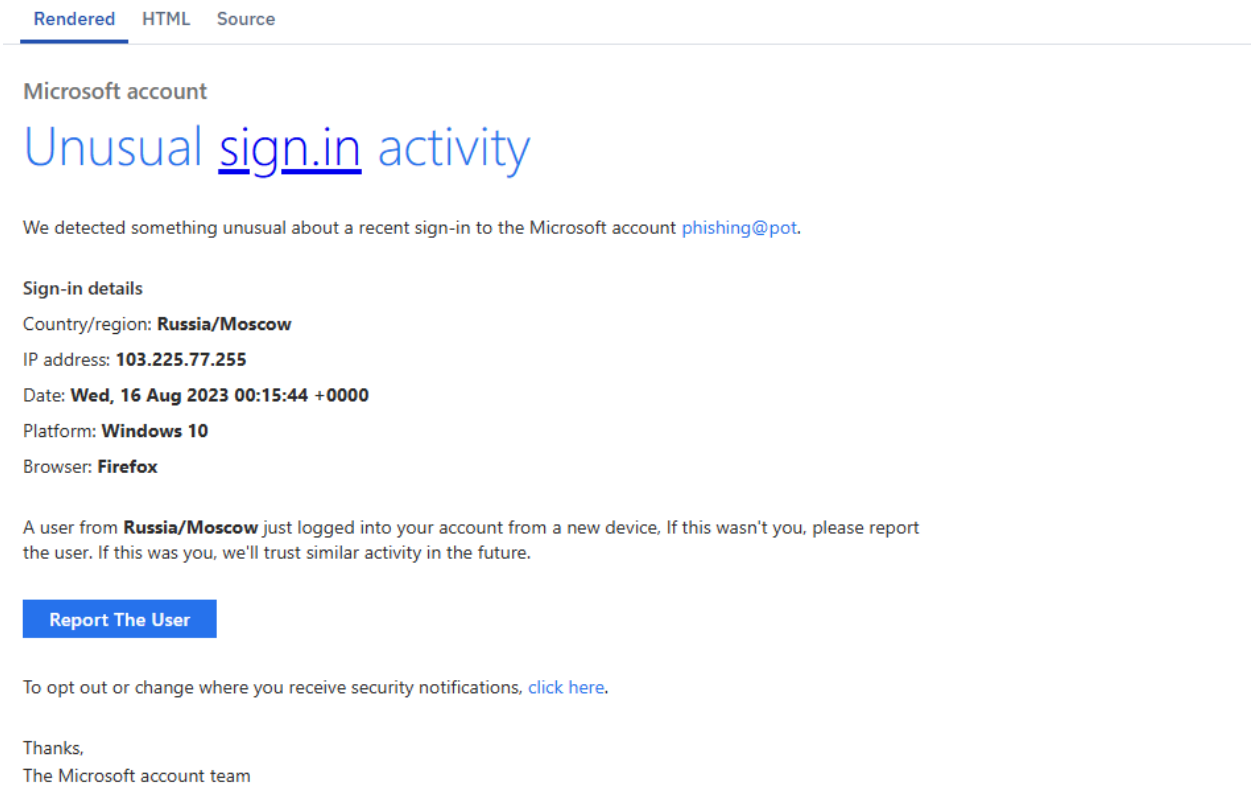


Image by phishtool

1. Email MetaData Overview

Below is metadata about the received email:

Field	Value
Message ID	<06550bd4-ce4e-4e8c-acf9-f8936085be09@MW2NAM04FT048.eop-NAM04.prod.protection.outlook.com>
Subject	Microsoft account unusual sign in activity
From	no-reply@access-accsecurity[.]com
Reply-To	solutionteamrecognizd03@gmail.com
To	phishing@pot
Date Received	12:15 am, Aug 16th, 2023

2. IP Address Analysis and Mail Flow

a. Originating IP Address

- **IP:** 89[.]144[.]44[.]41 (atujpdfghher.co[.]uk)
- **Geo-Location:** Bad Homburg, Germany
- **Does this match the sender's domain?** It does not match the “sender “domain access-accsecurity[.]com or any Microsoft infrastructure.

Domain lookup was performed to gain additional information about the originating IP address.

Whois Lookup

```
inetnum: 89.144.44.0 - 89.144.44.255
netname: DE-RUB-FRA
descr: ROETH und BECK GbR
country: DE
org: ORG-RUBG1-RIPE
admin-c: RUBG3-RIPE
tech-c: RUBG3-RIPE
mnt-by: GHOSTNET-MNT
status: ASSIGNED PA
created: 2025-02-28T08:41:48Z
last-modified: 2025-02-28T08:41:48Z
source: RIPE
organisation: ORG-RUBG1-RIPE
org-name: ROETH und BECK GbR
country: DE
phone: +4960514900300
mnt-by: GHOSTNET-MNT
mnt-ref: GHOSTNET-MNT
org-type: OTHER
```

whois lookup by VirusTotal

b. Received Header Chain:

- Below is the list of all servers (received headers) in order from origin to destination:

Hops

Hop	From	By	With	Date (UTC)	Delay
1	89.144.44.41, atujpdfghher.co.uk	10.13.30.233, mw2nam04ft048.mail.protection.outlook.com	microsoft smtp server id 15.20.6699.15 via frontend transport	2023-08-16T00:15:46Z	N/A
2	2603:10b6:303:85:cafe::78, mw2nam04ft048.eop-nam04.prod.protection.outlook.com	mw4pr04ca0179.outlook.office365.com, 2603:10b6:303:85::34	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.6652.33 via frontend transport	2023-08-16T00:15:44Z	a day
3	mw4pr04ca0179.namprd04.prod.outlook.com, 2603:10b6:303:85::34	ia1pr19mb6449.namprd19.prod.outlook.com, 2603:10b6:208:38b::5	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.6678.26	2023-08-16T00:15:45Z	a few second
4	ia1pr19mb6449.namprd19.prod.outlook.com, ::1	mn0pr19mb6312.namprd19.prod.outlook.com	https	2023-08-16T00:15:45Z	N/A

Image by Phishtool

- Total hops = 4

Any anomalies? The message originated from a suspicious IP address in Germany and lacked SPF authorization. Additionally, the hostnames were spoofed or forged to resemble Outlook servers.

3. Authentication Results

Email authentication results are important because they verify the legitimacy and integrity of email messages, enhancing security and improving deliverability. They help prevent phishing attacks, email spoofing, and spam, ensuring that legitimate emails reach the intended recipients and protecting both senders and recipients from malicious activity.

Security	Status	Explanation
SPF	Fail	atujpdfghher.co.uk has no SPF record, so the sender can't be verified
DKIM	Fail	The lack of a signature in the message implies the absence of DKIM protection.
DMARC	Permerror	This indicates a misconfigured or absent DMARC record, allowing spoofing.

SPF (Sender Policy Framework)

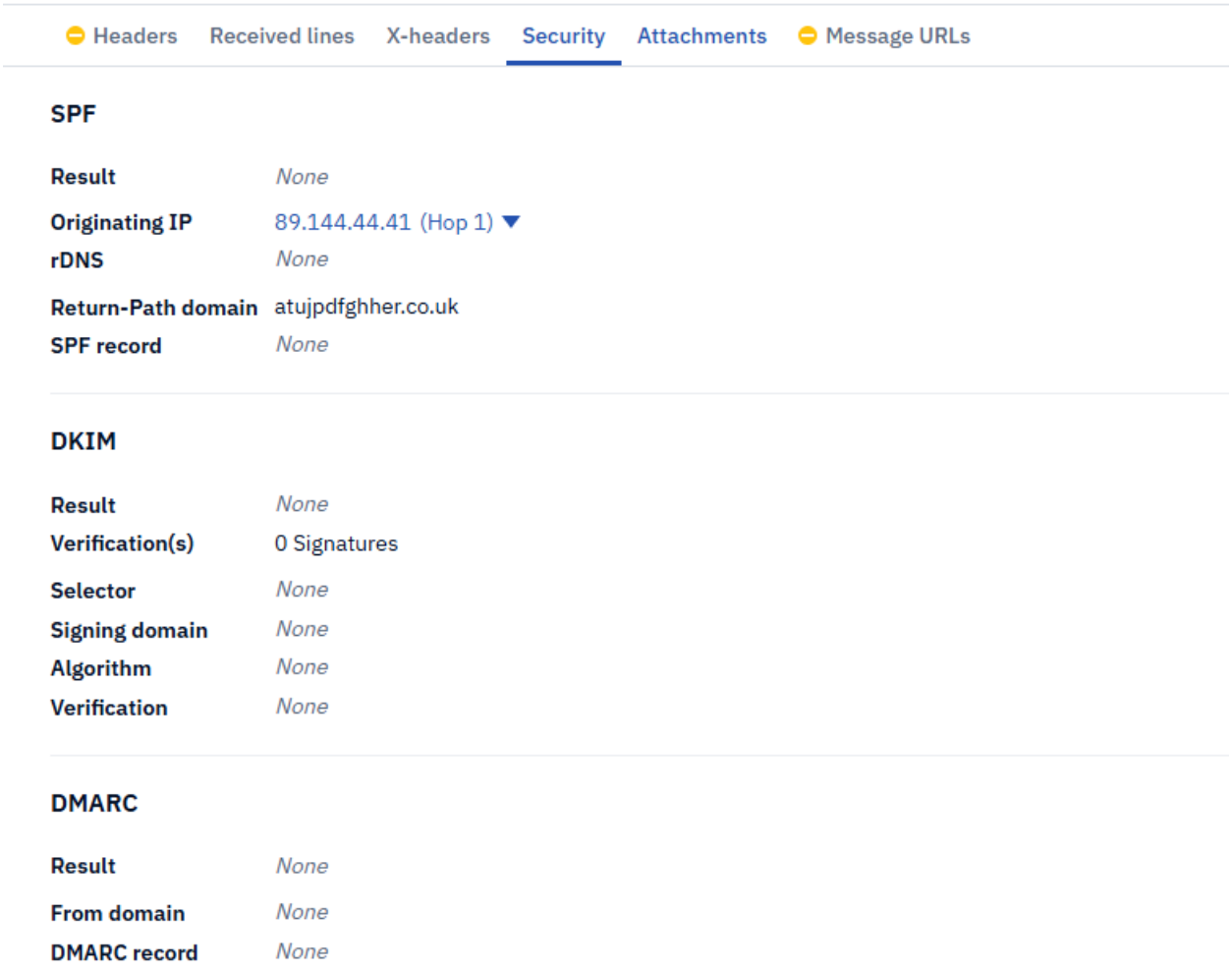
SPF is an email authentication method that verifies if an email was sent from an authorized mail server. It checks if the sender's IP address is listed in the domain's SPF record. SPF helps prevent email spoofing by making it harder for spammers to send messages on behalf of your domain.

DKIM (DomainKeys Identified Mail)

DKIM adds a digital signature to emails, which can be verified by the recipient's email server. This signature confirms that the email was sent by the domain owner and hasn't been altered during transit. DKIM ensures email integrity and authenticity.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

DMARC builds on SPF and DKIM. It tells the receiving email server what to do with messages that fail SPF and DKIM checks (e.g., quarantine or reject). DMARC also provides a reporting mechanism so domain owners can see who is sending emails on their behalf. DMARC helps protect against phishing and email spoofing by providing clear instructions on how to handle unauthenticated emails.



SPF, DKIM, DMARC checks (by phishtool)

4. Exchange Authentication Headers

Header	Value	Interpretation
X-MS-Exchange-Organization-AuthAs	Anonymous	Message was **unauthenticated** on arrival
X-MS-Exchange-Organization-AuthSource	MW2NAM04FT048.eop-NAM04.prod.protection.outlook.com	The message appeared to arrive via Outlook infrastructure, likely **forged** or **relayed**.

The X-MS-Exchange-Organization-AuthAs header indicates how the sender was authenticated when submitting the email to Exchange. In this case, the "Anonymous" value signifies that the email wasn't authenticated, raising a red flag for potential spoofing or phishing, especially when combined with the failure of SPF, DKIM, and DMARC checks. Although the email seemingly entered through Outlook infrastructure (MW2NAM04FT048.eop-NAM04.prod.protection.outlook.com), this could be misleading, as it might have been forged or relayed through an external connector.

5. Sender and Domain Validation

Stated sender = no-reply@access-accsecurity[.]com
Reply-To=solutionteamrecognizd03@gmail[.]com

The email's sender domain, **access-accsecurity[.]com**, doesn't match Microsoft's, and it's not a recognized Microsoft domain, which raises suspicions. Additionally, the use of a free Gmail address for replies in a supposed "Microsoft" security alert is a major warning sign, further indicating the email's fraudulent nature.

Below are the A records and MX records for Microsoft. The domain access-accsecurity[.]com was examined and compared against Microsoft's official records. This involved checking both A records, which map domain names to IP addresses, and MX records, which specify the mail servers responsible for handling a domain's email.

The results of this lookup showed that access-accsecurity[.]com was not present in Microsoft's A records. This mismatch indicates that the email claiming to be from Microsoft was not actually sent from a legitimate Microsoft domain, adding further evidence to its fraudulent nature.

a:outlook.com Find Problems

Type	Domain Name	IP Address
A	outlook.com	52.96.223.2 Microsoft Corporation (AS8075)
A	outlook.com	52.96.91.34 Microsoft Corporation (AS8075)
A	outlook.com	52.96.214.50 Microsoft Corporation (AS8075)
A	outlook.com	52.96.111.82 Microsoft Corporation (AS8075)
A	outlook.com	52.96.172.98 Microsoft Corporation (AS8075)
A	outlook.com	52.96.228.130 Microsoft Corporation (AS8075)
A	outlook.com	52.96.222.194 Microsoft Corporation (AS8075)
A	outlook.com	52.96.222.226 Microsoft Corporation (AS8075)
A	outlook.com	52.96.229.242 Microsoft Corporation (AS8075)

“A” records for outlook.com(by MXtoolbox)

SuperTool Beta9

outlook.com MX Lookup

mx:outlook.com Find Problems Solve Email Delivery Problems

Pref	Hostname	IP Address	TTL		
5	outlook-com.olc.protection.outlook.com	52.101.11.11 Microsoft Corporation (AS8075)	5 min	Blacklist Check	SMTP Test

“MX” records,outlook.com(by MXtoolbox)

6. Timestamp & Delivery Path Analysis

Hops

Hop	From	By	With	Date (UTC)	Delay
1	89.144.44.41, atujpdfghher.co.uk	10.13.30.233, mw2nam04ft048.mail.protection.outlook.com	microsoft smtp server id 15.20.6699.15 via frontend transport	2023-08-16T00:15:46Z	N/A
2	2603:10b6:303:85:cafe::78, mw2nam04ft048.eop-nam04.prod.protection.outlook.com	mw4pr04ca0179.outlook.office365.com, 2603:10b6:303:85::34	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.6652.33 via frontend transport	2023-08-16T00:15:44Z	a day
3	mw4pr04ca0179.namprd04.prod.outlook.com, 2603:10b6:303:85::34	ia1pr19mb6449.namprd19.prod.outlook.com, 2603:10b6:208:38b::5	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.6678.26	2023-08-16T00:15:45Z	a few second
4	ia1pr19mb6449.namprd19.prod.outlook.com, ::1	mn0pr19mb6312.namprd19.prod.outlook.com	https	2023-08-16T00:15:45Z	N/A

Image by phishtool

The analysis of the email headers reveals inconsistencies in the timestamps, which are either too close together or show discrepancies. This strongly suggests that the delivery time was manipulated, especially considering the email's path. Despite originating from a suspicious IP address, the headers indicate that the email was forwarded through multiple Microsoft servers, which is unusual and further points to potential tampering to mask the email's true origin and deceive the recipient.

Extracted URL and Domain

URL:
The analysis revealed an embedded tracking pixel in the email. Below is the image:

```
<img alt="" src="http://thebandalisty.com/track/o41799GCMXp22448528DkRM49413Hwr34421lnRD176" width="1px" height
="1px" style="visibility:hidden">
</tbody>
```

Image by EML Analyzer

What is this?
This is a **1x1 invisible image**, commonly known as a: Tracking Pixel (aka web beacon or spy pixel).
The purpose of these tracking pixels is typically used in marketing emails, phishing attempts, or malicious campaigns to:

- Detect when and if an email was opened
- Log the recipient's IP address
- Capture User-Agent / browser info
- Track recipient location (rough geolocation via IP)
- Fingerprint the user for further tracking

Dissecting the Code:

- **hxxp[://]thebandalisty[.]com/track/o41799GCMXp22448528DkRM49413Hwr34421lnRD176**
  This URL is the endpoint being hit when the email is opened. When your email client loads images (automatically or manually), it contacts that server, logging your interaction.

- **width="1px" height="1px"**
  Makes it tiny and unnoticeable

- **style="visibility:hidden"**
  Ensures it’s not visible even if the dimensions weren’t enough

The URL was subsequently searched on VirusTotal to gain further insight. The results, as shown below, indicate that four vendors have flagged the URL as malicious.

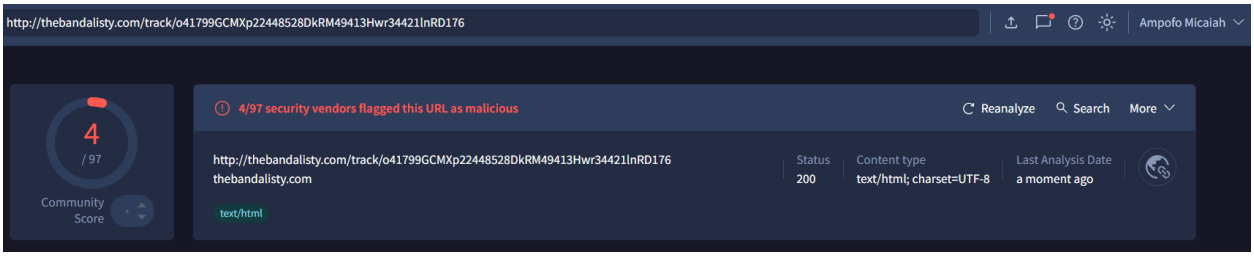


Image by virusTotal

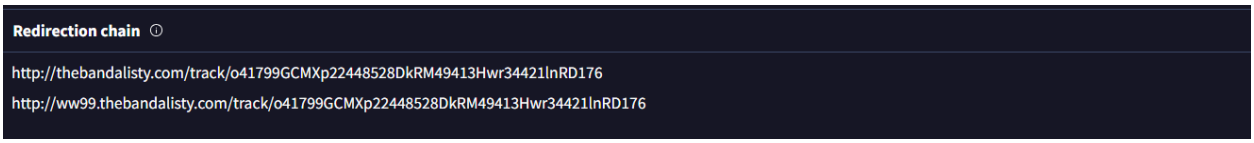
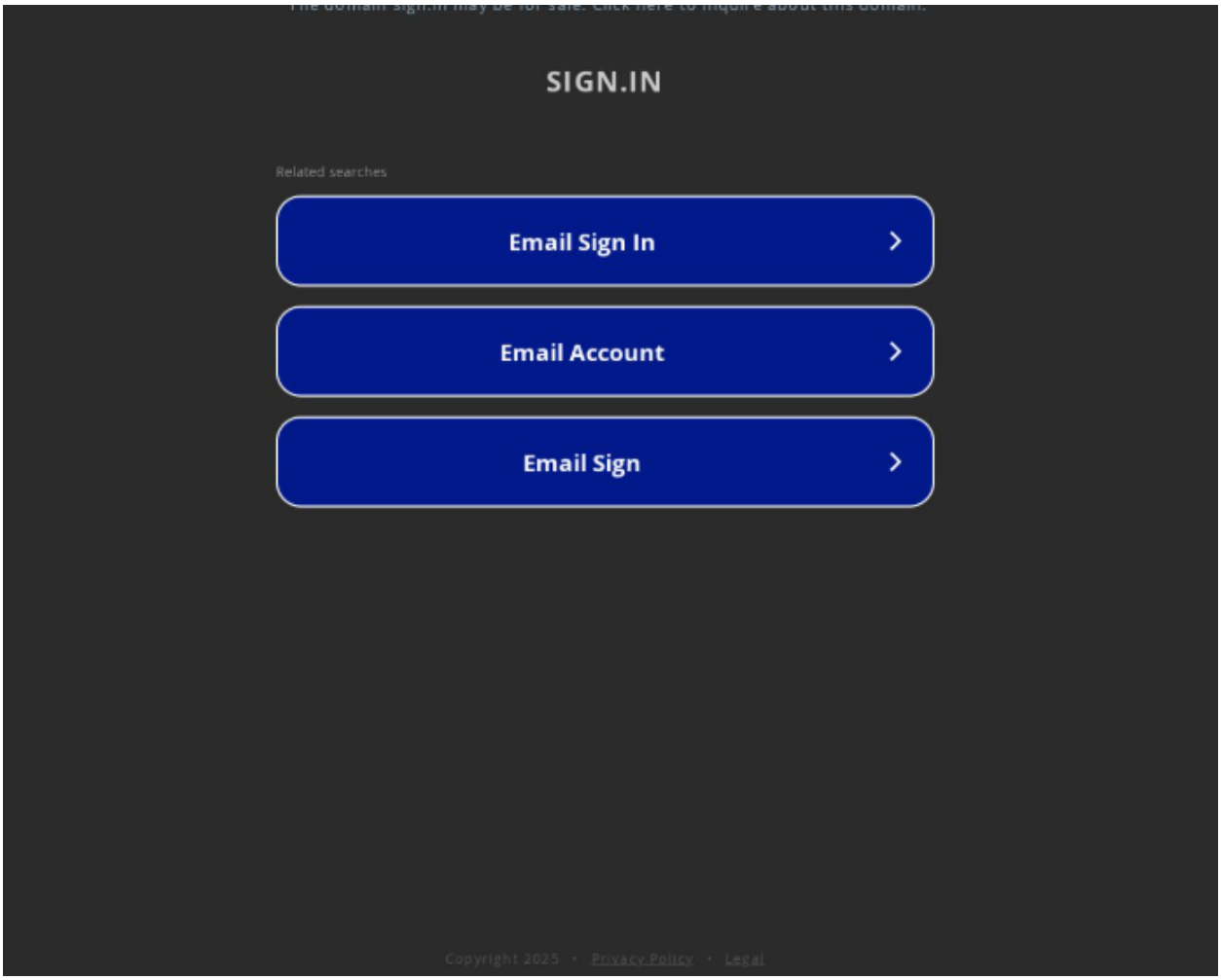


Image by VirusTotal

Domain:

Analysis also revealed an embedded domain in the email, which is **sign.in**.
Clicking the link directs the user to a fake login page, designed to steal their credentials.



sign.in page (by URLscan)

Overall Assessment

This email is a clear and deliberate phishing attempt designed to impersonate Microsoft's account security alerts. The subject line, "Microsoft account unusual sign-in activity," and the HTML-styled body of the email mimic legitimate Microsoft notifications. However, upon examining the email headers, it becomes evident that the message did not originate from Microsoft infrastructure. The sender domain access-accsecurity.com is not associated with Microsoft, and the Reply-To address points to a free Gmail account (solutionteamrecognizd03@gmail.com), which is highly uncharacteristic for corporate security communications.

Moreover, all major email authentication checks have failed or are missing. SPF returned 'None', DKIM is absent, and DMARC resulted in a permanent error, which means the domain is either misconfigured or lacks enforcement. These failures indicate the sender's domain cannot be trusted and is susceptible to spoofing. The X-MS-Exchange-Organization-AuthAs: Anonymous header confirms that the message was not authenticated when it entered the recipient's environment, further reinforcing that this message likely originated from outside the organization without verification.

Additionally, the originating IP address (89[.]144[.]44[.]41) traces back to a provider known for hosting suspicious or abusive content, and it is geolocated to Germany, which is inconsistent with Microsoft's global mail routing infrastructure. There is also a hidden tracking pixel hosted on a suspicious third-party domain (thebandalisty[.]com), commonly used in phishing to monitor user interaction with the email. Taken together, the spoofed brand appearance, authentication failures, mismatched domains, and obfuscated tracking behavior confirm this is a malicious phishing email attempting to socially engineer the recipient into replying or engaging with a fraudulent support address.

Recommended Improvements:

- **Block the sender domain (access-accsecurity[.]com) at the email gateway**: This domain is not affiliated with Microsoft and was used to spoof the brand. Blocking this domain at the perimeter (Exchange Online Protection, Proofpoint, Mimecast, etc.) will prevent further emails from this sender from reaching user inboxes

- **Blacklist the originating IP address (89[.]144[.]44[.]41)**: This IP address belongs to a hosting provider (HostSailor) with a known history of abuse-related activity. Blacklisting this IP prevents future attempts from the same infrastructure and may help reduce similar attack vectors.

- **Monitor for related campaigns or IOC matches (domains, IPs, headers)**: Use threat intel feeds or your SIEM to watch for similar Reply-To patterns, sender domains, or tracking pixel URLs (thebandalisty.com). Monitor for any other messages from the same ASN or IP block used in this campaign.

- **Quarantine or auto-delete unauthenticated Microsoft-branded messages**: Set conditional mail flow rules (Transport Rules / Mail Flow Rules) that quarantine or flag any message claiming to be from Microsoft.com or Outlook.com domains if they fail SPF, DKIM, or DMARC. This adds a defensive layer without outright blocking potentially legitimate external senders.

- **Add detection rules for tracking pixels and beaconing links**: Use a secure email gateway or a DLP/content filter to identify invisible `<img>` tags linked to remote third-party URLs. These are often used for tracking engagement or setting up further social engineering.

- **Consider integrating a sandbox/detonation environment**: If not already deployed, use a sandbox to detonate suspicious attachments or follow suspicious links. While this email was HTML-based and had no attachments, future variants may include weaponized files or redirect chains.

- **Notify internal users and conduct phishing awareness reinforcement**: Since the email mimics Microsoft account alerts, users may be susceptible to social engineering tactics. Circulating a short internal advisory with red flags from this case (e.g., Gmail reply address, unverified sender, Russia login bait) helps strengthen user awareness and reduce click risk.

Conclusion

This email is a clear phishing attempt designed to impersonate Microsoft's account security alerts. Key indicators include the non-Microsoft sender domain (access-accsecurity.com), a Gmail Reply-To address, failed or missing email authentication (SPF, DKIM, DMARC), an anonymous authentication status within Exchange, a suspicious originating IP address from Germany, and a hidden tracking pixel from an unrelated domain. These findings confirm the email's malicious intent to socially engineer recipients and compromise their credentials. Immediate actions, such as blocking the sender domain and IP and enhancing email authentication checks, are recommended to mitigate risks and prevent future phishing attacks.