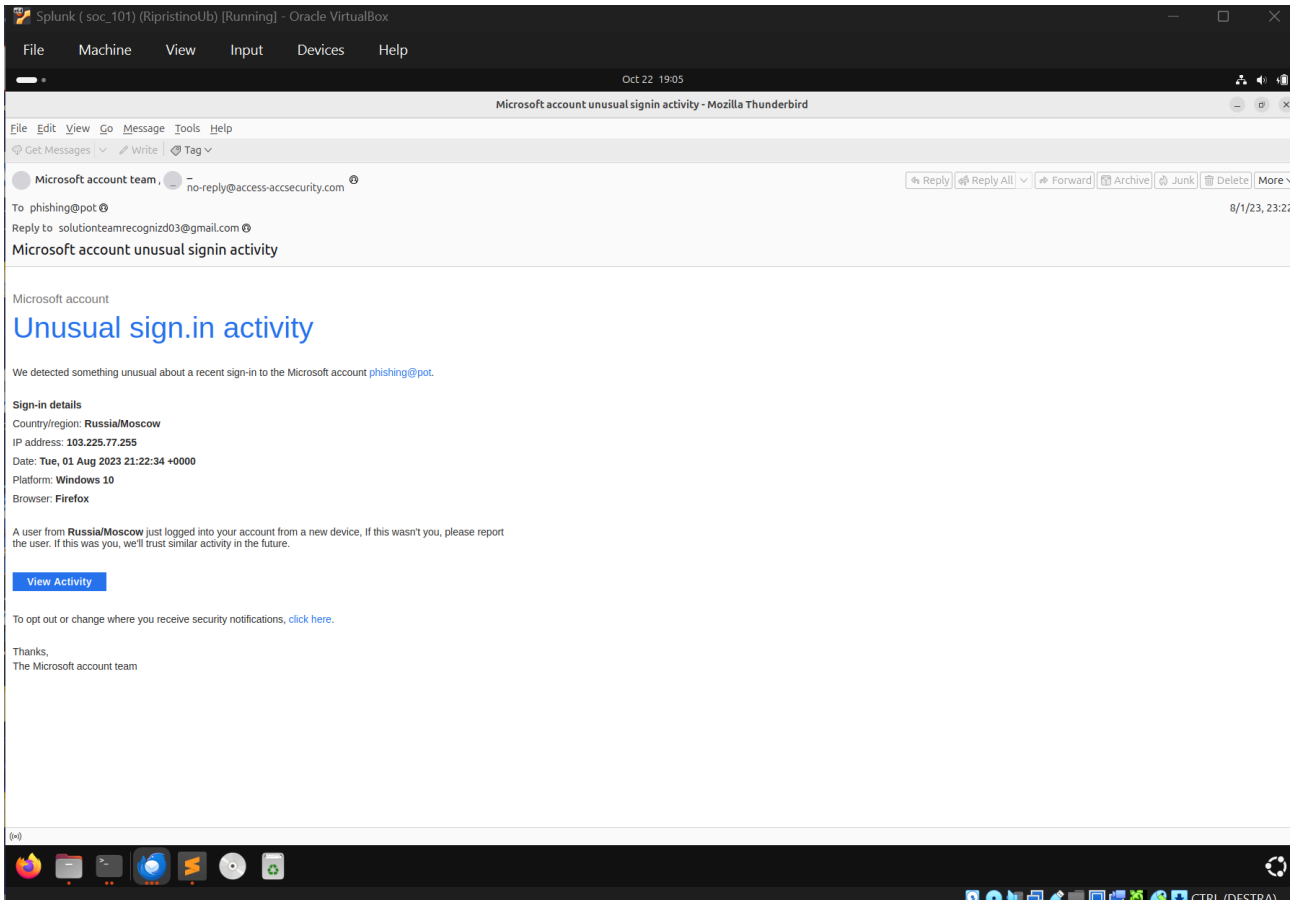
Suspicious Email Analysis – Credential Capture Attempt

During my email forensics training, I investigated a suspicious message disguised as a Microsoft security alert. The email, extracted as a .eml file, was analyzed in raw format. At first glance, the message seemed legitimate, warning about an unusual login from Moscow. However, several noteworthy details raised suspicion.



Initial Observations

The “From” address attempted to mimic Microsoft but used a domain with no affiliation to the company, while the “Return-Path” pointed to another unrelated domain. By carefully reviewing the headers, I determined the sender’s actual IP was associated with a German hosting provider—far removed from any Microsoft network. The message content aimed to trigger alarm by describing a sign-in from Russia, including technical specifics like the IP address, device, and

browser, but these details didn't align with the technical evidence found in the email headers.

HOME RESEARCH

DomainTools PROFILE CONNECT MONITOR SUPPORT WHOIS LOGIN Sign Up

Home > Whois Lookup > 89.144.44.4

Notice: Possible deprecation of Whois services after January 28, 2025. More Info

IP Information for 89.144.44.4

Quick Stats

IP Location	Germany Gelnhausen Ghostnet Gmbh
ASN	AS58212 DATAFOREST dataforest GmbH, DE (registered Apr 14, 2020)
Whois Server	whois.ripe.net
IP Address	89.144.44.4

```
% Abuse contact for '89.144.44.0 - 89.144.44.255' is '
 abuse@ghostnet.de '

inetnum:        89.144.44.0 - 89.144.44.255
netname:        GHOSTNET-FRA
descr:          GHOSTNET GmbH
country:        DE
admin-c:        GN-RIPE
tech-c:         GN-RIPE
mnt-by:         GHOSTNET-MNT
status:         ASSIGNED PA
created:        2025-07-11T04:14:05Z
last-modified:  2025-07-11T04:14:05Z
source:         RIPE

role:           GHOSTnet GmbH
admin-c:        GNSG-RIPE
tech-c:         GNSG-RIPE
address:        Am Dachsbau 17
address:        65812 Bad Soden a. Ts.
address:        Deutschland
phone:          +49 6172 185025
fax-no:         +49 6172 185029
e-mail:          noc@ghostnet.de
nic-hdl:        GN-RIPE
notify:          ripe@ghostnet.de
abuse-mailbox:   abuse@ghostnet.de
mnt-by:         GHOSTNET-MNT
```


Tools

Monitor Domain Properties

Reverse IP Address Lookup

Network Tools

Splunk (soc_101) (RipristinoUb) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Oct 22 19:06

~/Desktop/Soc101/01_Phishing_Analysis/00_Phishing_Attack_Types/cred-capture.eml - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

cred-capture.eml

```
Received: from SA3PR19MB8218.namprd19.prod.outlook.com (::1) by
 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 1 Aug 2023 21:22:49
 +0000
Received: from DU2PR04CA0154.eurprd04.prod.outlook.com (2603:10a6:10:2b0::9)
 by SA3PR19MB8218.namprd19.prod.outlook.com (2603:10b6:806:396::18) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.44; Tue, 1 Aug
 2023 21:22:47 +0000
Received: from DB3EUR04FT008.eop-eur04.prod.protection.outlook.com
 (2603:10a6:10:2b0:cafe::c1) by DU2PR04CA0154.outlook.office365.com
 (2603:10a6:10:2b0::9) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.44 via Frontend
 Transport; Tue, 1 Aug 2023 21:22:47 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.4)
 smtp.mailfrom=providentusezn.co.uk; dkim=none (message not signed)
 header.d=none;dmarc=permerror action=none header.from=access-accsecurity.com;
Received-SPF: None (protection.outlook.com: providentusezn.co.uk does not
 designate permitted sender hosts)
Received: from providentusezn.co.uk (89.144.44.4) by
 DB3EUR04FT008.mail.protection.outlook.com (10.152.24.117) with Microsoft SMTP
 Server id 15.20.6631.29 via Frontend Transport; Tue, 1 Aug 2023 21:22:47
 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:06D5E44D57FDABA2A9FF26571D32632925A077655904CD0FE295CB7E1AEB69F9;UpperCasedChecksum:CFA1D3E3C2E07B798603D0669ED9D0AAC7E2276D64994795B6E0
 A26A63708FE3;SizeAsReceived:394;Count:12
From: Microsoft account team ,_<no-reply@access-accsecurity.com>
Subject: Microsoft account unusual signin activity
To: phishing@pot
Content-Length: 22448528
Content-Length: 49413
Date: Tue, 1 Aug 2023 21:22:47 +0000
Reply-To: solutionteamrecognizd03@gmail.com
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
X-IncomingHeaderCount: 12
Message-ID:
 <191ad2cb-9324-4167-9e8b-30a60c49d341@DB3EUR04FT008.eop-eur04.prod.protection.outlook.com>
Return-Path: bounce@providentusezn.co.uk
X-MS-Exchange-Organization-ExpirationStartTime: 01 Aug 2023 21:22:47.3986
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
```

Line 1, Column 1 Tab Size: 4 Email Header

Splunk (soc_101) (RipristinoUb) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Oct 22 19:09

~/Desktop/Soc101/01_Phishing_Analysis/00_Phishing_Attack_Types/cred-capture.eml - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

cred-capture.eml

```
 A26A63708FE3;SizeAsReceived:394;Count:12
From: Microsoft account team ,_<no-reply@access-accsecurity.com>
Subject: Microsoft account unusual signin activity
To: phishing@pot
Content-Length: 22448528
Content-Length: 49413
Date: Tue, 1 Aug 2023 21:22:47 +0000
Reply-To: solutionteamrecognizd03@gmail.com
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
X-IncomingHeaderCount: 12
Message-ID:
 <191ad2cb-9324-4167-9e8b-30a60c49d341@DB3EUR04FT008.eop-eur04.prod.protection.outlook.com>
Return-Path: bounce@providentusezn.co.uk
X-MS-Exchange-Organization-ExpirationStartTime: 01 Aug 2023 21:22:47.3986
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id:
 224aaf6c-8b6c-45cb-0023-08db92d573f2
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
X-MS-PublicTrafficType: Email
X-MS-TrafficTypeDiagnostic:
 DB3EUR04FT008:EE_|SA3PR19MB8218:EE_|MN0PR19MB6312:EE_
X-MS-Exchange-Organization-AuthSource:
 DB3EUR04FT008.eop-eur04.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-UserLastLogonTime: 8/1/2023 9:21:56 PM
X-MS-Office365-Filtering-Correlation-Id: 224aaf6c-8b6c-45cb-0023-08db92d573f2
X-MS-Exchange-EOPDirect: true
X-Sender-IP: 89.144.44.4
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: 01 Aug 2023 21:22:47.3048
 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: 224aaf6c-8b6c-45cb-0023-08db92d573f2
```

Line 1, Column 1 Tab Size: 4 Email Header

Link Inspection

A crucial moment in the analysis involved examining the “View Activity” button. While the visible link displayed a genuine Microsoft web address, the actual URL redirected users to a site hosted on Vercel (“mc4-two.vercel.app”). This domain is not managed by Microsoft and is known to be used in other phishing campaigns, leveraging trusted cloud hosting to evade some defenses.

Indicators of Phishing

The following key findings confirm the email’s malicious nature:

- The sender domain (“From”) and the “Return-Path” are both unaffiliated with Microsoft.
- The sender IP belongs to an independent hosting provider, not Microsoft infrastructure.
- The action link, despite appearing safe, leads to a phishing site rather than an official Microsoft property.
- The message employs urgency, technical jargon, and fear to increase the chance of user interaction.

Conclusion

This case demonstrates why technical professionals must look beyond the visible content and thoroughly analyze the metadata and infrastructure behind emails. By inspecting headers, cross-referencing sender information, and verifying link destinations, it’s possible to reliably uncover even well-disguised phishing attempts. Ultimately, this investigation highlights the importance of layered email analysis in defending against credential theft campaigns.