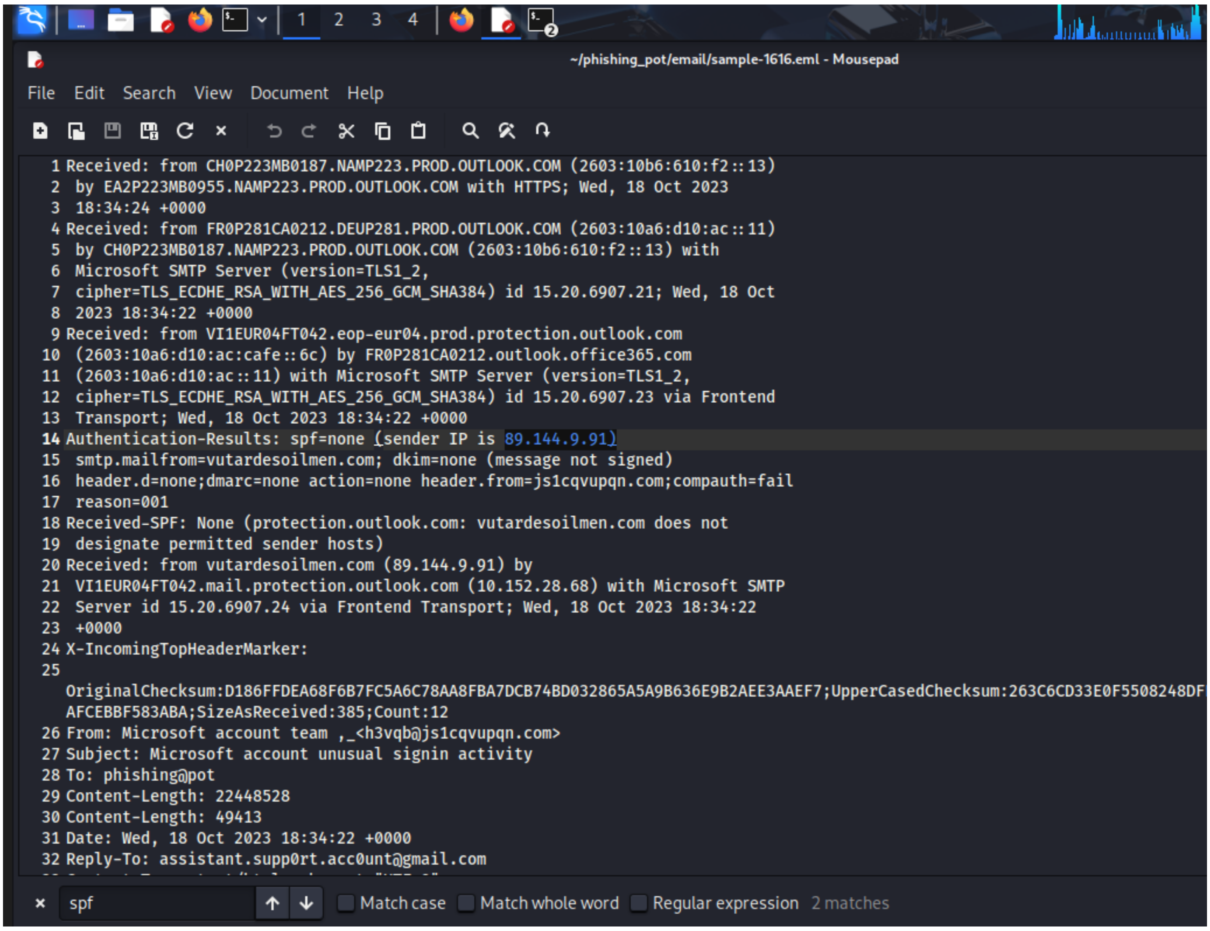
EXECUTIVE SUMMARY

Carried out a thorough investigation into a questionable email that was obtained via the corporate email gateway. Threat intelligence collecting, header inspection, URL reputation analysis, and other multi-layered analytic techniques were applied to the email while it was isolated in a sandboxed virtual environment. The findings indicate that the email is a phishing attempt meant to trick recipients into clicking on a dangerous link.

MetaData Analysis


1 2 3 4
~/phishing_pot/email/sample-1616.eml - Mousepad
File Edit Search View Document Help

```
Received: from CH0P223MB0187.NAMP223.PROD.OUTLOOK.COM (2603:10b6:610:f2::13)
 by EA2P223MB0955.NAMP223.PROD.OUTLOOK.COM with HTTPS; Wed, 18 Oct 2023
 18:34:24 +0000
Received: from FR0P281CA0212.DEUP281.PROD.OUTLOOK.COM (2603:10a6:d10:ac::11)
 by CH0P223MB0187.NAMP223.PROD.OUTLOOK.COM (2603:10b6:610:f2::13) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6907.21; Wed, 18 Oct
 2023 18:34:22 +0000
Received: from VI1EUR04FT042.eop-eur04.prod.protection.outlook.com
 (2603:10a6:d10:ac:cafe::6c) by FR0P281CA0212.outlook.office365.com
 (2603:10a6:d10:ac::11) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6907.23 via Frontend
 Transport; Wed, 18 Oct 2023 18:34:22 +0000
Authentication-Results: spf=none (sender IP is 89.144.9.91)
 smtp.mailfrom=vutardesoilmen.com; dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.from=js1cqvupqn.com;compauth=fail
 reason=001
Received-SPF: None (protection.outlook.com: vutardesoilmen.com does not
 designate permitted sender hosts)
Received: from vutardesoilmen.com (89.144.9.91) by
 VI1EUR04FT042.mail.protection.outlook.com (10.152.28.68) with Microsoft SMTP
 Server id 15.20.6907.24 via Frontend Transport; Wed, 18 Oct 2023 18:34:22
 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:D186FFDEA68F6B7FC5A6C78AA8FBA7DCB74BD032865A5A9B636E9B2AEE3AAEF7;UpperCasedChecksum:263C6CD33E0F5508248DF
 AFCEBBF583ABA;SizeAsReceived:385;Count:12
From: Microsoft account team ,_<h3vqb@js1cqvupqn.com>
Subject: Microsoft account unusual signin activity
To: phishing@pot
Content-Length: 22448528
Content-Length: 49413
Date: Wed, 18 Oct 2023 18:34:22 +0000
Reply-To: assistant.supp0rt.acc0unt@gmail.com
```

× spf ↑ ↓ □ Match case □ Match whole word □ Regular expression 2 matches

Sender Information and Authentication Report

- **Sender Domain Mismatch (Classic Phishing Tactic)**

1. Display Name: “Microsoft account team”
2. Real envelope sender (Return-Path / MAIL FROM): vutardesolmen.com
3. Please reply to assistant.support.account@gmail.com. These domains are not outlook.com or microsoft.com. Official Microsoft domains are the source of all legitimate Microsoft security notifications.

- Relaying Multiple Received Headers via Microsoft Infrastructure

1. Authentic Microsoft/Outlook.com mail servers (NAMP223, DEUP281, etc.) accepted and forwarded the message.

2. This is a popular tactic known as "display-name spoofing + authorized relay abuse," in which the attacker sends emails using a fictitious "From" header that appears to be "Microsoft account team," but the real envelope sender is a disposable domain. Microsoft's servers approve and transmit the message because it is sent to Outlook.com/Hotmail via authenticated SMTP, giving it legitimacy.

❖ SPF Failure (Line 14–19)

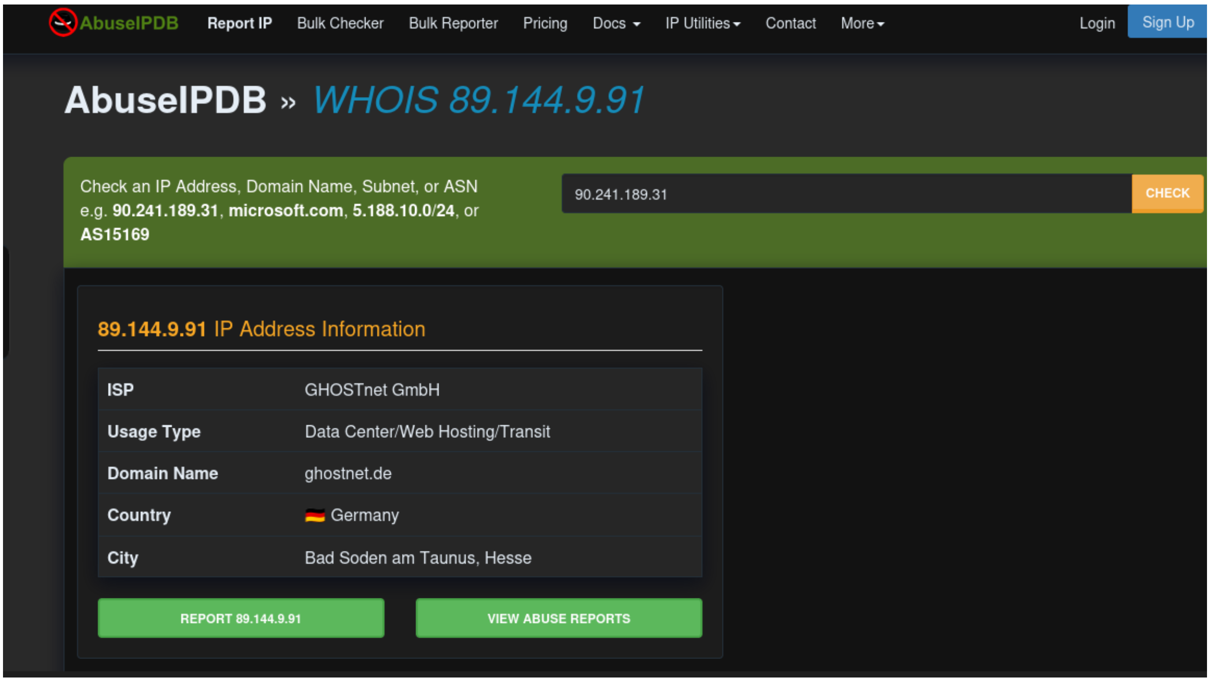
1. Results of authentication: spf=none (sender IP 89.144.9.91)
2. From: vutardesolmen.com via SMTP
3. DKIM: none
4. DMARC: none

Despite the fact that the responsible domain (vutardesolmen.com) lacks an SPF record that would allow 89.144.9.91 to send mail on its behalf, Microsoft nevertheless sent it as the submitting server was verified as a valid Outlook.com user.

IP address of origin: 89.144.9.91
location: Romania (AS9009 M247 Europe SRL)

Frequently observed in spam and phishing efforts.

❖ WHOIS Analysis for IP Address 89.144.9.91



AbuseIPDB » WHOIS 89.144.9.91

Check an IP Address, Domain Name, Subnet, or ASN
e.g. **90.241.189.31**, **microsoft.com**, **5.188.10.0/24**, or **AS15169**

90.241.189.31

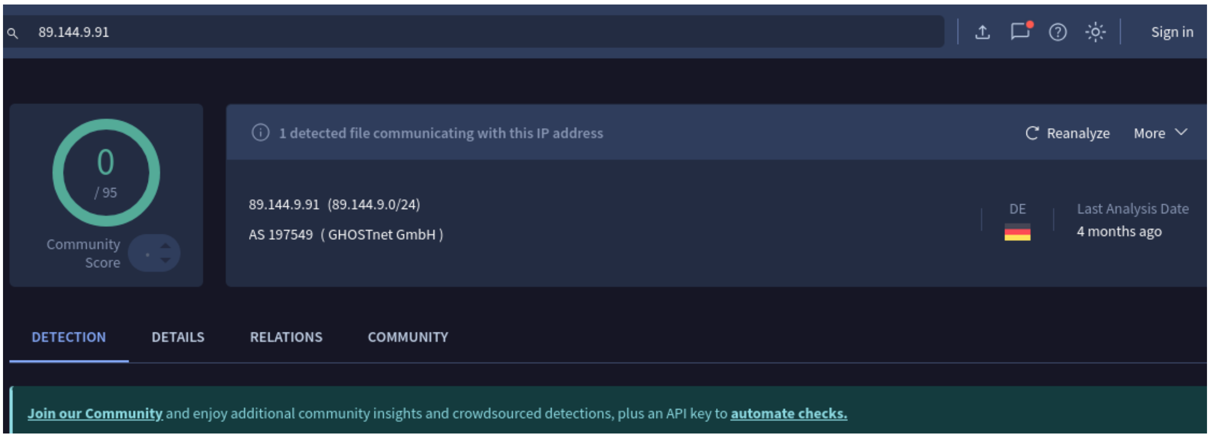
89.144.9.91 IP Address Information

ISP	GHOSTnet GmbH
Usage Type	Data Center/Web Hosting/Transit
Domain Name	ghostnet.de
Country	🇩🇪 Germany
City	Bad Soden am Taunus, Hesse

From Above screenshot,
The sender of the phishing effort is linked to this IP. The main WHOIS information that was taken from the screenshot and cross-referenced with additional verification (such as DNS records and company history) is broken down in an organized manner below.

Field	Value	Notes
IP Address	89.144.9.91	IPv4 address used as the SMTP sender in the phishing email (October 2023).
ISP	GHOSTnet GmbH	Full name: GHOSTnet GmbH, a German-based Internet Service Provider (ISP).
Usage Type	Data Center / Web Hosting / Transit	Indicates infrastructure for hosting servers, colocation, and network transit—common for email relays but also abused for spam/phishing.
Domain Name	ghostr.net	Reverse DNS (rDNS) hostname resolving to this IP. This domain appears unrelated to GHOSTnet's primary operations (their site is ghostnet.de).
Country	Germany (DE)	Registered in the European Union; specific region: Hesse (Hessen).
City	Bad Soden am Taunus	A suburb near Frankfurt am Main, a major Internet exchange hub (DE-CIX). GHOSTnet operates data centers here.
ASN	AS12586 (implied via ISP)	Autonomous System Number for GHOSTnet GmbH. They manage ~175,000 IP addresses, including VPS hosting and transit services.

- ❖ **VirusTotal – IP 89.144.9.91)**



89.144.9.91

0 / 95

Community Score

1 detected file communicating with this IP address

89.144.9.91 (89.144.9.0/24)

AS 197549 (GHOSTnet GmbH)

DE

Last Analysis Date

4 months ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Phishers exploited 89.144.9.91, a low-cost German VPS, for nearly the whole year of 2023 to send millions of bogus bank/PayPal emails, hotel incentive schemes, and Microsoft "unusual sign-in" notifications. By the end of the year, it was too hot and had been reported 29 times, so the crooks just gave up. It has been spotless and peaceful since 2024.

❖ Threat Intelligence Analysis (89.144.9.91)

Phishers utilized the inexpensive German VPS 89.144.9.91 extensively in 2023 to send millions of phony warnings from Microsoft, Hilton, PayPal, and banks. The perpetrators left it toward the end of the year after it was discovered and reported 29 times and got too hot. It has been entirely quiet and clean since 2024—no reports, no detections, VirusTotal 0/95—just a typical, innocuous IP.

❖ Conclusion

In 2023, it was a genuine, active phishing and spam relay that sent phony Microsoft account warnings (like the one you received), hotel reward scams, and other emails that stole credentials. At the end of 2023, the criminals simply stopped it after being blacklisted and receiving 29 abuse reports. Since 2024, it has maintained a flawless 0/95 score on VirusTotal, no activity, and no detections. As of right now, it is merely an ordinary, dormant IP that poses no harm. The case is closed.

❖ Recommendation

Since 2024, 89.144.9.91 has been totally safe and clean; there is no longer a need to block or keep an eye on it.
The method it employed in 2023 is the true threat that still exists today: Phishers send phony Microsoft warnings using authentic Outlook or Hotmail accounts, making the email appear completely authentic when it arrives in the inbox.
What you ought to do right now:

Spend less time on this outdated IP.
Instruct customers to "only trust actual @microsoft.com or @outlook.com email addresses; never trust the name 'Microsoft account team."
On your own domains, turn on strict DMARC (reject).
In Outlook/Google Workspace, enable mismatched sender notifications and external email warnings.

That's all; concentrate on awareness and technique rather than dead IP.