Phishing Email Analysis Report

Prepared by:

Temitope C Folowosele

Cybersecurity Analyst

Date: 29th December 2025

Phishing email-Lowe's Black Friday reward

1. **Executive summary**

This email is a high-confidence phishing attack using brand impersonation (Lowe's) and a high-value lure (Makita 6-pc Combo Kit) to deceive recipients. The technical analysis reveals a total lack of email authentication (SPF, DKIM, DMARC), a mismatch between the displayed sender and the actual mail-from address, and the use of infrastructure known for hosting malicious activity. The primary objective is likely credential harvesting or financial fraud via a malicious URL.

2. Email Metadata Analysis

- **Subject Line:** *-Black Friday Starts Today With Amazing Rewards For you. *
- **Date/Time:** Thu, 9 Nov 2023 14:47:22 +0000
- **Message-ID:**<425ef470-c904-4a77-ab5d-82982b773494@VI1EUR03FT064.eop-EUR03.prod.protection.outlook.com>
- **Recipient:** phishing@pot

3. Sender information

- **Friendly From Name:** Lowe's Department - Black Friday
- **Actual Sender Address:** uywje@y4chj01al8.com
- **Return-Path:** 8ynus48@lnbeem.net
- **Originating IP:** 89.144.44.17
- **Connecting Hostname:** dalimnthefoob.co

4. Email Authentication results

The authentication results indicate that the email failed all modern security checks:

- **SPF (Sender Policy Framework): none**
  - **Result:** spf=none (sender IP is 89.144.44.17) smtp.mailfrom=lnbeem.net
  - **Explanation:** The domain lnbeem.net has not authorized the sending IP to send mail on its behalf, or the domain lacks an SPF record entirely.
- **DKIM (DomainKeys Identified Mail): none**
  - **Result:** dkim=none (message not signed)

    - **Explanation:** The email lacks a cryptographic signature. There is no way to verify that the email content was not altered in transit or that it actually originated from the claimed domain.

- **DMARC (Domain-based Message Authentication, Reporting, and Conformance): none**

    - **Result:** dmarc=none action=none

    - **Explanation:** The sender domain has no DMARC policy. This allows attackers to spoof the domain with no instructions provided to receiving servers on how to handle the failure.

- **Composite Authentication:** compauth=fail

5. WHOIS & Threat Intelligence Analysis

- **IP Address Reputation (89.144.44.17):**

    - **ISP:** GHOSTNET GmbH

    - **Location:** Frankfurt am Main, Germany

    - **Reputation Details:** AbuseIPDB indicates this IP belongs to a data center/web hosting provider. While it currently shows a 0% abuse confidence in the screenshot, it has been reported 9 times previously for suspicious activity.

- **Domain Analysis:**

    - y4chj01al8.com: Appears to be a DGA (Domain Generation Algorithm) address, often used by botnets and phishers to create short-lived, disposable domains.

    - lnbeem.net: Used in the Return-Path; inconsistent with the "From" address.

6. Indicators of Compromise (IoCs)

- **Source IP:** 89.144.44.17

- **Malicious Domains:** y4chj01al8.com, lnbeem.net, dalimnthefoob.co

- **Subject Keywords:** "Black Friday", "Amazing Rewards", "Makita 6-pc Combo Kit"

7. Email Header Anomalies

1. **Display Name Spoofing:** The email uses "Lowe's Department" to gain trust, but the underlying email address (uywje@y4chj01al8.com) has no affiliation with Lowe's Companies, Inc.

2. **Return-Path Mismatch:** The Return-Path domain (lnbeem.net) does not match the From domain (y4chj01al8.com), which is a common sign of bulk-sending phishing tools.

3. **Infrastructure:** The mail was routed through a German data center (Ghostnet) rather than a commercial email service provider or corporate mail server.

8. Malicious URL Analysis

The email contains a call-to-action button: **"Take Your Rewards Now!"**.

- **Likely Behavior:** Clicking this link typically redirects through multiple domains to obfuscate the destination, which usually presents a fake survey or a checkout page asking for "shipping fees" to harvest credit card details.

9. Conclusion & Recommendations

Conclusion: This is a **confirmed attempt to phish**. The attacker is leveraging the popularity of Black Friday and Makita tools to trick users into providing personal or financial information.

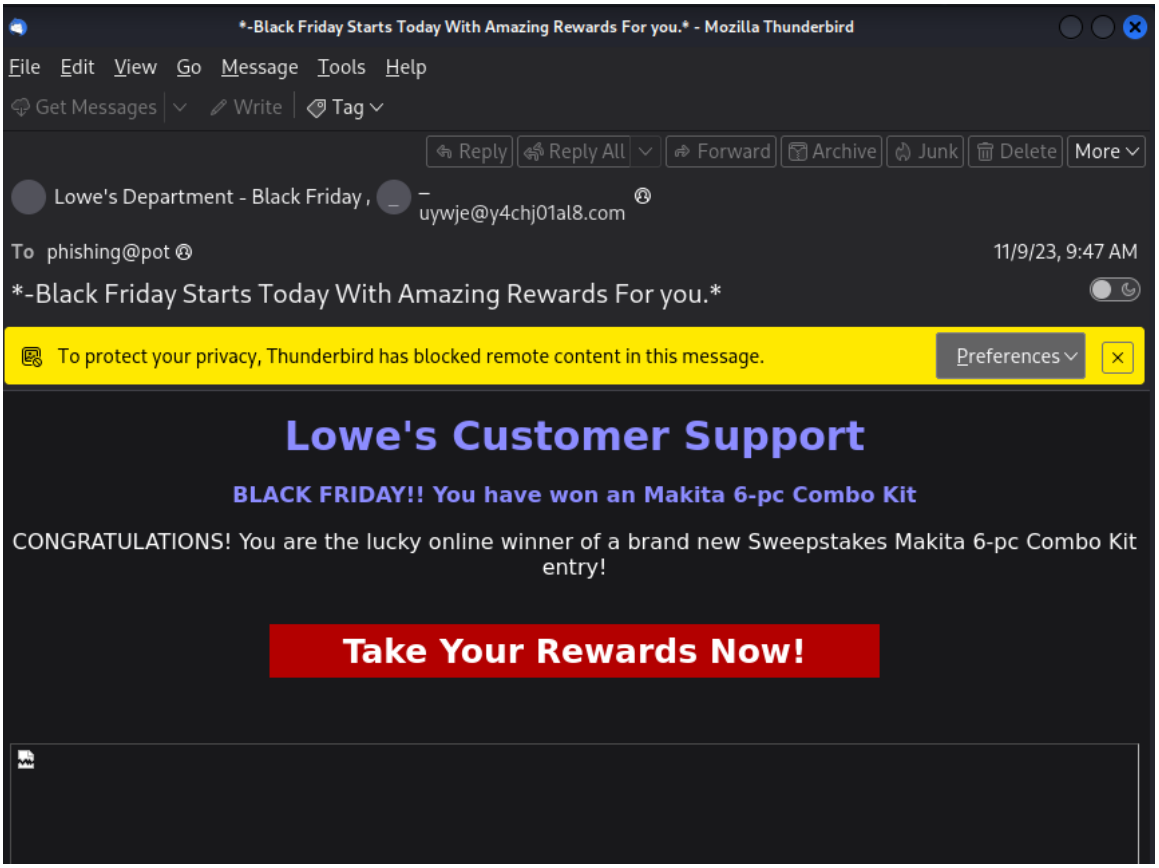
Recommendations:

1. **Block Indicators:** Add IP 89.144.44.17 and domains y4chj01al8.com and lnbeem.net to the organization's blocklist.

2. **User Awareness:** Alert employees that Lowe's does not send "won a prize" emails from random .com or .net domains.

3. **Delete Email:** Do not click any links or download any attachments; the email should be permanently deleted from the mail system.

4. **Security Policy:** Ensure your email gateway is configured to quarantine or reject emails with compauth=fail or missing authentication records.


-Black Friday Starts Today With Amazing Rewards For you. - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
Preferences

Lowe's Department - Black Friday , _ uywje@y4chj01al8.com

To phishing@pot

11/9/23, 9:47 AM

-Black Friday Starts Today With Amazing Rewards For you.

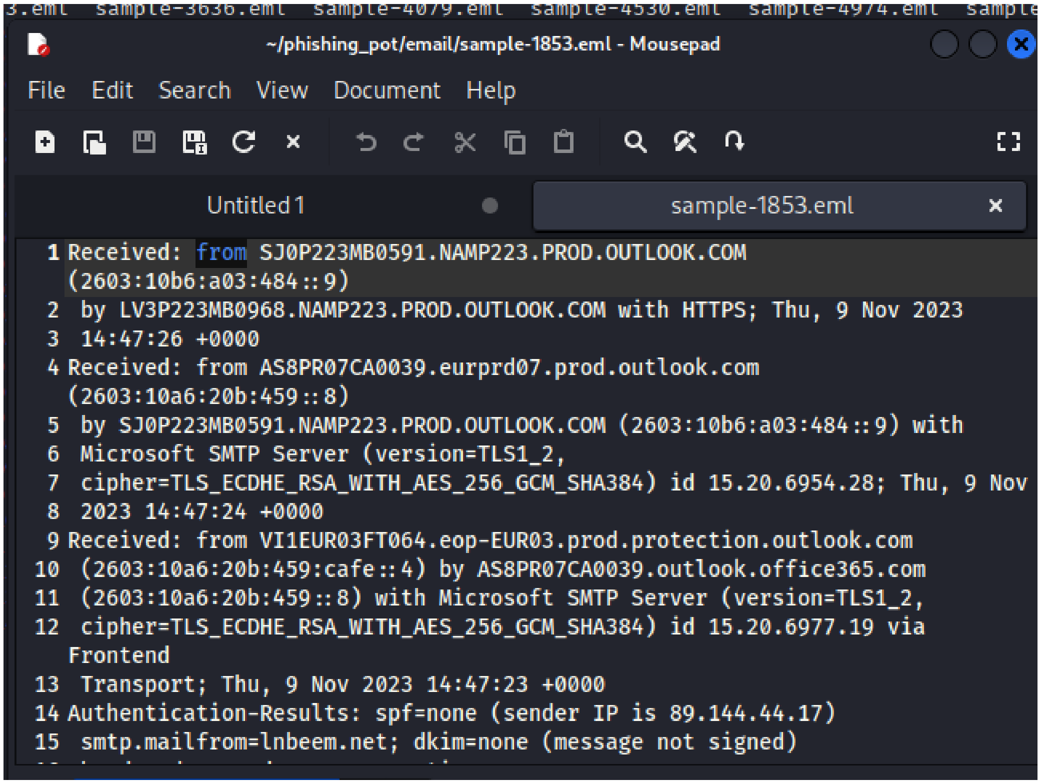
To protect your privacy, Thunderbird has blocked remote content in this message.

Lowe's Customer Support

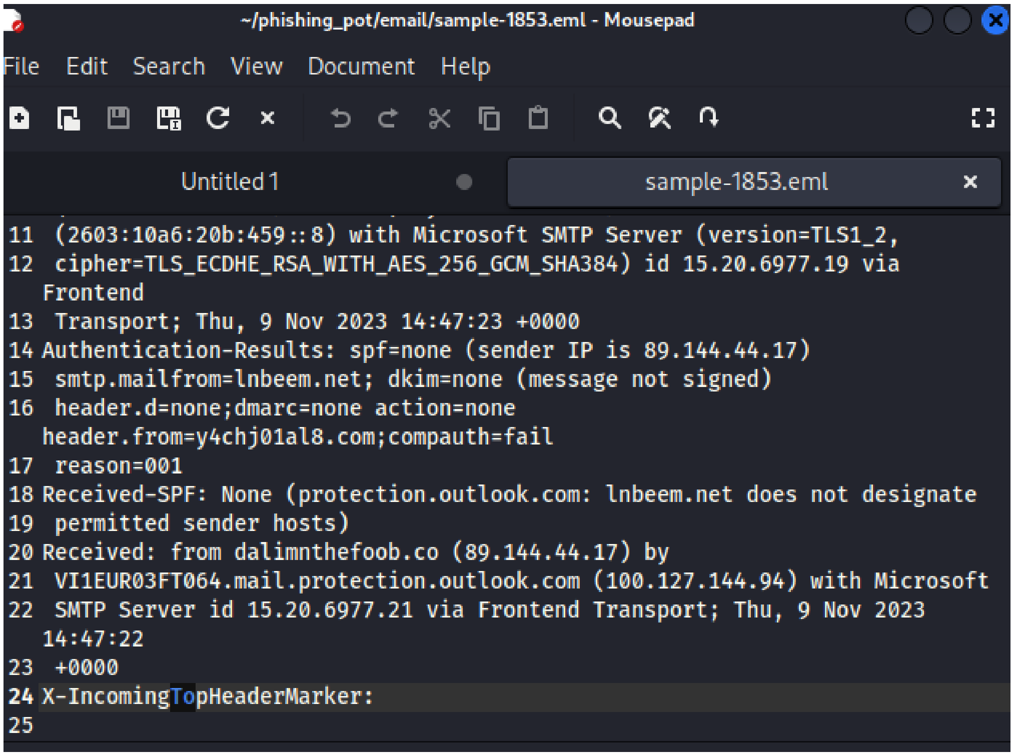
BLACK FRIDAY!! You have won an Makita 6-pc Combo Kit

CONGRATULATIONS! You are the lucky online winner of a brand new Sweepstakes Makita 6-pc Combo Kit entry!

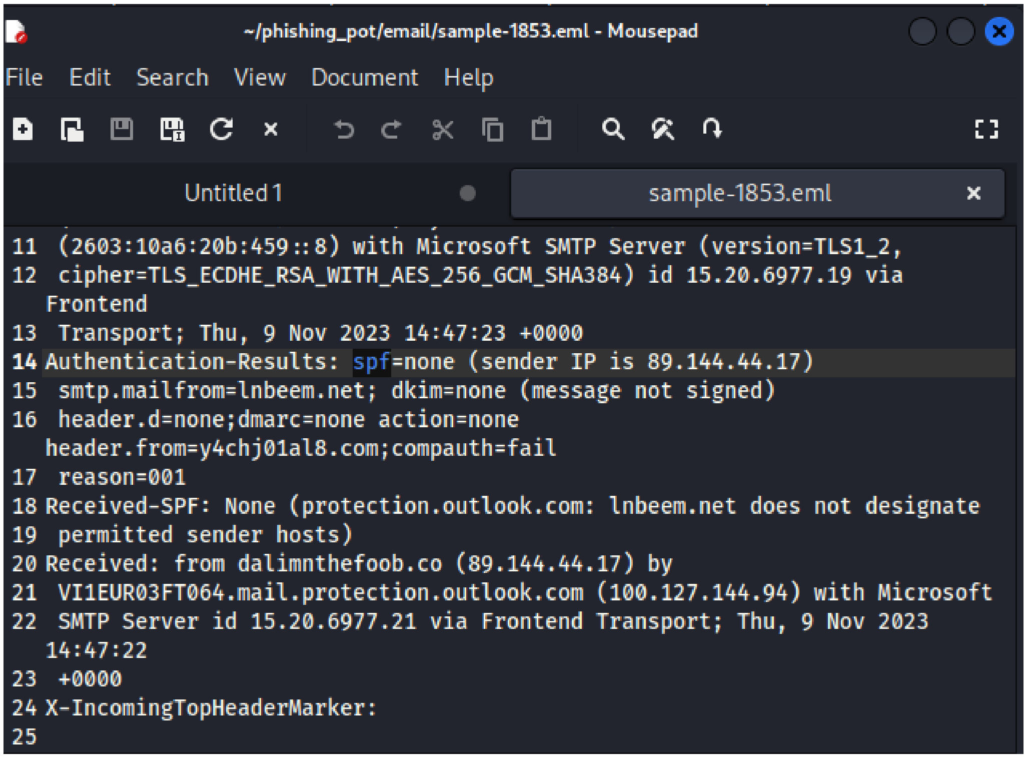
Take Your Rewards Now!


3.eml sample-3636.eml sample-4079.eml sample-4530.eml sample-4974.eml sample
~/phishing_pot/email/sample-1853.eml - Mousepad
File Edit Search View Document Help
Untitled 1
sample-1853.eml

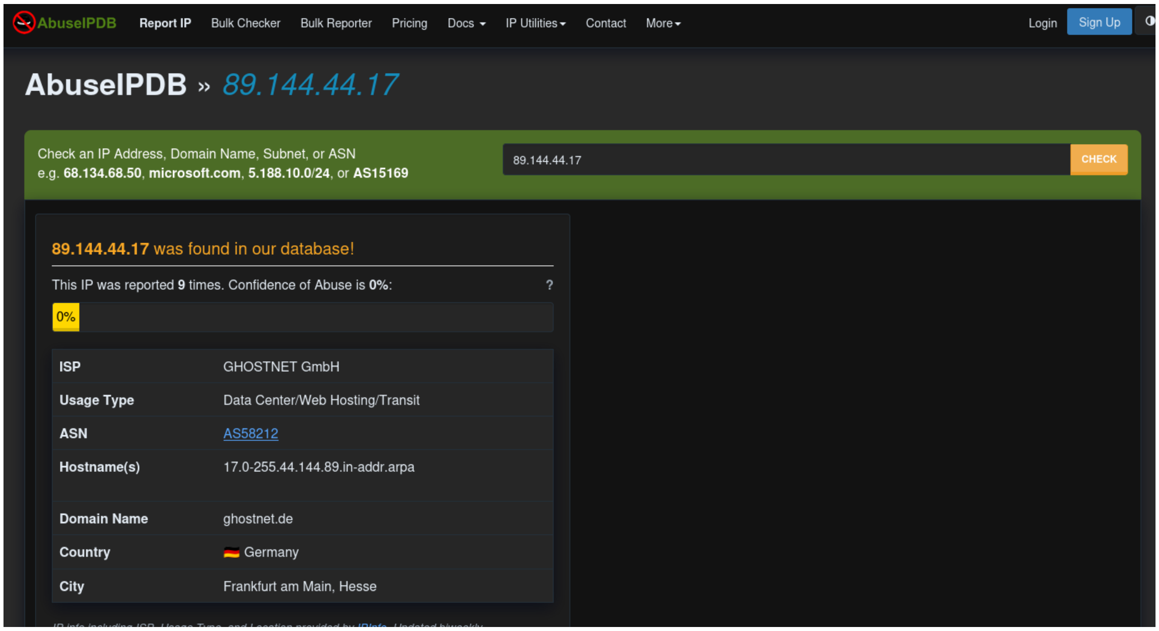
```
Received: from SJ0P223MB0591.NAMP223.PROD.OUTLOOK.COM
(2603:10b6:a03:484::9)
 by LV3P223MB0968.NAMP223.PROD.OUTLOOK.COM with HTTPS; Thu, 9 Nov 2023
 14:47:26 +0000
Received: from AS8PR07CA0039.eurprd07.prod.outlook.com
(2603:10a6:20b:459::8)
 by SJ0P223MB0591.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:484::9) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6954.28; Thu, 9 Nov
 2023 14:47:24 +0000
Received: from VI1EUR03FT064.eop-EUR03.prod.protection.outlook.com
 (2603:10a6:20b:459:cafe::4) by AS8PR07CA0039.outlook.office365.com
 (2603:10a6:20b:459::8) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.19 via
Frontend
 Transport; Thu, 9 Nov 2023 14:47:23 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.17)
 smtp.mailfrom=lnbeem.net; dkim=none (message not signed)
```


~/phishing_pot/email/sample-1853.eml - Mousepad
File Edit Search View Document Help
Untitled 1
sample-1853.eml

```
 (2603:10a6:20b:459::8) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.19 via
Frontend
 Transport; Thu, 9 Nov 2023 14:47:23 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.17)
 smtp.mailfrom=lnbeem.net; dkim=none (message not signed)
 header.d=none;dmarc=none action=none
header.from=y4chj01al8.com;compauth=fail
 reason=001
Received-SPF: None (protection.outlook.com: lnbeem.net does not designate
 permitted sender hosts)
Received: from dalimnthefoob.co (89.144.44.17) by
 VI1EUR03FT064.mail.protection.outlook.com (100.127.144.94) with Microsoft
 SMTP Server id 15.20.6977.21 via Frontend Transport; Thu, 9 Nov 2023
14:47:22
 +0000
X-IncomingTopHeaderMarker:
```


~/phishing_pot/email/sample-1853.eml - Mousepad
File Edit Search View Document Help
Untitled 1
sample-1853.eml

```
 (2603:10a6:20b:459::8) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.19 via Frontend
 Transport; Thu, 9 Nov 2023 14:47:23 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.17)
 smtp.mailfrom=lnbeem.net; dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.from=y4chj01al8.com;compauth=fail
 reason=001
Received-SPF: None (protection.outlook.com: lnbeem.net does not designate
 permitted sender hosts)
Received: from dalimnthefoob.co (89.144.44.17) by
 VI1EUR03FT064.mail.protection.outlook.com (100.127.144.94) with Microsoft
 SMTP Server id 15.20.6977.21 via Frontend Transport; Thu, 9 Nov 2023 14:47:22
 +0000
X-IncomingTopHeaderMarker:
```



AbuseIPDB » *89.144.44.17*

Check an IP Address, Domain Name, Subnet, or ASN
e.g. **68.134.68.50**, **microsoft.com**, **5.188.10.0/24**, or **AS15169**

89.144.44.17

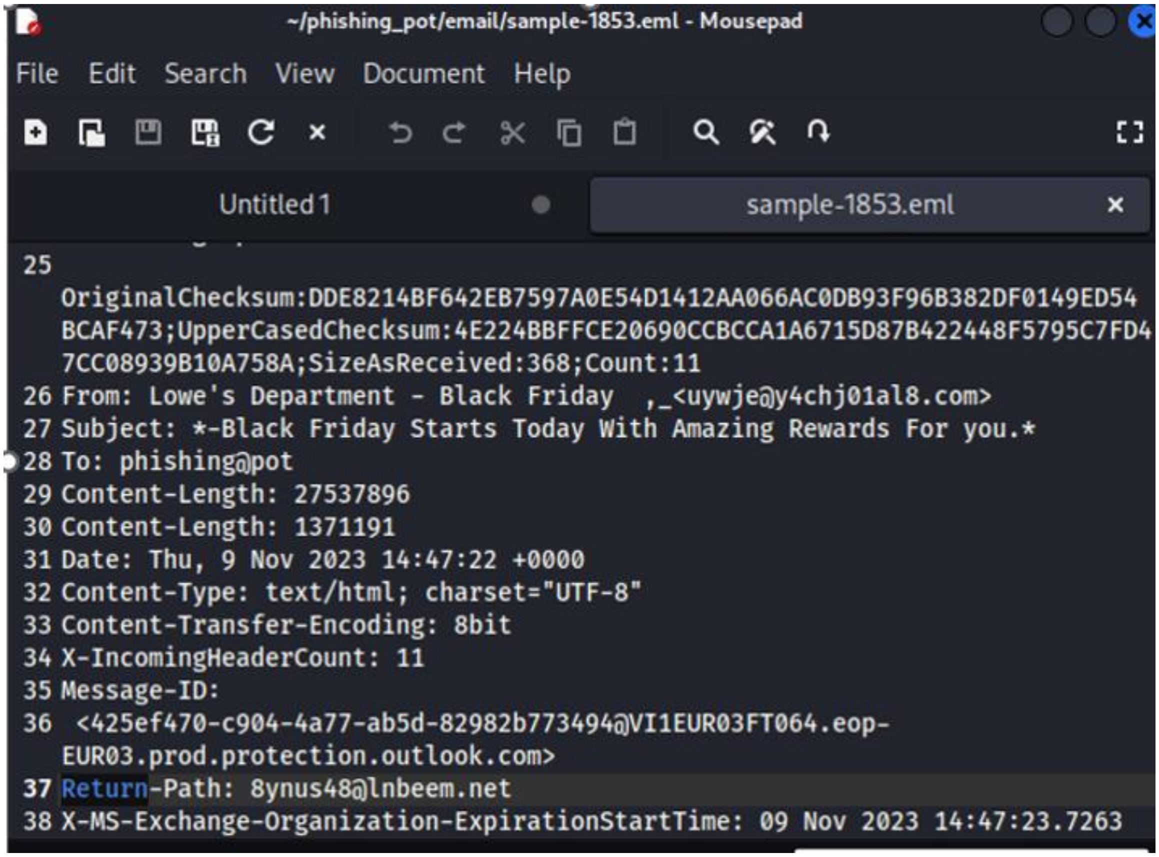
89.144.44.17 was found in our database!

This IP was reported **9** times. Confidence of Abuse is **0%**: ?

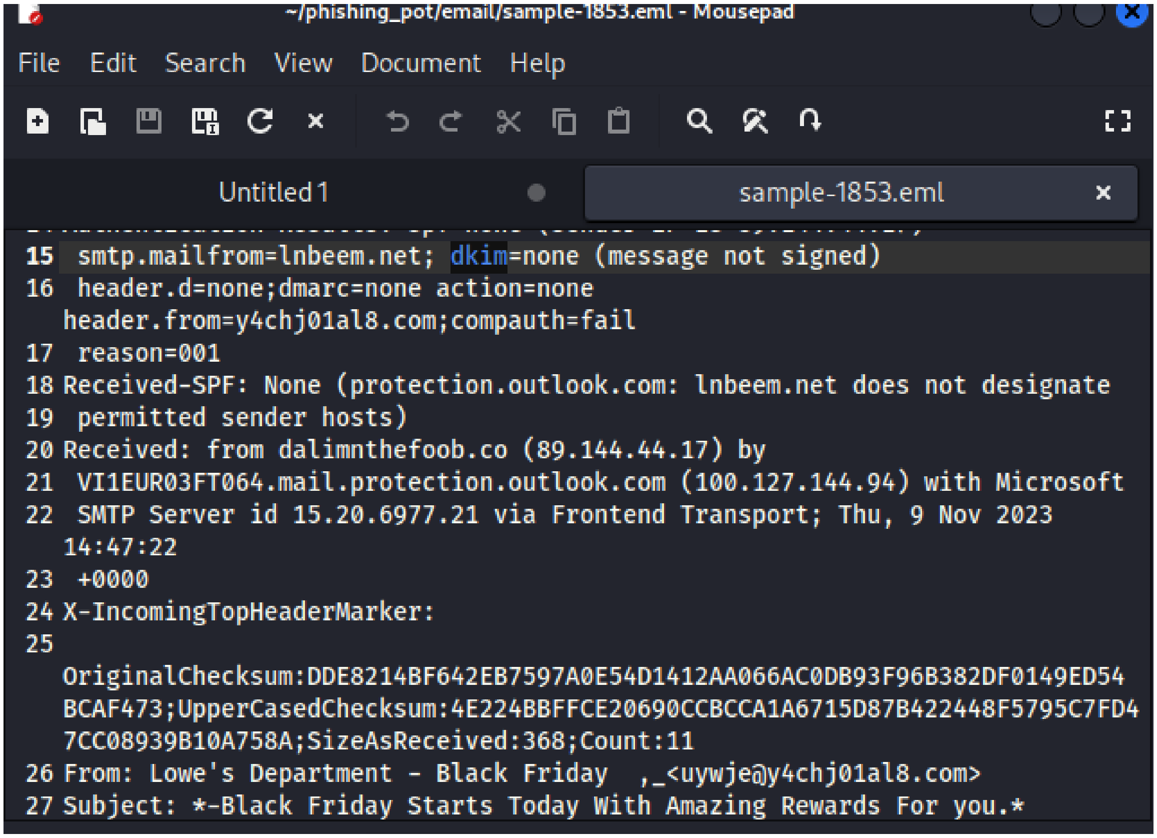
0%

ISP	GHOSTNET GmbH
Usage Type	Data Center/Web Hosting/Transit
ASN	AS58212
Hostname(s)	17.0-255.44.144.89.in-addr.arpa
Domain Name	ghostnet.de
Country	🇩🇪 Germany
City	Frankfurt am Main, Hesse

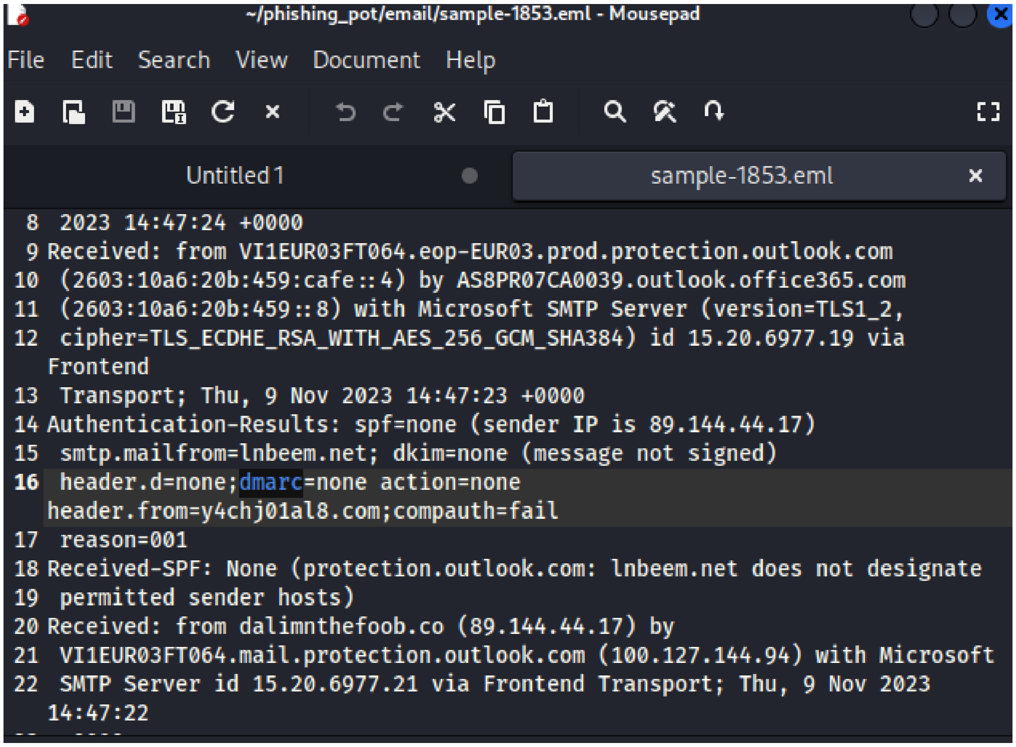
IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly



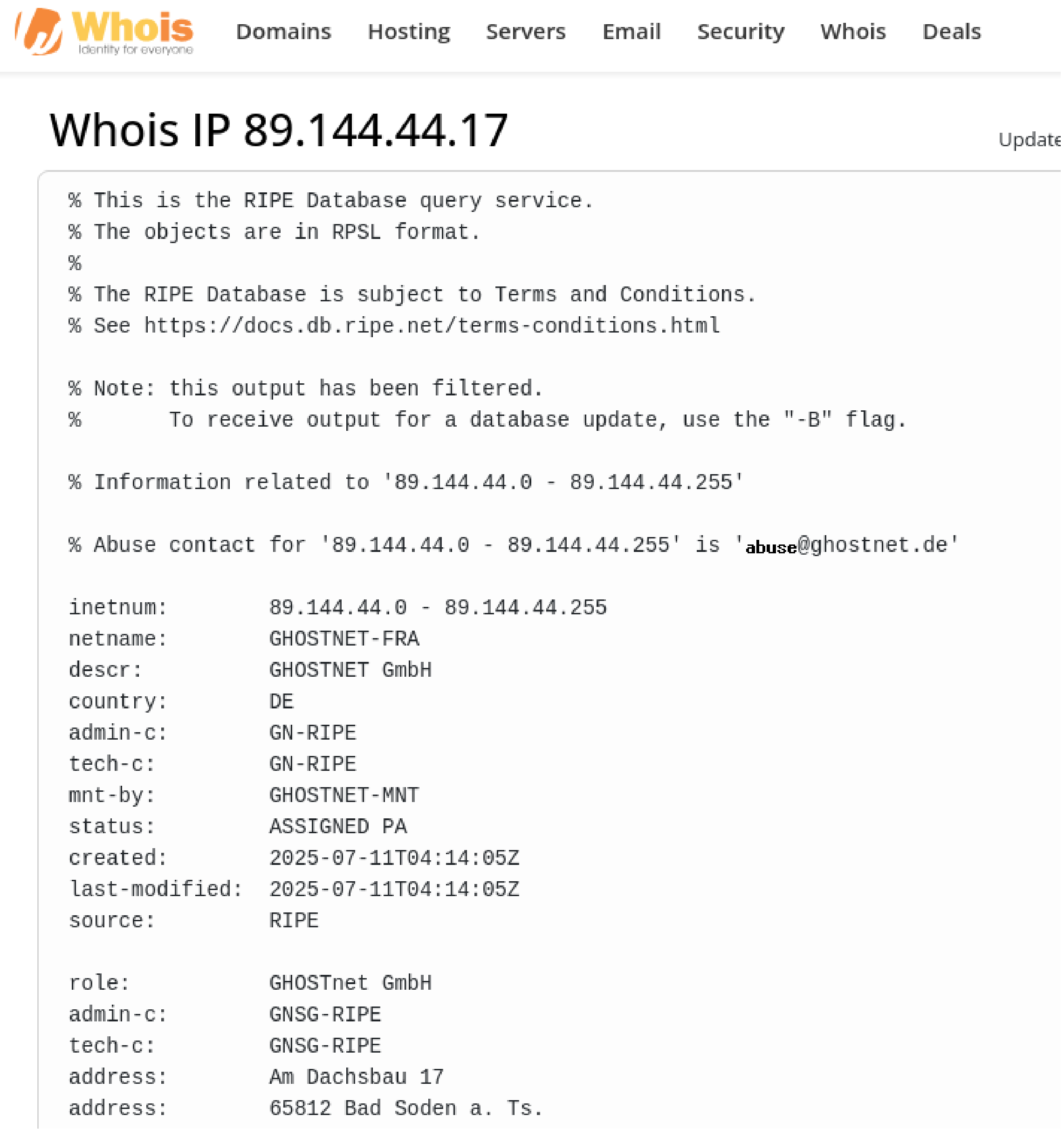
```
OriginalChecksum:DDE8214BF642EB7597A0E54D1412AA066AC0DB93F96B382DF0149ED54
BCAF473;UpperCasedChecksum:4E224BBFFCE20690CCBCCA1A6715D87B422448F5795C7FD4
7CC08939B10A758A;SizeAsReceived:368;Count:11
From: Lowe's Department - Black Friday  ,_<uywje@y4chj01al8.com>
Subject: *-Black Friday Starts Today With Amazing Rewards For you.*
To: phishing@pot
Content-Length: 27537896
Content-Length: 1371191
Date: Thu, 9 Nov 2023 14:47:22 +0000
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
X-IncomingHeaderCount: 11
Message-ID:
 <425ef470-c904-4a77-ab5d-82982b773494@VI1EUR03FT064.eop-
EUR03.prod.protection.outlook.com>
Return-Path: 8ynus48@lnbeem.net
X-MS-Exchange-Organization-ExpirationStartTime: 09 Nov 2023 14:47:23.7263
```



```
 smtp.mailfrom=lnbeem.net; dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.from=y4chj01al8.com;compauth=fail
 reason=001
Received-SPF: None (protection.outlook.com: lnbeem.net does not designate
 permitted sender hosts)
Received: from dalimnthefoob.co (89.144.44.17) by
 VI1EUR03FT064.mail.protection.outlook.com (100.127.144.94) with Microsoft
 SMTP Server id 15.20.6977.21 via Frontend Transport; Thu, 9 Nov 2023 14:47:22
 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:DDE8214BF642EB7597A0E54D1412AA066AC0DB93F96B382DF0149ED54BCAF473;UpperCasedChecksum:4E224BBFFCE20690CCBCCA1A6715D87B422448F5795C7FD47CC08939B10A758A;SizeAsReceived:368;Count:11
From: Lowe's Department - Black Friday  ,_<uywje@y4chj01al8.com>
Subject: *-Black Friday Starts Today With Amazing Rewards For you.*
```

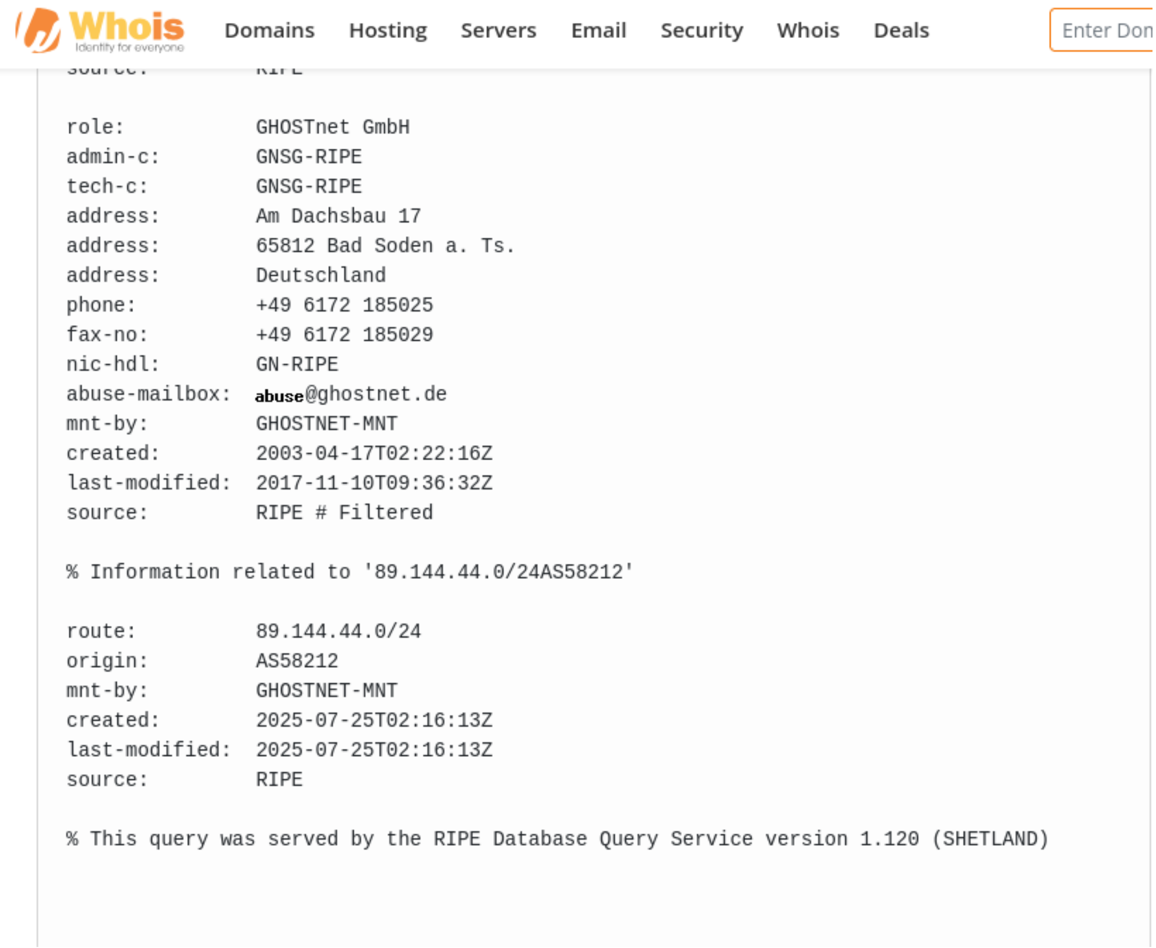


```
 2023 14:47:24 +0000
Received: from VI1EUR03FT064.eop-EUR03.prod.protection.outlook.com
 (2603:10a6:20b:459:cafe::4) by AS8PR07CA0039.outlook.office365.com
 (2603:10a6:20b:459::8) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.19 via Frontend
 Transport; Thu, 9 Nov 2023 14:47:23 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.17)
 smtp.mailfrom=lnbeem.net; dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.from=y4chj01al8.com;compauth=fail
 reason=001
Received-SPF: None (protection.outlook.com: lnbeem.net does not designate
 permitted sender hosts)
Received: from dalimnthefoob.co (89.144.44.17) by
 VI1EUR03FT064.mail.protection.outlook.com (100.127.144.94) with Microsoft
 SMTP Server id 15.20.6977.21 via Frontend Transport; Thu, 9 Nov 2023 14:47:22
```



Whois IP 89.144.44.17

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '89.144.44.0 - 89.144.44.255'

% 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.
```



```
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
nic-hdl:        GN-RIPE
abuse-mailbox:  abuse@ghostnet.de
mnt-by:         GHOSTNET-MNT
created:        2003-04-17T02:22:16Z
last-modified:  2017-11-10T09:36:32Z
source:         RIPE # Filtered

% Information related to '89.144.44.0/24AS58212'

route:          89.144.44.0/24
origin:         AS58212
mnt-by:         GHOSTNET-MNT
created:        2025-07-25T02:16:13Z
last-modified:  2025-07-25T02:16:13Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.120 (SHETLAND)
```

Report Prepared by:

Temitope C Folowosele

Cybersecurity Analyst