Phishing Email Analysis Report

By:

Jarinat kareem, Cybersecurity Analyst

Date: November 26, 2025

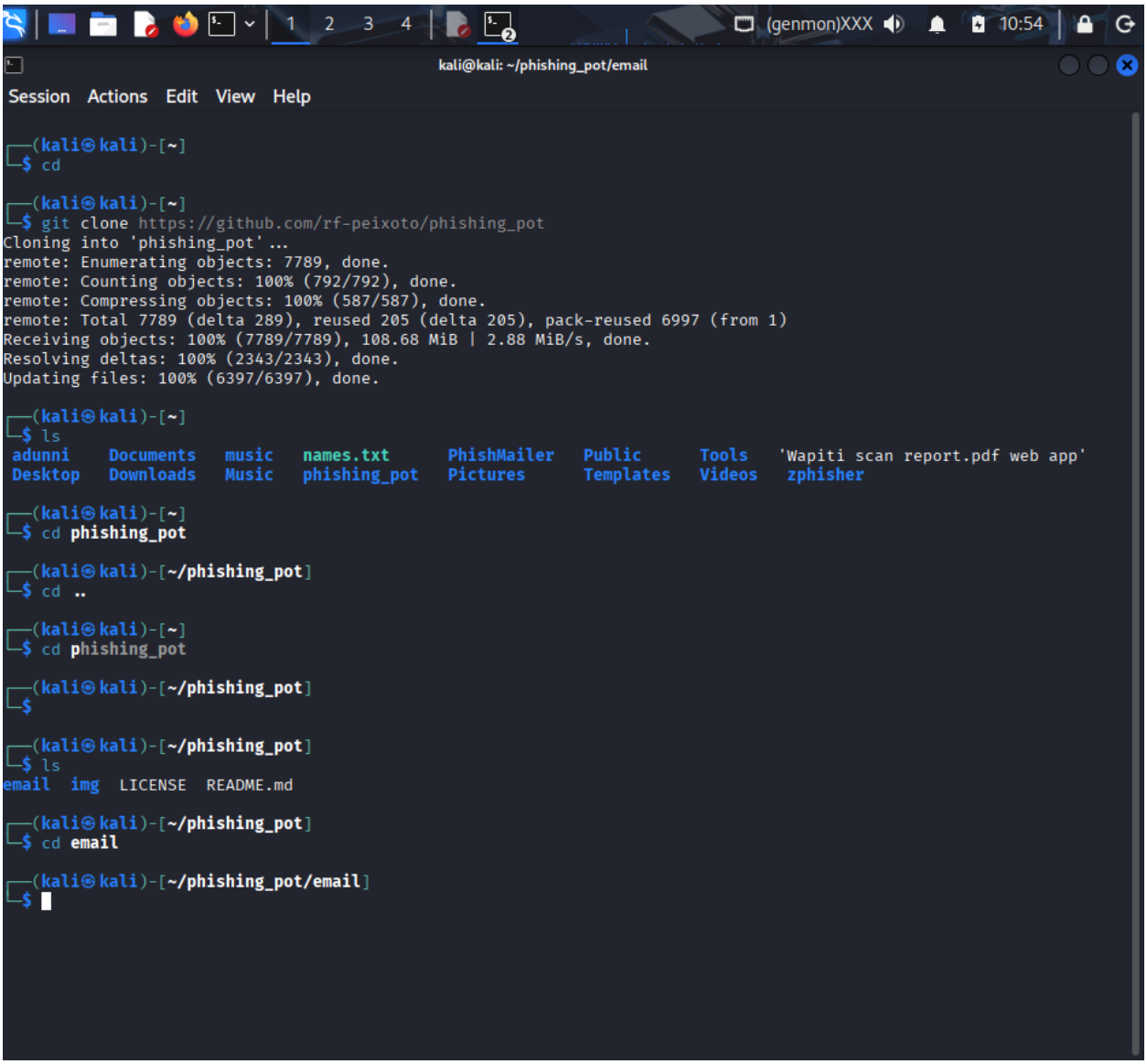
1. Executive Summary

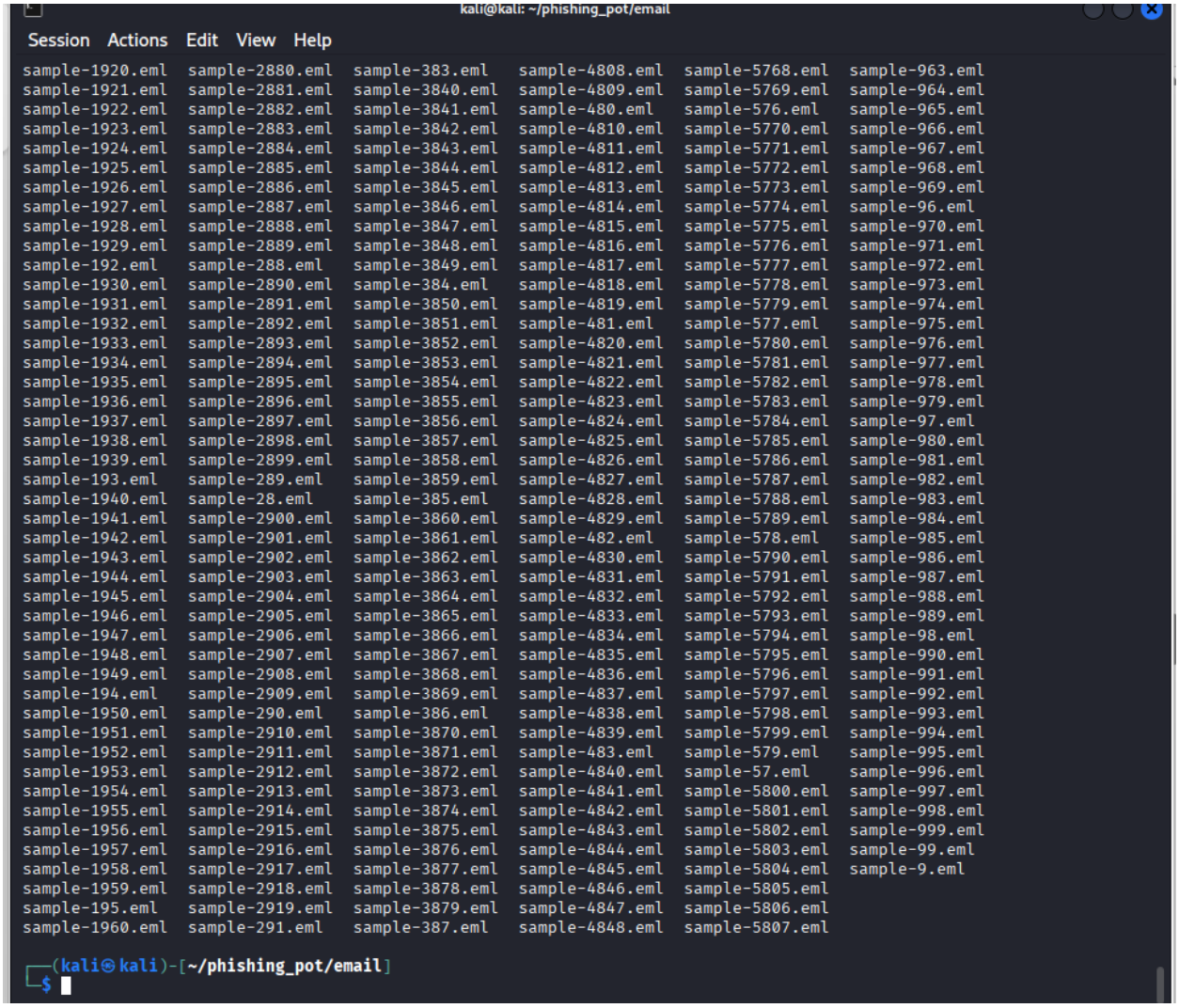
Conducted an in-depth analysis of a suspicious email received through the corporate email gateway. The email was isolated in a sandboxed virtual environment and subjected to multi‑layered analysis techniques, including header inspection, URL reputation analysis, and threat intelligence gathering. Based on the results, it is concluded that the email is a phishing attempt designed to lure users into clicking a malicious link.

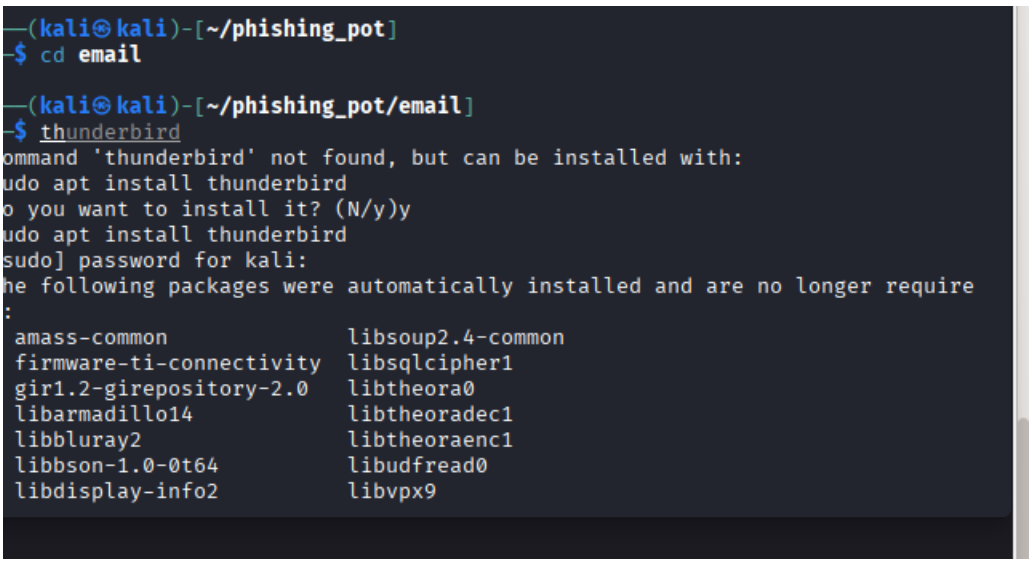
2. Email Metadata Analysis

2.1 Sender Information

- Return-Path: apache@sk.globalexceltrade.xyz
- Sending Server: SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (::1)
- Sender IP Address: 151.80.93.107
- IP Reputation Check (AbuseIPDB): No existing reports were found for this IP address in the AbuseIPDB database. However, the lack of reports does not indicate safety, especially given the suspicious context.


1 2 3 4
(genmon)XXX
10:54
kali@kali: ~/phishing_pot/email
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/rf-peixoto/phishing_pot
Cloning into 'phishing_pot' ...
remote: Enumerating objects: 7789, done.
remote: Counting objects: 100% (792/792), done.
remote: Compressing objects: 100% (587/587), done.
remote: Total 7789 (delta 289), reused 205 (delta 205), pack-reused 6997 (from 1)
Receiving objects: 100% (7789/7789), 108.68 MiB | 2.88 MiB/s, done.
Resolving deltas: 100% (2343/2343), done.
Updating files: 100% (6397/6397), done.
┌──(kali㉿kali)-[~]
└─$ ls
adunni Documents music names.txt PhishMailer Public Tools 'Wapiti scan report.pdf web app'
Desktop Downloads Music phishing_pot Pictures Templates Videos zphisher
┌──(kali㉿kali)-[~]
└─$ cd phishing_pot
┌──(kali㉿kali)-[~/phishing_pot]
└─$ cd ..
┌──(kali㉿kali)-[~]
└─$ cd phishing_pot
┌──(kali㉿kali)-[~/phishing_pot]
└─$
┌──(kali㉿kali)-[~/phishing_pot]
└─$ ls
email img LICENSE README.md
┌──(kali㉿kali)-[~/phishing_pot]
└─$ cd email
┌──(kali㉿kali)-[~/phishing_pot/email]
└─$


kali@kali: ~/phishing_pot/email
Session Actions Edit View Help
sample-1920.eml sample-2880.eml sample-383.eml sample-4808.eml sample-5768.eml sample-963.eml
sample-1921.eml sample-2881.eml sample-3840.eml sample-4809.eml sample-5769.eml sample-964.eml
sample-1922.eml sample-2882.eml sample-3841.eml sample-480.eml sample-576.eml sample-965.eml
sample-1923.eml sample-2883.eml sample-3842.eml sample-4810.eml sample-5770.eml sample-966.eml
sample-1924.eml sample-2884.eml sample-3843.eml sample-4811.eml sample-5771.eml sample-967.eml
sample-1925.eml sample-2885.eml sample-3844.eml sample-4812.eml sample-5772.eml sample-968.eml
sample-1926.eml sample-2886.eml sample-3845.eml sample-4813.eml sample-5773.eml sample-969.eml
sample-1927.eml sample-2887.eml sample-3846.eml sample-4814.eml sample-5774.eml sample-96.eml
sample-1928.eml sample-2888.eml sample-3847.eml sample-4815.eml sample-5775.eml sample-970.eml
sample-1929.eml sample-2889.eml sample-3848.eml sample-4816.eml sample-5776.eml sample-971.eml
sample-192.eml sample-288.eml sample-3849.eml sample-4817.eml sample-5777.eml sample-972.eml
sample-1930.eml sample-2890.eml sample-384.eml sample-4818.eml sample-5778.eml sample-973.eml
sample-1931.eml sample-2891.eml sample-3850.eml sample-4819.eml sample-5779.eml sample-974.eml
sample-1932.eml sample-2892.eml sample-3851.eml sample-481.eml sample-577.eml sample-975.eml
sample-1933.eml sample-2893.eml sample-3852.eml sample-4820.eml sample-5780.eml sample-976.eml
sample-1934.eml sample-2894.eml sample-3853.eml sample-4821.eml sample-5781.eml sample-977.eml
sample-1935.eml sample-2895.eml sample-3854.eml sample-4822.eml sample-5782.eml sample-978.eml
sample-1936.eml sample-2896.eml sample-3855.eml sample-4823.eml sample-5783.eml sample-979.eml
sample-1937.eml sample-2897.eml sample-3856.eml sample-4824.eml sample-5784.eml sample-97.eml
sample-1938.eml sample-2898.eml sample-3857.eml sample-4825.eml sample-5785.eml sample-980.eml
sample-1939.eml sample-2899.eml sample-3858.eml sample-4826.eml sample-5786.eml sample-981.eml
sample-193.eml sample-289.eml sample-3859.eml sample-4827.eml sample-5787.eml sample-982.eml
sample-1940.eml sample-28.eml sample-385.eml sample-4828.eml sample-5788.eml sample-983.eml
sample-1941.eml sample-2900.eml sample-3860.eml sample-4829.eml sample-5789.eml sample-984.eml
sample-1942.eml sample-2901.eml sample-3861.eml sample-482.eml sample-578.eml sample-985.eml
sample-1943.eml sample-2902.eml sample-3862.eml sample-4830.eml sample-5790.eml sample-986.eml
sample-1944.eml sample-2903.eml sample-3863.eml sample-4831.eml sample-5791.eml sample-987.eml
sample-1945.eml sample-2904.eml sample-3864.eml sample-4832.eml sample-5792.eml sample-988.eml
sample-1946.eml sample-2905.eml sample-3865.eml sample-4833.eml sample-5793.eml sample-989.eml
sample-1947.eml sample-2906.eml sample-3866.eml sample-4834.eml sample-5794.eml sample-98.eml
sample-1948.eml sample-2907.eml sample-3867.eml sample-4835.eml sample-5795.eml sample-990.eml
sample-1949.eml sample-2908.eml sample-3868.eml sample-4836.eml sample-5796.eml sample-991.eml
sample-194.eml sample-2909.eml sample-3869.eml sample-4837.eml sample-5797.eml sample-992.eml
sample-1950.eml sample-290.eml sample-386.eml sample-4838.eml sample-5798.eml sample-993.eml
sample-1951.eml sample-2910.eml sample-3870.eml sample-4839.eml sample-5799.eml sample-994.eml
sample-1952.eml sample-2911.eml sample-3871.eml sample-483.eml sample-579.eml sample-995.eml
sample-1953.eml sample-2912.eml sample-3872.eml sample-4840.eml sample-57.eml sample-996.eml
sample-1954.eml sample-2913.eml sample-3873.eml sample-4841.eml sample-5800.eml sample-997.eml
sample-1955.eml sample-2914.eml sample-3874.eml sample-4842.eml sample-5801.eml sample-998.eml
sample-1956.eml sample-2915.eml sample-3875.eml sample-4843.eml sample-5802.eml sample-999.eml
sample-1957.eml sample-2916.eml sample-3876.eml sample-4844.eml sample-5803.eml sample-99.eml
sample-1958.eml sample-2917.eml sample-3877.eml sample-4845.eml sample-5804.eml sample-9.eml
sample-1959.eml sample-2918.eml sample-3878.eml sample-4846.eml sample-5805.eml
sample-195.eml sample-2919.eml sample-3879.eml sample-4847.eml sample-5806.eml
sample-1960.eml sample-291.eml sample-387.eml sample-4848.eml sample-5807.eml
(kali㉿kali)-[~/phishing_pot/email]
$

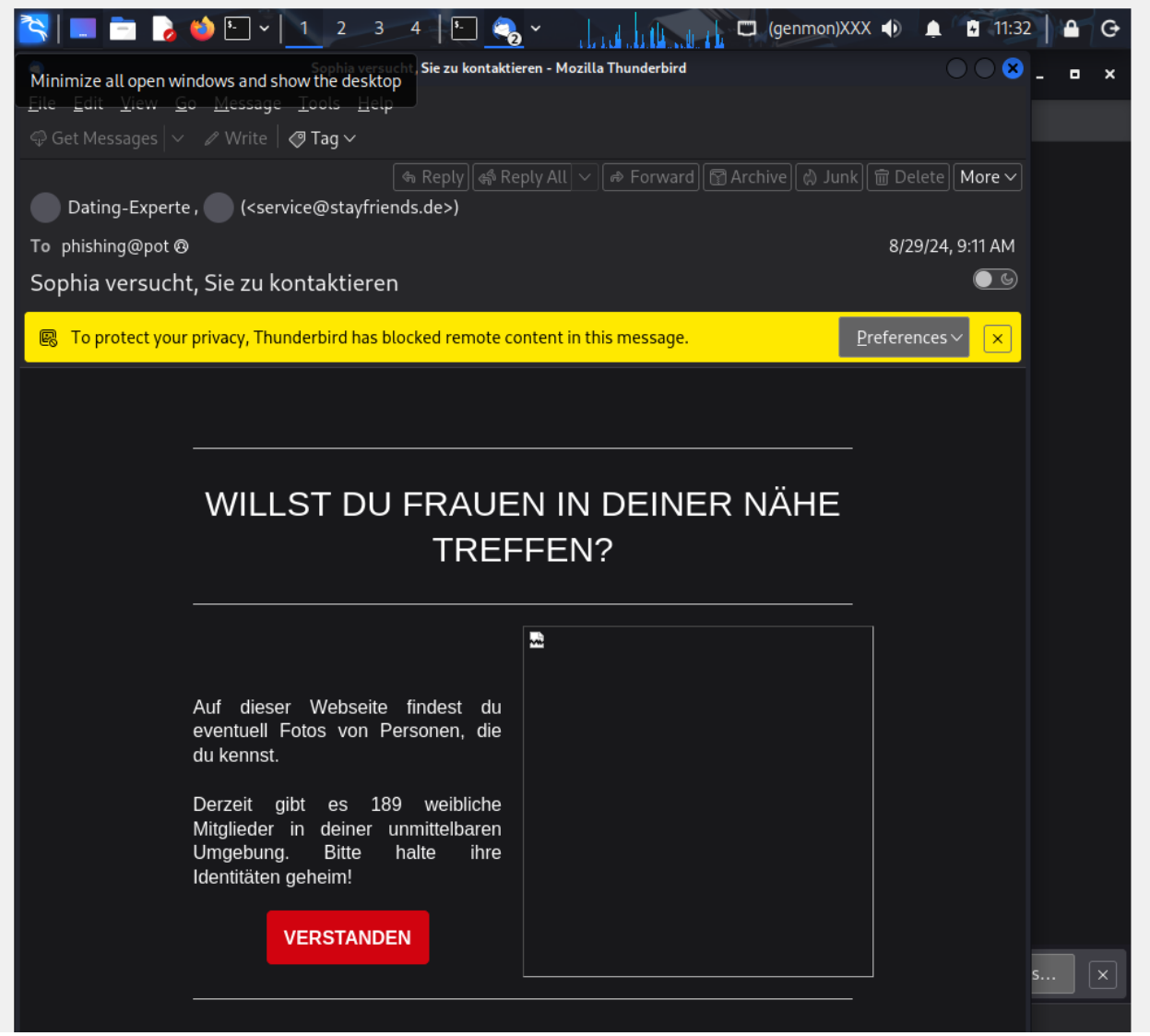

(kali㉿kali)-[~/phishing_pot]
$ cd email
(kali㉿kali)-[~/phishing_pot/email]
$ thunderbird
ommand 'thunderbird' not found, but can be installed with:
udo apt install thunderbird
o you want to install it? (N/y)y
udo apt install thunderbird
sudo] password for kali:
he following packages were automatically installed and are no longer require
:
amass-common
firmware-ti-connectivity
gir1.2-girepository-2.0
libarmadillo14
libbluray2
libbson-1.0-0t64
libdisplay-info2
libsoup2.4-common
libsqlcipher1
libtheora0
libtheoradec1
libtheoraenc1
libudfread0
libvpx9

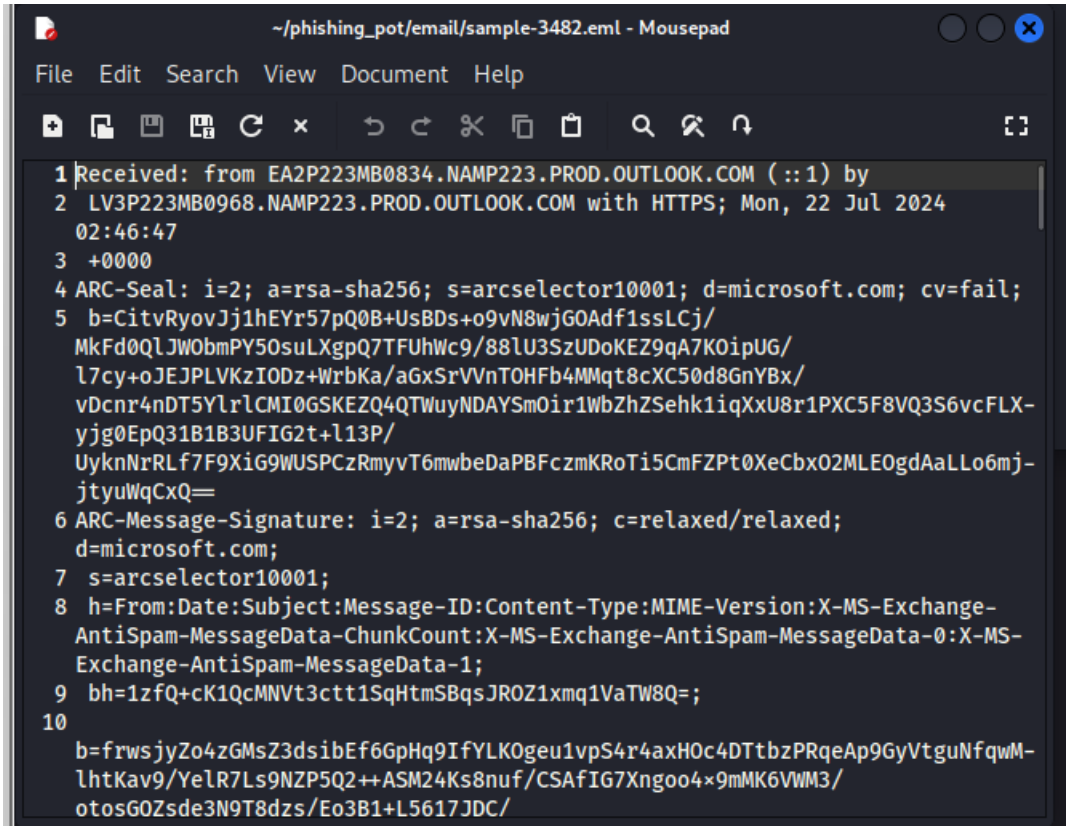
```
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/phishing_pot/email]
└─$ thunderbird
Command 'thunderbird' not found, but can be installed with:
sudo apt install thunderbird
Do you want to install it? (N/y)y
sudo apt install thunderbird
[sudo] password for kali:
The following packages were automatically installed and are no longer require
d:
  amass-common              libsoup2.4-common
  firmware-ti-connectivity  libsqlcipher1
  gir1.2-girepository-2.0   libtheora0
  libarmadillo14            libtheoradec1
  libbluray2                libtheoraenc1
  libbson-1.0-0t64          libudfread0
  libdisplay-info2          libvpx9
  libgdal36                 libwireshark18
  libgdata-common           libwiretap15
  libgdata22                libwsutil16
  libgeos3.13.1             libx264-164
  libgirepository-1.0-1     python3-bluepy
  libhdf4-0-alt             python3-click-plugins
  libinstpatch-1.0-2        python3-gpg
  libjs-jquery-ui           python3-kismetcapturebtgeiger
  libjs-underscore          python3-kismetcapturefreaklabszigbee
  libmongoc-1.0-0t64        python3-kismetcapturertl433
  libnet1                   python3-kismetcapturertladsb
  libobjc-14-dev            python3-kismetcapturertlamr
  libogdi4.1                python3-packaging-whl
  libplacebo349             python3-protobuf
  libportmidi0              python3-wheel-whl
  libqt5ct-common1.8        python3-zombie-imp
  librav1e0.7               samba-ad-dc
  libsframe1                samba-ad-provision
  libsigsegv2               samba-dsdb-modules
  libsoup-2.4-1
Use 'sudo apt autoremove' to remove them.

Installing:
  thunderbird

Installing dependencies:
  libbotan-3-7  libotr5t64  librnp0  libsexpp0  libtspi1

Suggested packages:
  libotr5-bin

Summary:
```

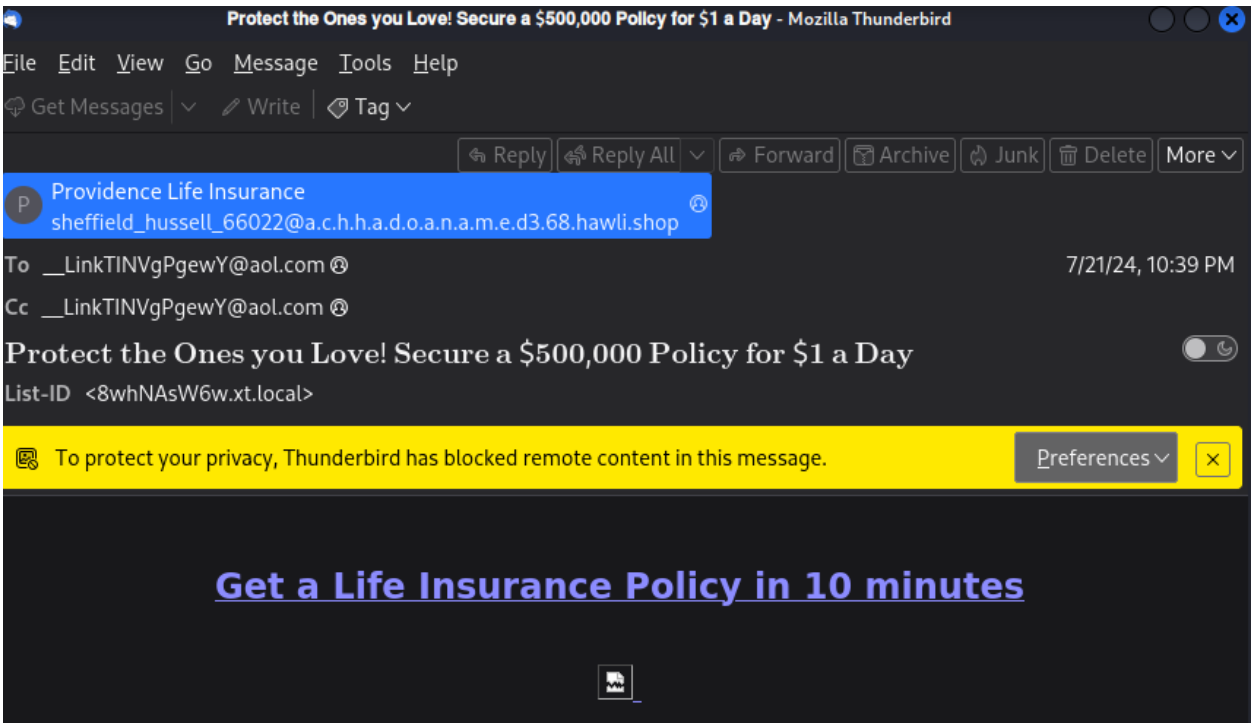
```
Installing:
  thunderbird

Installing dependencies:
  libbotan-3-7  libotr5t64  librnp0  libsexpp0  libtspi1

Suggested packages:
  libotr5-bin

Summary:
  Upgrading: 0, Installing: 6, Removing: 0, Not Upgrading: 8
  Download size: 69.2 MB / 72.4 MB
  Space needed: 291 MB / 51.5 GB available

Continue? [Y/n] y
Err:1 http://http.kali.org/kali kali-rolling/main amd64 thunderbird amd64 1:1
40.4.0esr-1
  404  Not Found [IP: 54.39.128.230 80]
Error: Failed to fetch http://http.kali.org/kali/pool/main/t/thunderbird/thun
derbird_140.4.0esr-1_amd64.deb  404  Not Found [IP: 54.39.128.230 80]
Error: Unable to fetch some archives, maybe run apt update or try with --fix-
missing?
```

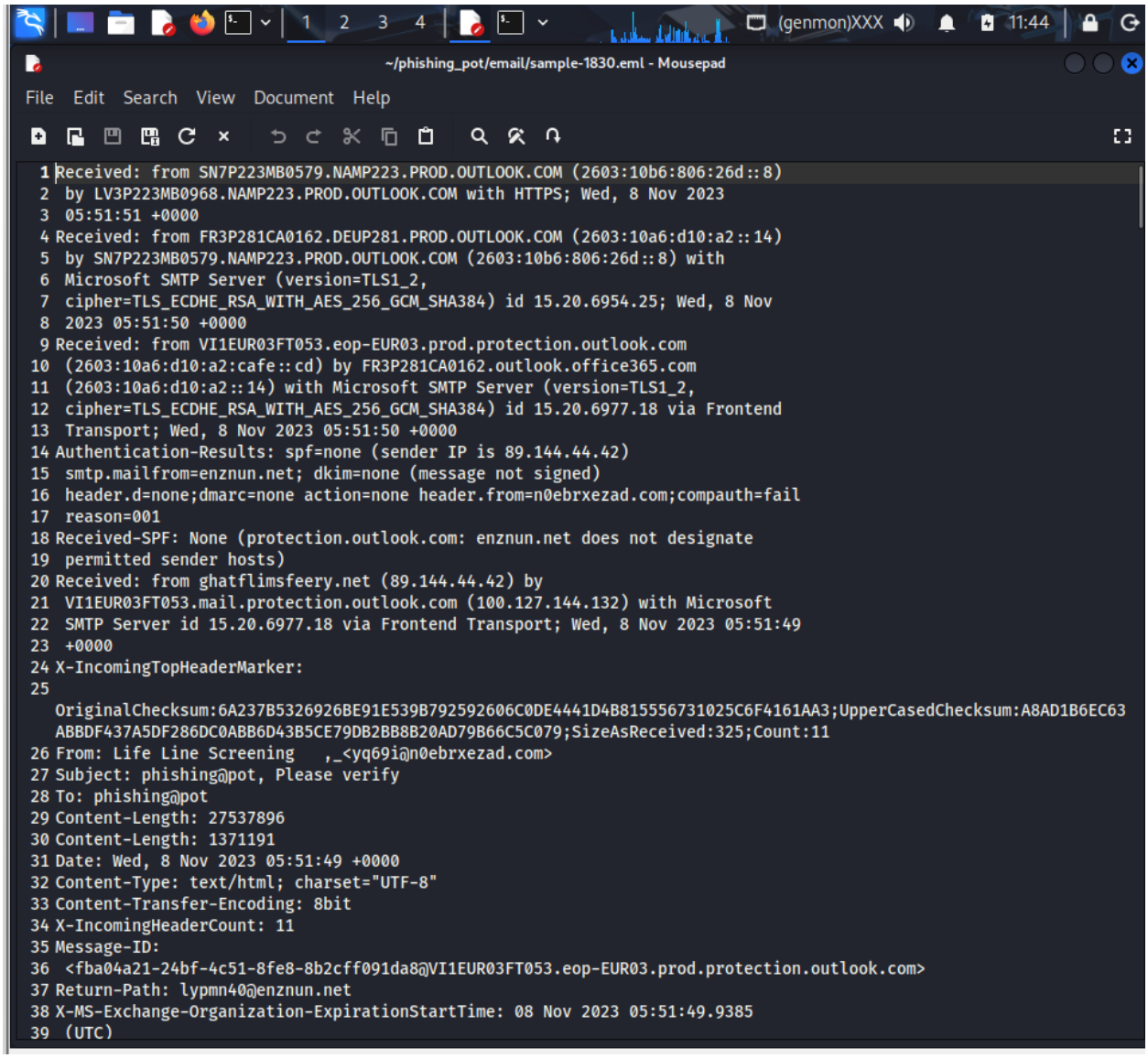
```
┌──(kali㉿kali)-[~/phishing_pot/email]
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.6
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [25
9 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [188 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8
94 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
 [11.7 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents
 (deb) [28.5 kB]
Fetched 75.0 MB in 24s (3,147 kB/s)
154 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~/phishing_pot/email]
└─$
```

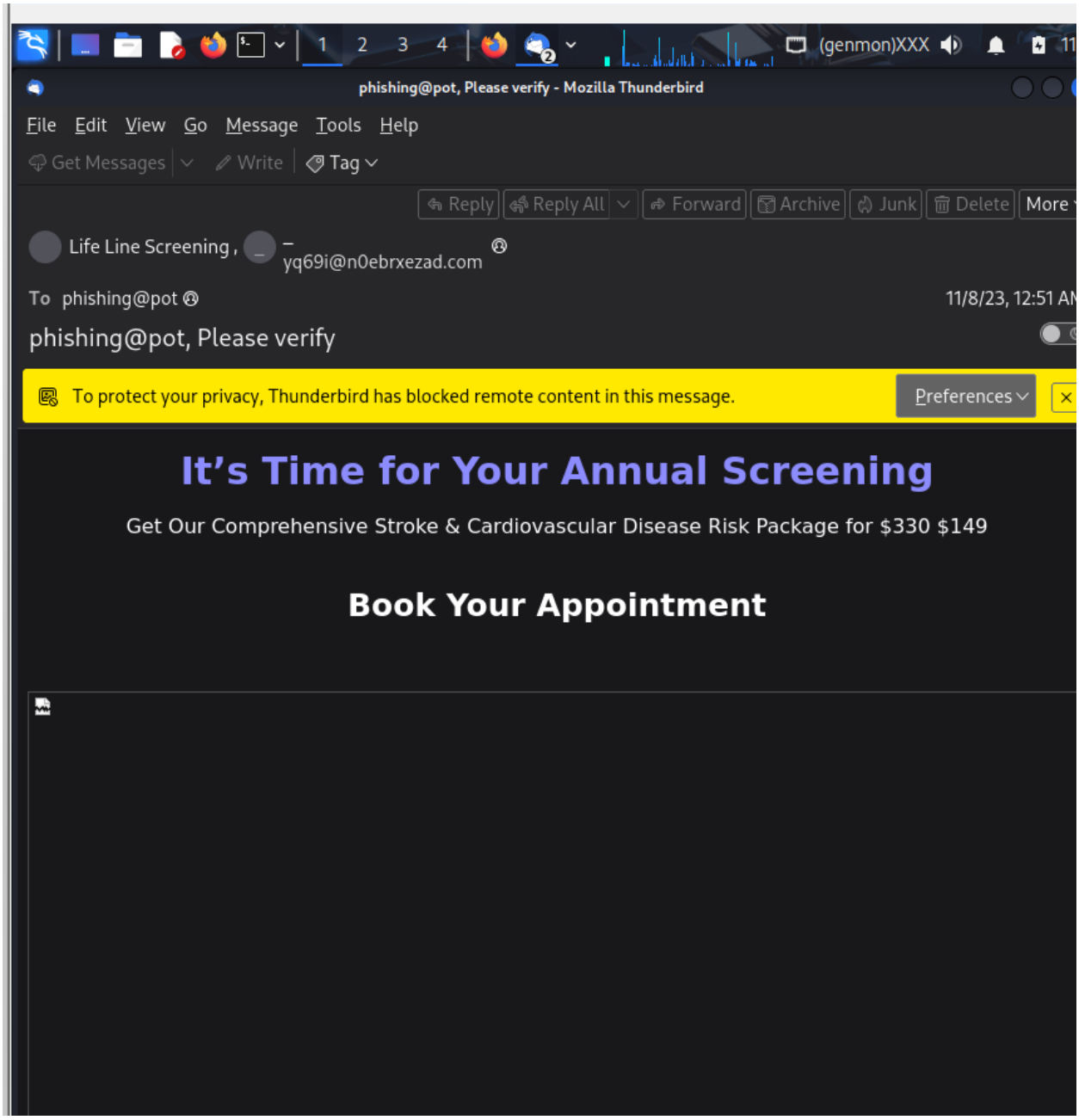
```
Summary:
  Upgrading: 0, Installing: 6, Removing: 0, Not Upgrading: 154
  Download size: 69.7 MB / 72.5 MB
  Space needed: 291 MB / 51.4 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 librnp0 amd64 0.18.1-1 [441 kB]
Get:2 http://us.mirror.ionos.com/linux/distributions/kali/kali kali-rolling/main amd64 thunderbird amd64 1:140.5.0e
sr-1 [69.3 MB]
Fetched 69.7 MB in 39s (1,768 kB/s)
Selecting previously unselected package libtspi1.
(Reading database ... 432261 files and directories currently installed.)
Preparing to unpack .../0-libtspi1_0.3.15-1_amd64.deb ...
Unpacking libtspi1 (0.3.15-1) ...
Selecting previously unselected package libbotan-3-7:amd64.
Preparing to unpack .../1-libbotan-3-7_3.7.1+dfsg-2_amd64.deb ...
Unpacking libbotan-3-7:amd64 (3.7.1+dfsg-2) ...
Selecting previously unselected package libotr5t64:amd64.
Preparing to unpack .../2-libotr5t64_4.1.1-6_amd64.deb ...
Unpacking libotr5t64:amd64 (4.1.1-6) ...
Selecting previously unselected package libsexpp0:amd64.
Preparing to unpack .../3-libsexpp0_0.8.7-4+b1_amd64.deb ...
Unpacking libsexpp0:amd64 (0.8.7-4+b1) ...
Selecting previously unselected package librnp0:amd64.
Preparing to unpack .../4-librnp0_0.18.1-1_amd64.deb ...
Unpacking librnp0:amd64 (0.18.1-1) ...
Selecting previously unselected package thunderbird.
Preparing to unpack .../5-thunderbird_1%3a140.5.0esr-1_amd64.deb ...
Unpacking thunderbird (1:140.5.0esr-1) ...
Setting up libtspi1 (0.3.15-1) ...
Setting up libbotan-3-7:amd64 (3.7.1+dfsg-2) ...
Setting up libsexpp0:amd64 (0.8.7-4+b1) ...
Setting up libotr5t64:amd64 (4.1.1-6) ...
Setting up librnp0:amd64 (0.18.1-1) ...
Setting up thunderbird (1:140.5.0esr-1) ...
Skipping profile in /etc/apparmor.d/disable: usr.bin.thunderbird
Processing triggers for kali-menu (2025.4.2) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for hicolor-icon-theme (0.18-2) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 added doc-base file...
Processing triggers for libc-bin (2.41-12) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for mailcap (3.75) ...

┌──(kali㉿kali)-[~/phishing_pot/email]
└─$
```


Minimize all open windows and show the desktop
Sie zu kontaktieren - Mozilla Thunderbird
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
Dating-Experte ,
(<service@stayfriends.de>)
To phishing@pot
8/29/24, 9:11 AM
Sophia versucht, Sie zu kontaktieren
To protect your privacy, Thunderbird has blocked remote content in this message.
Preferences
WILLST DU FRAUEN IN DEINER NÄHE TREFFEN?
Auf dieser Webseite findest du eventuell Fotos von Personen, die du kennst.
Derzeit gibt es 189 weibliche Mitglieder in deiner unmittelbaren Umgebung. Bitte halte ihre Identitäten geheim!
VERSTANDEN


~/phishing_pot/email/sample-3482.eml - Mousepad
File Edit Search View Document Help
1 Received: from EA2P223MB0834.NAMP223.PROD.OUTLOOK.COM (::1) by
2 LV3P223MB0968.NAMP223.PROD.OUTLOOK.COM with HTTPS; Mon, 22 Jul 2024
02:46:47
3 +0000
4 ARC-Seal: i=2; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=fail;
5 b=CitvRyovJj1hEYr57pQ0B+UsBDs+o9vN8wjGOAdf1ssLCj/
MkFd0QlJWObmPY5OsuLXgpQ7TFUhWc9/88lU3SzUDoKEZ9qA7KOipUG/
l7cy+oJEJPLVKzIODz+WrbKa/aGxSrVVnTOHFb4MMqt8cXC50d8GnYBx/
vDcnr4nDT5YlrlCMI0GSKEZQ4QTWuyNDAYSmOir1WbZhZSehk1iqXxU8r1PXC5F8VQ3S6vcFLX-
yjg0EpQ31B1B3UFIG2t+l13P/
UyknNrRLf7F9XiG9WUSPCzRmyvT6mwbeDaPBFczmKRoTi5CmFZPt0XeCbxO2MLEOgdAaLLo6mj-
jtyuWqCxQ==
6 ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed;
d=microsoft.com;
7 s=arcselector10001;
8 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-
AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-
Exchange-AntiSpam-MessageData-1;
9 bh=1zfQ+cK1QcMNVt3ctt1SqHtmSBqsJROZ1xmq1VaTW8Q=;
10
b=frwsjyZo4zGMsZ3dsibEf6GpHq9IfYLKOgeu1vpS4r4axHOc4DTtbzPRqeAp9GyVtguNfqwM-
lhtKav9/YelR7Ls9NZP5Q2++ASM24Ks8nuf/CSAfIG7Xngoo4×9mMK6VWM3/
otosGOZsde3N9T8dzs/Eo3B1+L5617JDC/


Protect the Ones you Love! Secure a $500,000 Policy for $1 a Day - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Tag
Reply Reply All Forward Archive Junk Delete More
Providence Life Insurance
sheffield_hussell_66022@a.c.h.h.a.d.o.a.n.a.m.e.d3.68.hawli.shop
To __LinkTINVgPgewY@aol.com
7/21/24, 10:39 PM
Cc __LinkTINVgPgewY@aol.com
Protect the Ones you Love! Secure a $500,000 Policy for $1 a Day
List-ID <8whNAsW6w.xt.local>
To protect your privacy, Thunderbird has blocked remote content in this message.
Preferences
Get a Life Insurance Policy in 10 minutes


1 2 3 4
(genmon)XXX
11:44
~/phishing_pot/email/sample-1830.eml - Mousepad
File Edit Search View Document Help
1 Received: from SN7P223MB0579.NAMP223.PROD.OUTLOOK.COM (2603:10b6:806:26d::8)
2 by LV3P223MB0968.NAMP223.PROD.OUTLOOK.COM with HTTPS; Wed, 8 Nov 2023
3 05:51:51 +0000
4 Received: from FR3P281CA0162.DEUP281.PROD.OUTLOOK.COM (2603:10a6:d10:a2::14)
5 by SN7P223MB0579.NAMP223.PROD.OUTLOOK.COM (2603:10b6:806:26d::8) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6954.25; Wed, 8 Nov
8 2023 05:51:50 +0000
9 Received: from VI1EUR03FT053.eop-EUR03.prod.protection.outlook.com
10 (2603:10a6:d10:a2:cafe::cd) by FR3P281CA0162.outlook.office365.com
11 (2603:10a6:d10:a2::14) with Microsoft SMTP Server (version=TLS1_2,
12 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.18 via Frontend
13 Transport; Wed, 8 Nov 2023 05:51:50 +0000
14 Authentication-Results: spf=none (sender IP is 89.144.44.42)
15 smtp.mailfrom=enznun.net; dkim=none (message not signed)
16 header.d=none;dmarc=none action=none header.from=n0ebrxezad.com;compauth=fail
17 reason=001
18 Received-SPF: None (protection.outlook.com: enznun.net does not designate
19 permitted sender hosts)
20 Received: from ghatflimsfeery.net (89.144.44.42) by
21 VI1EUR03FT053.mail.protection.outlook.com (100.127.144.132) with Microsoft
22 SMTP Server id 15.20.6977.18 via Frontend Transport; Wed, 8 Nov 2023 05:51:49
23 +0000
24 X-IncomingTopHeaderMarker:
25
OriginalChecksum:6A237B5326926BE91E539B792592606C0DE4441D4B815556731025C6F4161AA3;UpperCasedChecksum:A8AD1B6EC63
ABBDF437A5DF286DC0ABB6D43B5CE79DB2BB8B20AD79B66C5C079;SizeAsReceived:325;Count:11
26 From: Life Line Screening ,_<yq69i@n0ebrxezad.com>
27 Subject: phishing@pot, Please verify
28 To: phishing@pot
29 Content-Length: 27537896
30 Content-Length: 1371191
31 Date: Wed, 8 Nov 2023 05:51:49 +0000
32 Content-Type: text/html; charset="UTF-8"
33 Content-Transfer-Encoding: 8bit
34 X-IncomingHeaderCount: 11
35 Message-ID:
36 <fba04a21-24bf-4c51-8fe8-8b2cff091da8@VI1EUR03FT053.eop-EUR03.prod.protection.outlook.com>
37 Return-Path: lypmn40@enznun.net
38 X-MS-Exchange-Organization-ExpirationStartTime: 08 Nov 2023 05:51:49.9385
39 (UTC)



2.2 Email Authentication Results

- **SPF (Sender Policy Framework**): PASS o The SPF record validated successfully, suggesting that the sending server is authorized to send mail on behalf of the domain. However, SPF alone is not a reliable indicator of legitimacy.

- **DKIM (DomainKeys Identified Mail**): NONE

  No DKIM signature was present, indicating the email was not cryptographically signed. This reduces credibility and makes the email susceptible to spoofing.

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

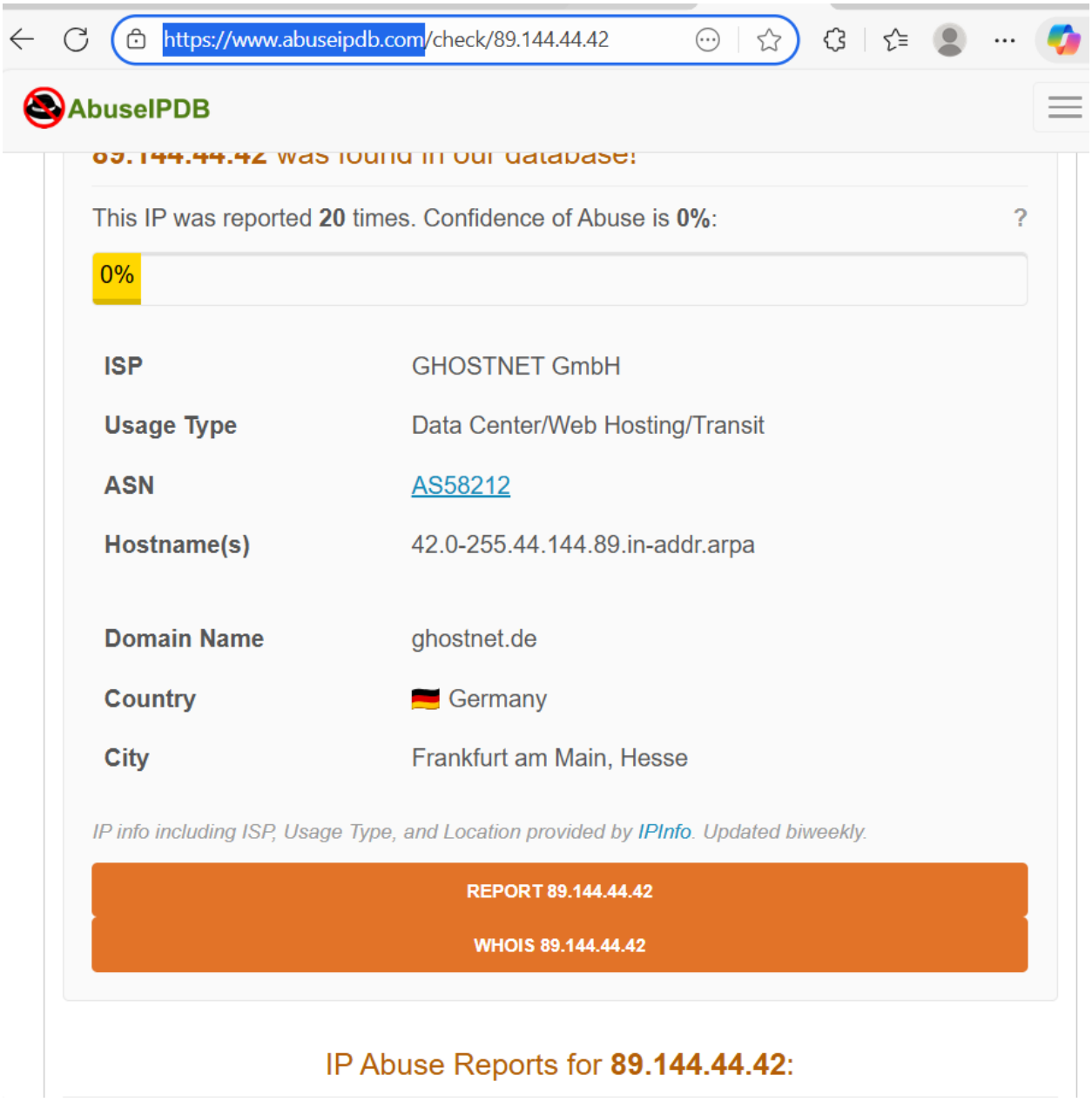
  o The domain lacks a DMARC policy, increasing the likelihood of unauthorized use and spoofing.

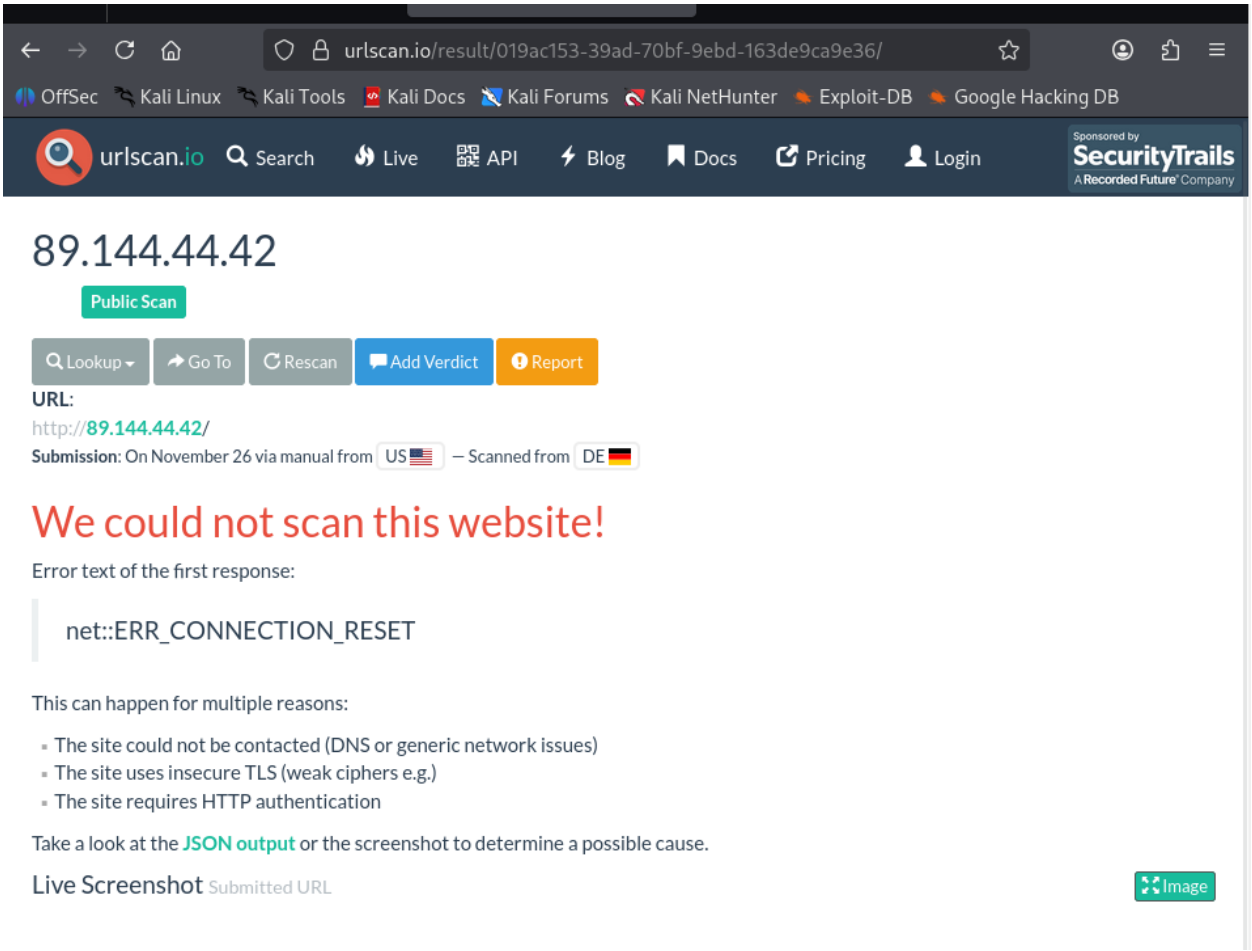
3. Embedded URL Analysis

3.1 Suspicious Link

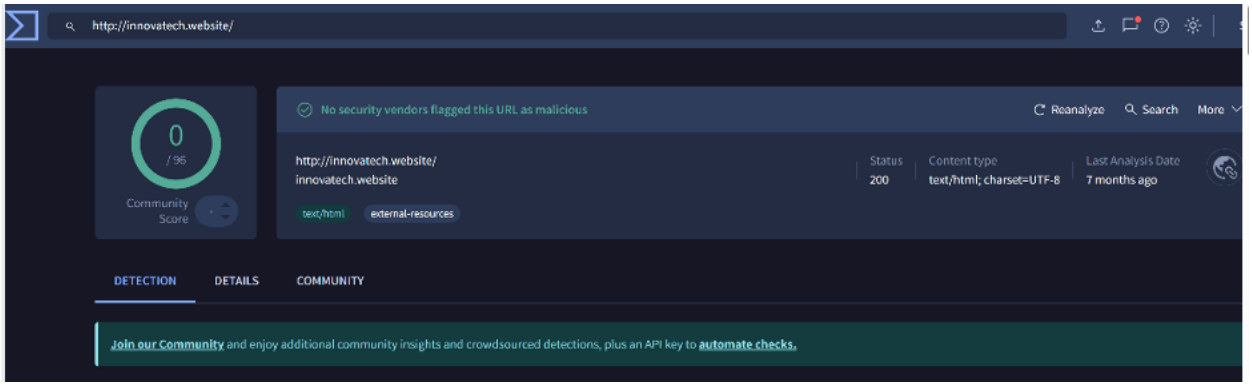
- **URL Found in Email: https://innovatech.website**

I extracted the link and performed scans using the following tools:

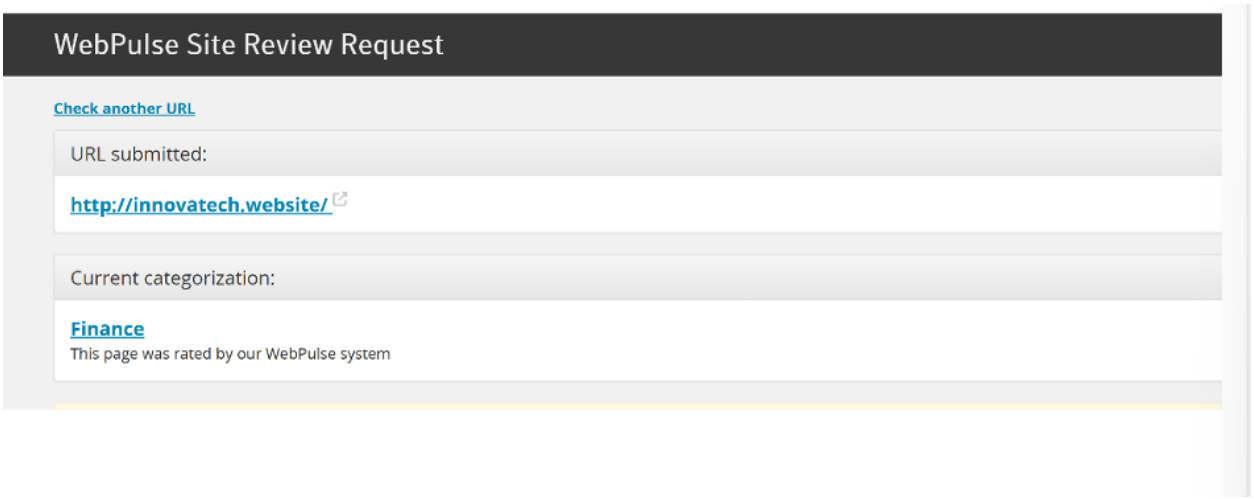




Virus Total



o Bluecoat SiteReview



3.2 Threat Intelligence on Domain

- **Domain:** innovatech.website

A WHOIS lookup revealed

Registrar:HOSTINGER operations, UAB

Registered On:2024-05-28

The domain appears to be newly registered and lacks a solid reputation,

which is consistent with common phishing infrastructure.

4. Threat Intelligence Analysis

4.1 IP Address Reputation

• IP Address: 151.80.93.107

• The IP address did not return any reports on AbuseIPDB. However, attackers often rotate IPs and domains, so absence of prior activity does not imply trustworthiness. **4.2 Indicators of Compromise (IoCs)**

4.2 Indicators of Compromise (IoCs)

• Email Header Anomalies: Missing DKIM/DMARC, mismatched Return-Path and sending server.

• Malicious URL: The URL embedded in the email links to a suspicious domain.

• Unusual Return-Path Domain: sk.globalexceltrade.xyz is a non-standard and suspicious domain name.