Phishing Email Analysis Documentation.

by Samsudeen Olapade

1. Introduction

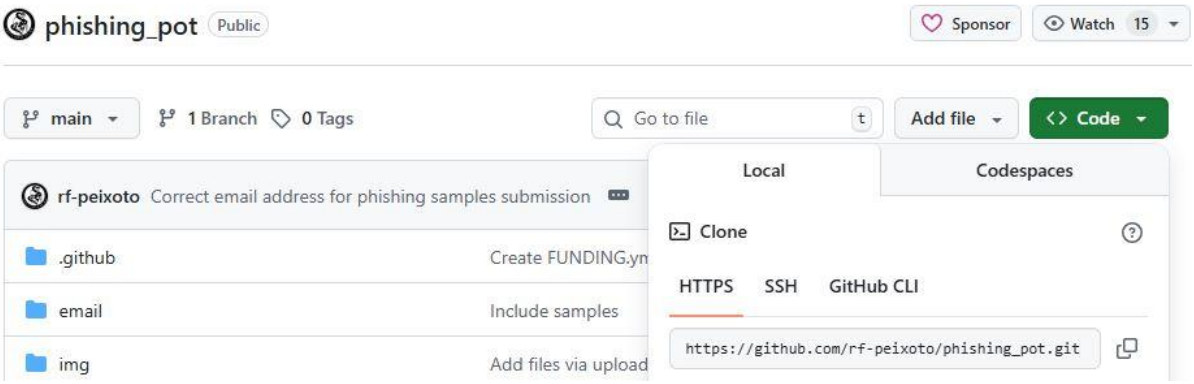
This documentation outlines the process of analysing a phishing email sample for educational and cybersecurity training purposes. The phishing email used in this report was obtained from the **phishing_pot** repository on GitHub. Phishing-pot contains publicly available phishing email samples intended solely for research, awareness, and safe analysis.

The objective of this exercise is to demonstrate how to properly investigate suspicious emails using various open-source tools and analytical techniques, including header analysis, URL analysis, IP reputation checks, and email security validation.

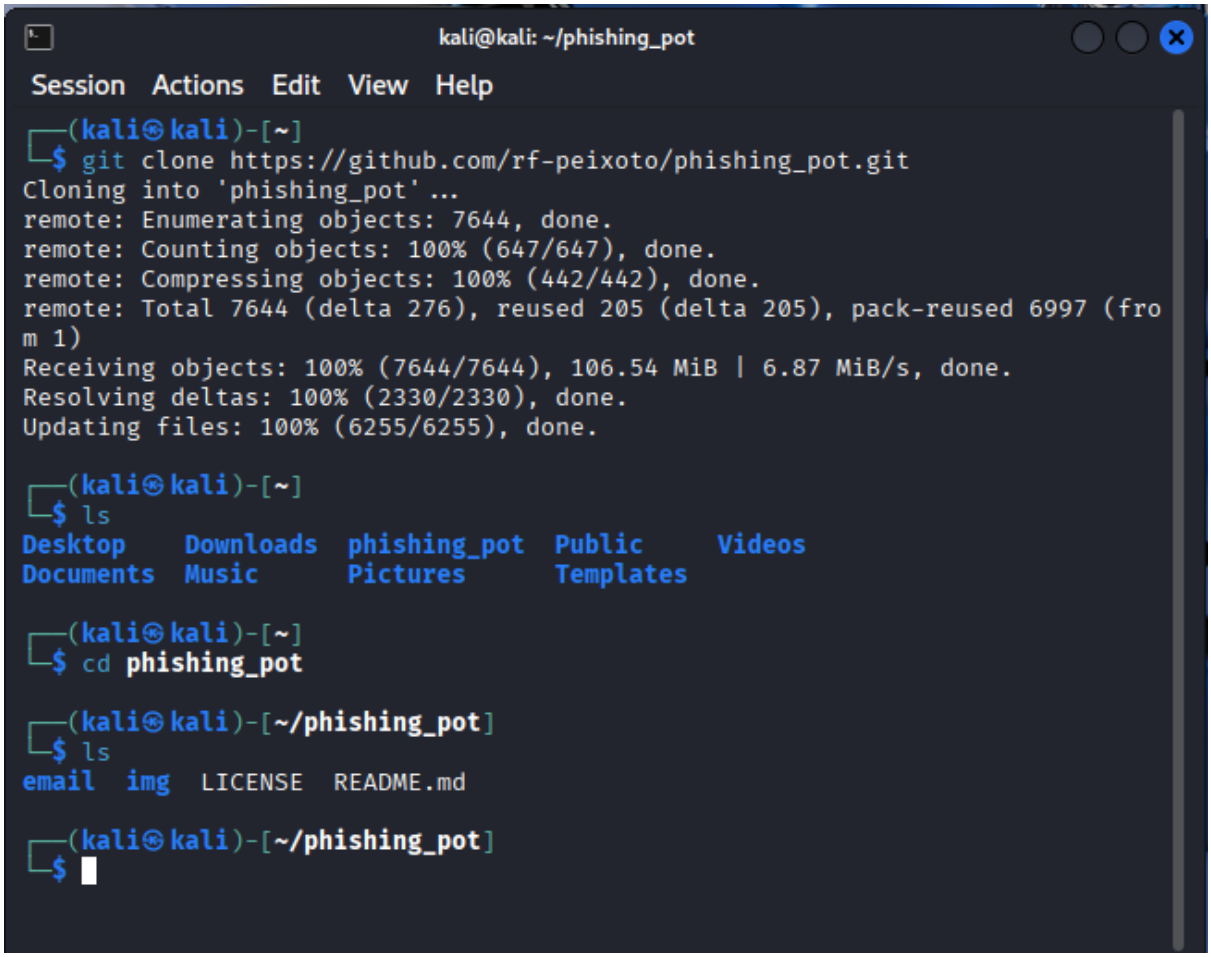
2. Environment Setup

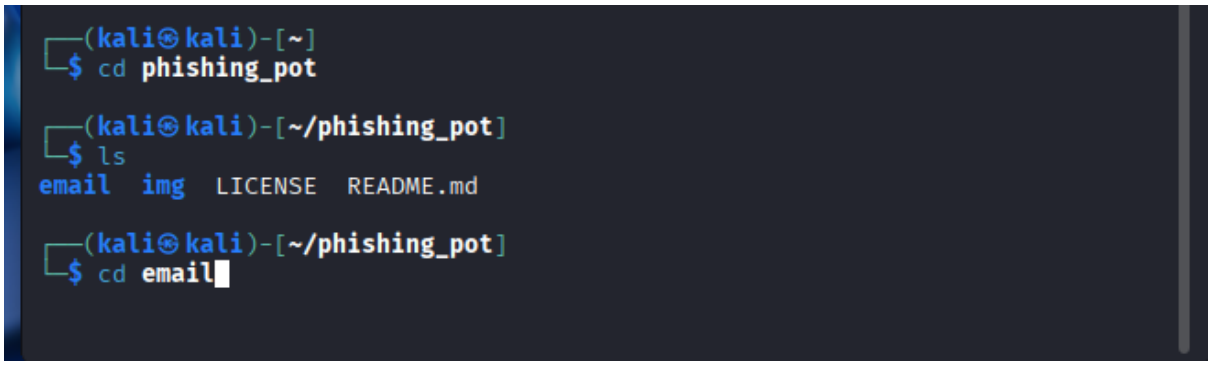
2.1 Cloning the Phishing Email Repository

1. On a Kali Linux virtual machine, the phishing_pot repository URL was copied from GitHub.



2. Using the terminal, the repository was cloned:
3. git clone < https://github.com/rf-peixoto/phishing_pot.git>
4. After cloning, the directory was opened using the command line 'ls' and selecting email by changing the directory to email and the available phishing email samples were reviewed.





2.2 Selecting an Email Sample

The phishing email samples inside the repository were inspected, and one sample email (.eml file) was selected for analysis from the list of sample email.

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

┌──(kali㉿kali)-[~/phishing_pot/email]
└─$ ls
sample-1000.eml  sample-2408.eml  sample-3815.eml  sample-5230.eml
sample-1001.eml  sample-2409.eml  sample-3816.eml  sample-5231.eml
sample-1002.eml  sample-240.eml   sample-3817.eml  sample-5232.eml
sample-1003.eml  sample-2410.eml  sample-3818.eml  sample-5233.eml
sample-1004.eml  sample-2411.eml  sample-3819.eml  sample-5234.eml
sample-1005.eml  sample-2412.eml  sample-381.eml   sample-5235.eml
sample-1006.eml  sample-2413.eml  sample-3820.eml  sample-5236.eml
sample-1007.eml  sample-2414.eml  sample-3821.eml  sample-5237.eml
sample-1008.eml  sample-2415.eml  sample-3822.eml  sample-5238.eml
sample-1009.eml  sample-2416.eml  sample-3823.eml  sample-5239.eml
sample-100.eml   sample-2417.eml  sample-3824.eml  sample-523.eml
sample-1010.eml  sample-2418.eml  sample-3825.eml  sample-5240.eml
sample-1011.eml  sample-2419.eml  sample-3826.eml  sample-5241.eml
sample-1012.eml  sample-241.eml   sample-3827.eml  sample-5242.eml
```

```
sample-2398.eml  sample-3804.eml  sample-521.eml   sample-991.eml
sample-2399.eml  sample-3805.eml  sample-5220.eml  sample-992.eml
sample-239.eml   sample-3806.eml  sample-5221.eml  sample-993.eml
sample-23.eml    sample-3807.eml  sample-5222.eml  sample-994.eml
sample-2400.eml  sample-3808.eml  sample-5223.eml  sample-995.eml
sample-2401.eml  sample-3809.eml  sample-5224.eml  sample-996.eml
sample-2402.eml  sample-380.eml   sample-5225.eml  sample-997.eml
sample-2403.eml  sample-3810.eml  sample-5226.eml  sample-998.eml
sample-2404.eml  sample-3811.eml  sample-5227.eml  sample-999.eml
sample-2405.eml  sample-3812.eml  sample-5228.eml  sample-99.eml
sample-2406.eml  sample-3813.eml  sample-5229.eml  sample-9.eml
sample-2407.eml  sample-3814.eml  sample-522.eml

┌──(kali㉿kali)-[~/phishing_pot/email]
└─$ mousepad sample-265.eml
```

---

3. Preparing the Email for Analysis

3.1 Opening the Email File

1. The selected email sample was opened using **Mousepad** text editor on the Kali machine:
2. mousepad sample_email.eml
3. The email file was also downloaded to the sandbox environment within the virtual machine for safe inspection.

```
┌──(kali㉿kali)-[~/phishing_pot/email]
└─$ mousepad sample-3501.eml

(mousepad:76823): Gtk-WARNING **: 09:17:43.013: Negative content width -13 (a
llocation 1, extents 7×7) while allocating gadget (node button, owner GtkTogg
leButton)

(mousepad:76823): Gtk-WARNING **: 09:17:43.016: Negative content height -5 (a
llocation 1, extents 3×3) while allocating gadget (node button, owner GtkTogg
leButton)
```

3.2 Observations

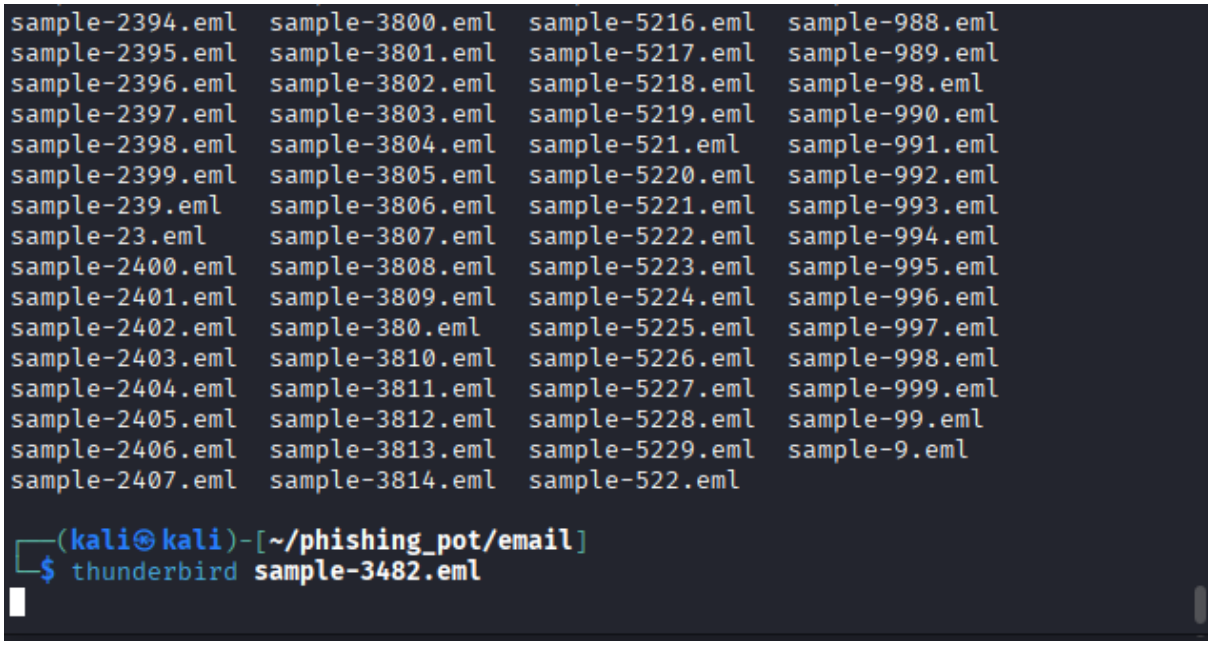
Mousepad allows viewing:

- Email headers
- Email body
- Embedded URLs
- Encoded or suspicious content

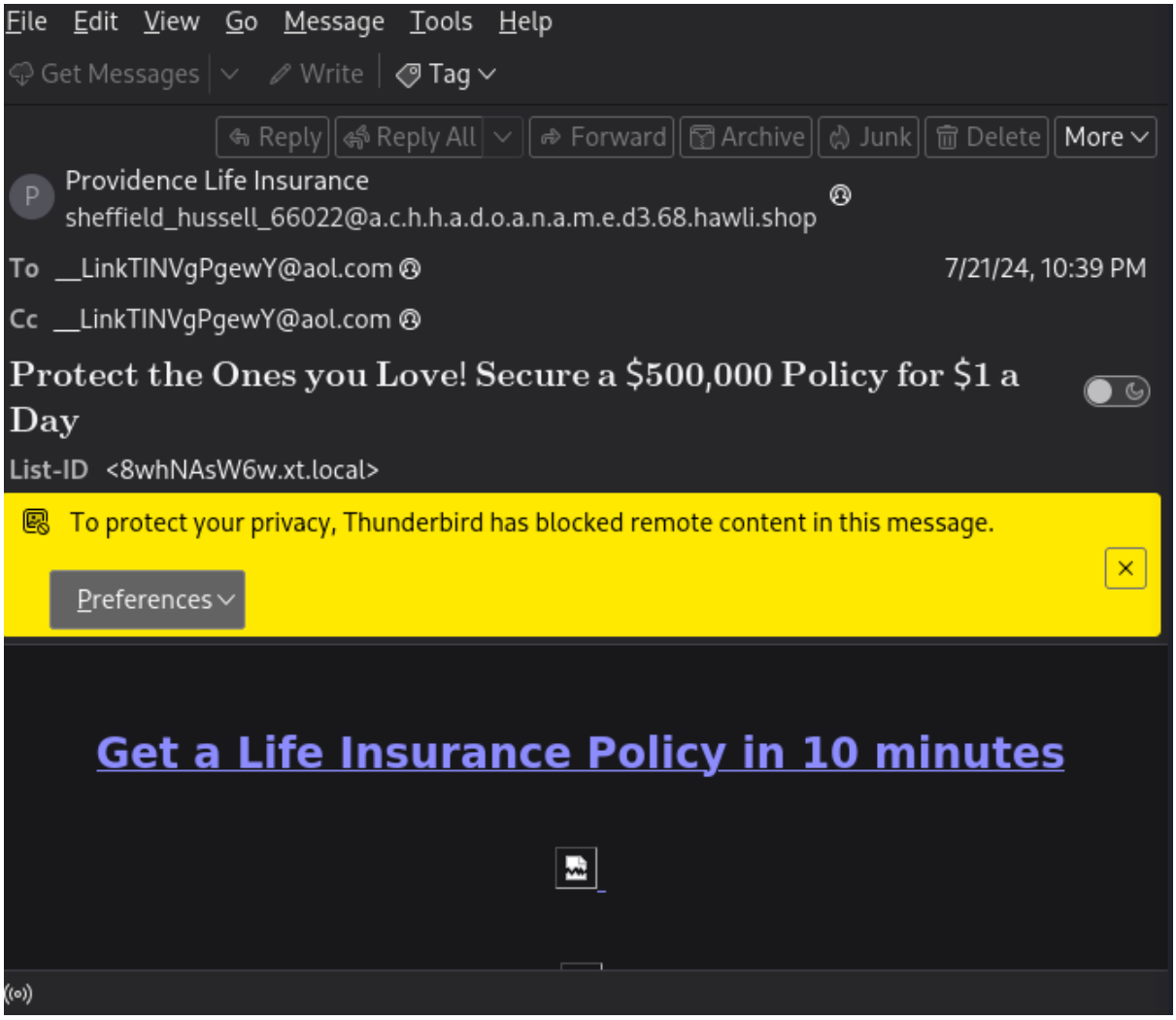
```
 8  2023 05:51:50 +0000
 9 Received: from VI1EUR03FT053.eop-EUR03.prod.protection.outlook.com
10  (2603:10a6:d10:a2:cafe::cd) by FR3P281CA0162.outlook.office365.com
11  (2603:10a6:d10:a2::14) with Microsoft SMTP Server (version=TLS1_2,
12  cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.18 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:
```

3.3 Opening the Email File

1. The selected email sample was opened using **Thunderbird** text editor on the Kali machine:
2. thunderbird sample_email.eml
3. The email file was opened on a browser tab



4. Mail was displayed



4. Phishing Email Analysis Process

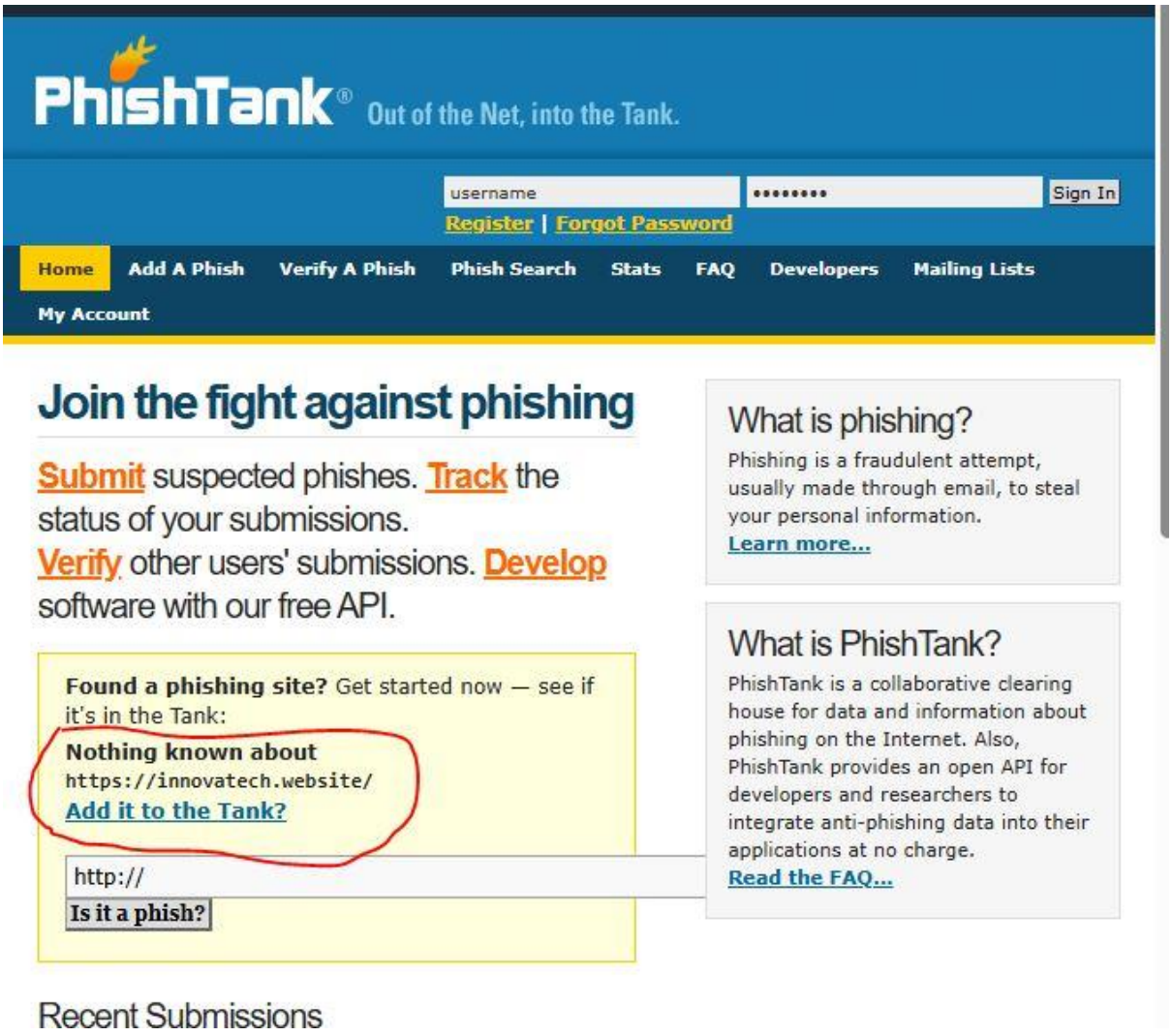
4.1 URL Analysis

All URLs contained within the email body were extracted and analysed using the following tools:

a. Phishtank

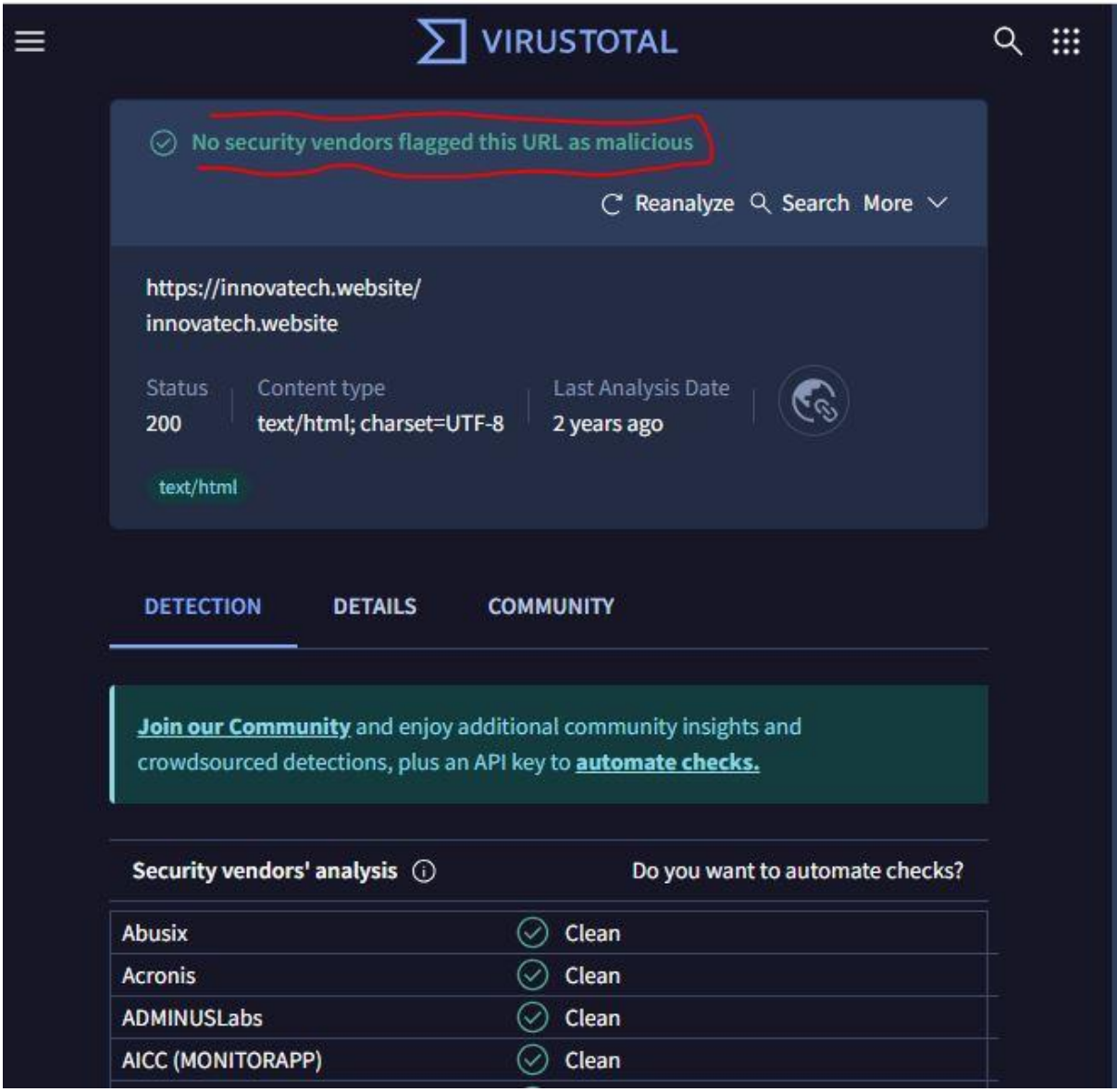
- Used to inspect the URL's:
    - Final destination
    - Redirects
    - Associated domains
    - Screenshot and behaviour

- Helps detect malicious or phishing activity.



b. VirusTotal

- The URL was submitted to VirusTotal for multi-engine scanning.
- Analysis included:
    - Malware detection
    - Phishing flags
    - Domain reputation
    - Presence on blocklists



Indicators of Malicious Activity May Include:

- Recently created domains
- Domains registered with privacy protection
- Detected phishing or malware signatures
- IP address associated with known abuse activities

4.2 Email Header Analysis

The email header was examined carefully to identify anomalies.

Key Sections Analysed:

a. SPF Record

- SPF (Sender Policy Framework) helps verify whether the sender is authorised to send emails from the domain.
- If SPF = **none**, **fail**, or **disabled**, this can be a strong sign of spoofing.

```
13  Transport; Wed, 17 Jul 2024 19:40:19 +0000
14 Authentication-Results: spf=pass (sender IP is 151.80.93.107)
15  smtp.mailfrom=sk.globalexceltrade.xyz; dkim=none (message not signed)
16  header.d=none;dmarc=none action=none header.from=;
```

b. Return-Path Address

- The **Return-Path** should match the **From** address.
- A mismatch indicates spoofing or domain impersonation.

```
19  receiver=protection.outlook.com; client-ip=151.80.93.107;
20  helo=sk.globalexceltrade.xyz; pr=C
21 Received: from sk.globalexceltrade.xyz (151.80.93.107) by
22  CO1PEPF000042A8.mail.protection.outlook.com (10.167.243.37) with
   Microsoft
```

```
31 From: =?UTF-8?B?RGVCYW5r?= <>
32 Content-type: multipart/mixed; boundary="--tn3FdD492a"
33 Message-Id: <20240717193809.3F51D64514@sk.globalexceltrade.xyz>
34 Date: Wed, 17 Jul 2024 15:38:09 -0400 (EDT)
35 X-IncomingHeaderCount: 8
36 Return-Path: apache@sk.globalexceltrade.xyz
37 X-MS-Exchange-Organization-ExpirationStartTime: 17 Jul 2024 19:40:18.9934
38  (UTC)
39 X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
```

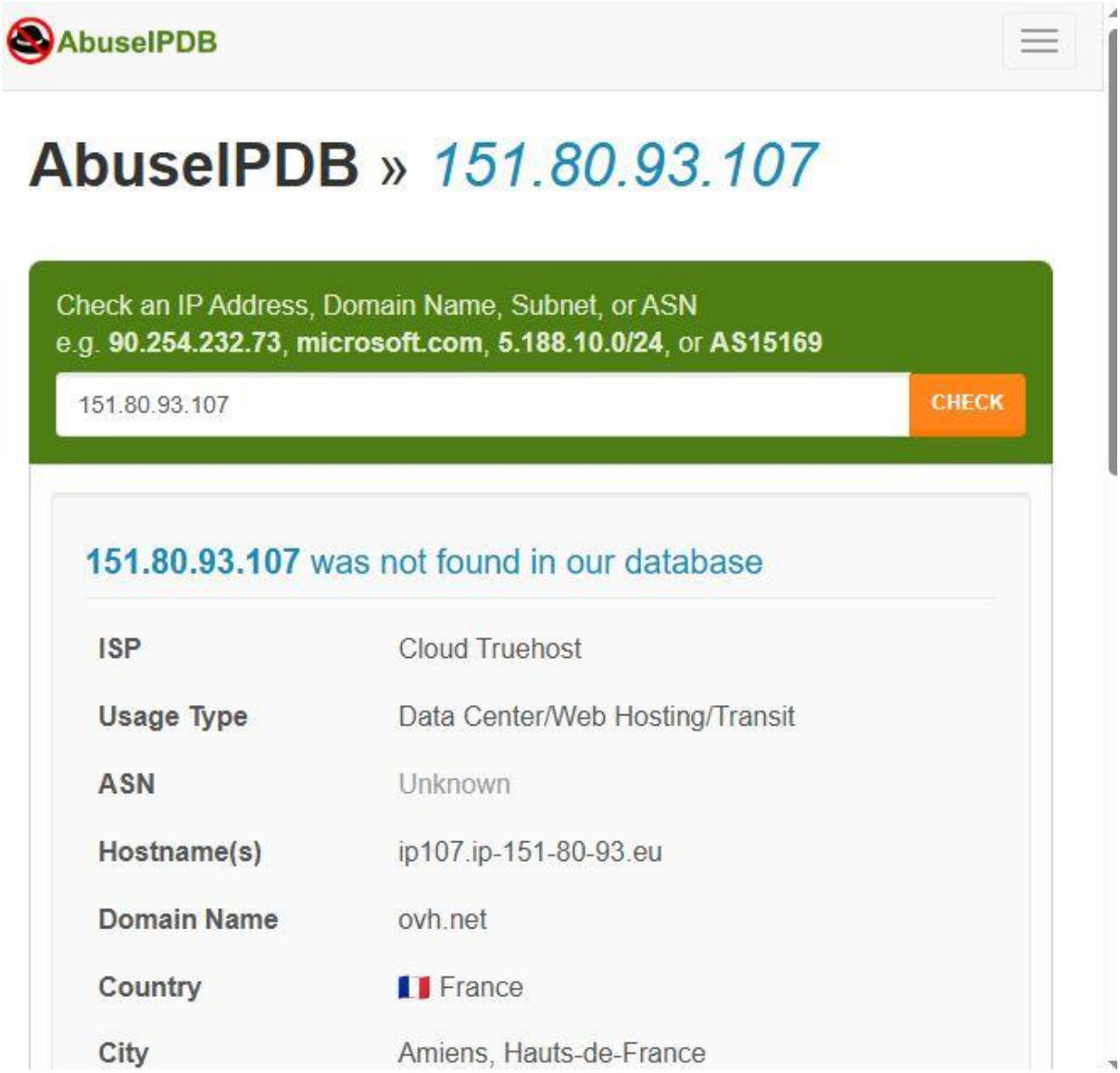
c. From Address vs. Reply-To Address

- If the sender claims to be a known organisation but the reply-to address points to an unrelated or suspicious domain, this is a phishing indicator.

d. Sending IP Address

- Extracted from the header (Received lines).
- The IP address was checked on **AbuseIPDB** to determine whether it had:
    - A history of malicious activity
    - Spam reports
    - Botnet association

If the IP had multiple reports or a high abuse score, this further indicates malicious intent.



4.3 Additional Security Tools Used

Bitdefender Email Filtering Tools

Bitdefender's scanning and filtering tools were used to:

- Detect embedded malicious links
- Identify phishing behaviour
- Check for known malware attachments
- Validate the email structure

---

5. Indicators of Compromise (IOCs) Identified

Based on the analysis, IOCs may include:

- Suspicious or mismatched email addresses
- Spoofed sender domain
- Failing SPF authenticity checks
- Malicious or suspicious URLs
- Abusive IP address in the email header
- Phishing signatures detected by security engines

---

6. Conclusion

The phishing email sample obtained from the phishing_pot GitHub repository demonstrated several red flags commonly associated with phishing attacks. Through careful analysis using tools such as Mousepad, URLscan.io, VirusTotal, AbuseIPDB, and Bitdefender filtering, potential malicious indicators were identified.

This structured approach helps cybersecurity analysts understand how phishing campaigns are crafted and equips them with hands-on skills for detecting and reporting phishing attempts in real environments.