Phishing Email Analysis Report

Prepared By: Dennis Gilbert

Date: April 10, 2025

Table Of Content

Executive Summary

This report summarizes the analysis of phishing emails to identify common tactics and assess threat levels. URLs were examined using tools like Symantec Bluecoat, URLScan.io, and VirusTotal, to detect malicious links. Email headers were analyzed for anomalies, including weak or missing SPF records, mismatched return and "From" addresses, and suspicious sender IPs checked via AbuseIPDB.

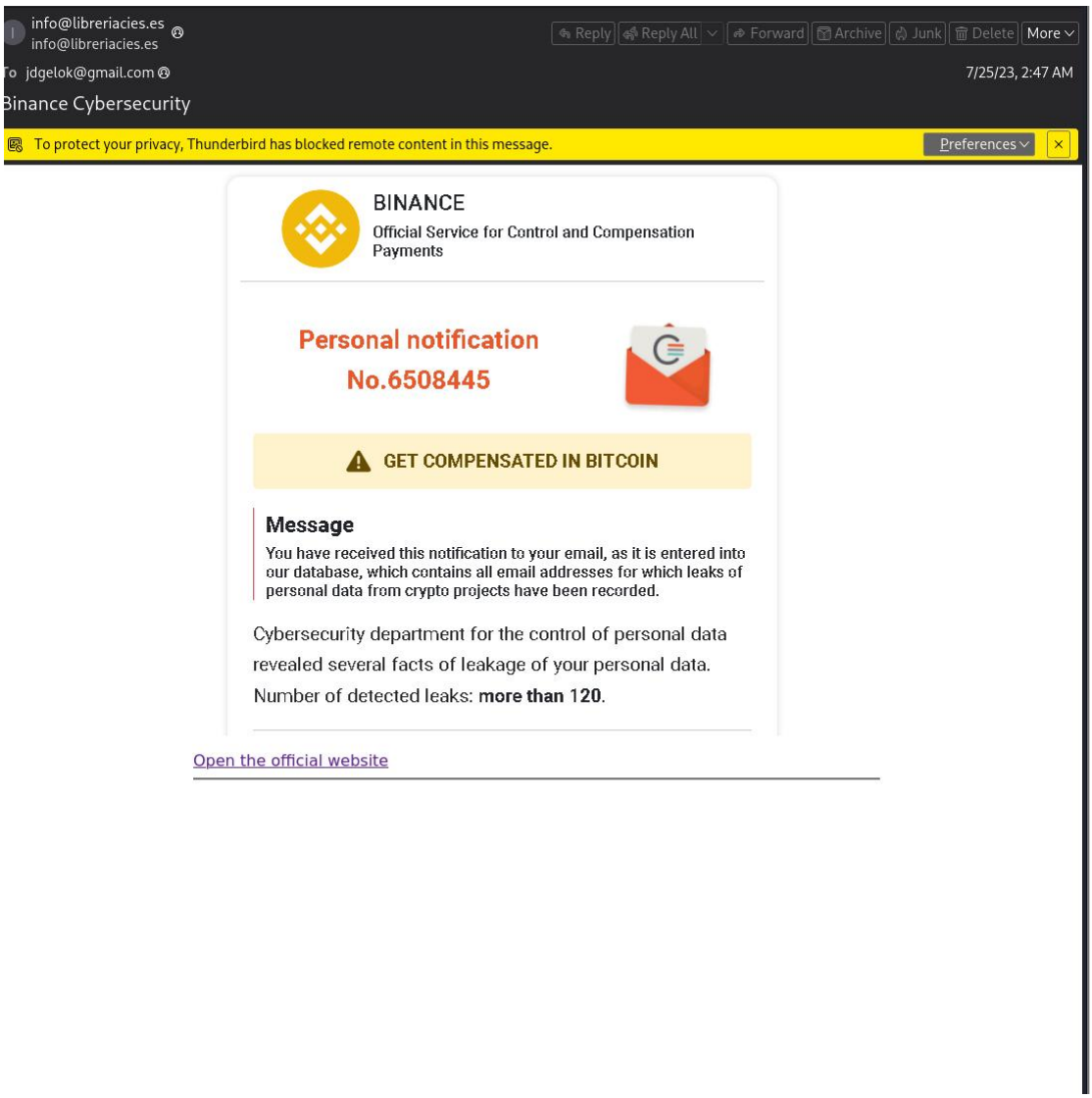
The findings highlight key indicators of phishing and reinforce the importance of thorough email analysis and security awareness.

Tools Used

- **Symantec Bluecoat** – for checking domain categorization and reputation.
- **URLScan.io** – to visualize how the link behaves when accessed.
- **VirusTotal** – for scanning the URL across multiple antivirus engines.
- **AbuseIPDB** – to check sender IP reputation.
- **SPF Record Lookup Tools** – to check domain authentication.

Email

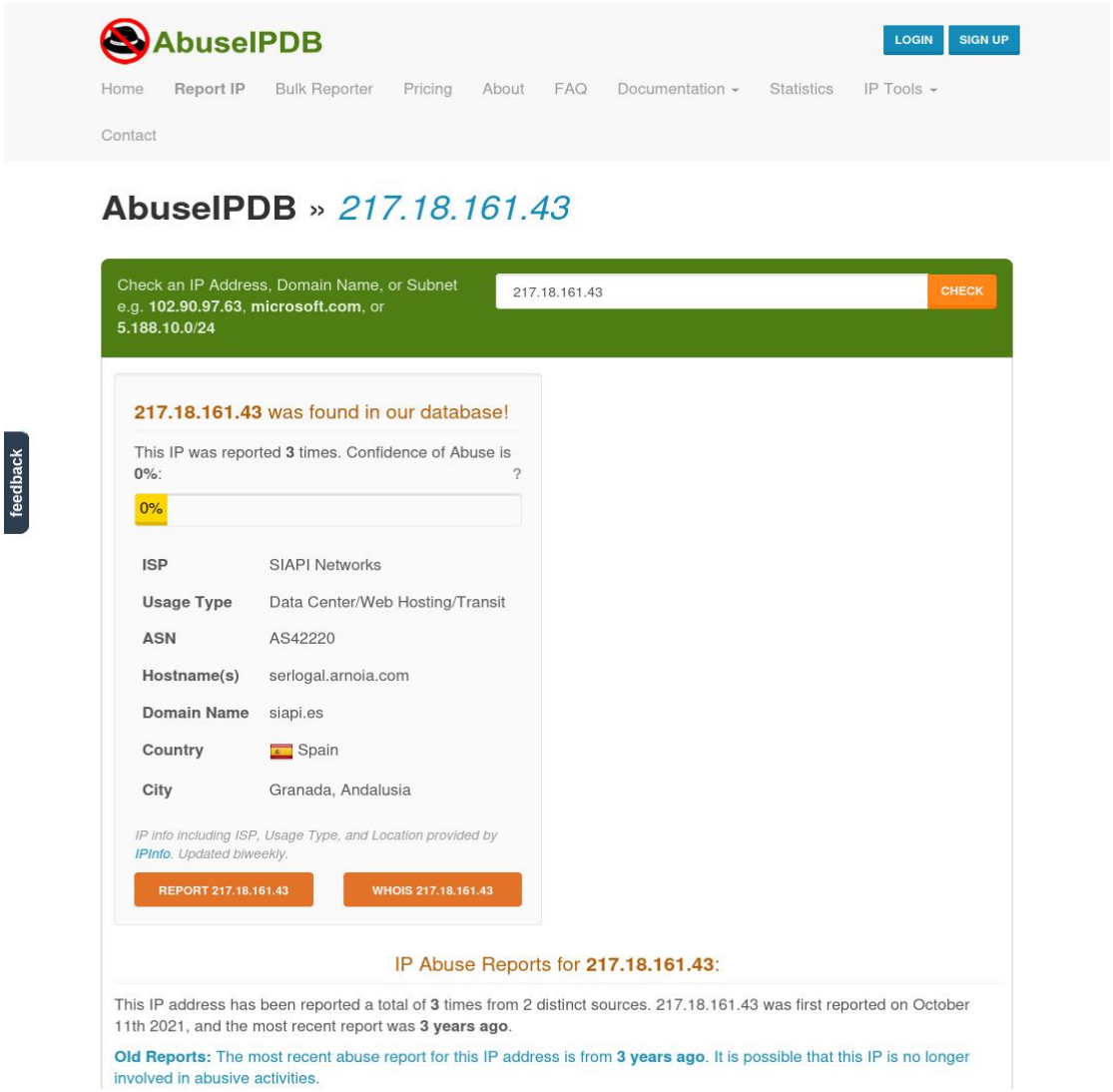
This is the email that will be analyzed



Email Metadata Analysis

Sender Information:

- Return Path Vs From: The Return Path is info@libreriacies.es while it was from PH0PR19MB5396.namprd19.prod.outlook.com(::1). This indicates spoofing.
- SPF Record: Set to “none” which means no authentication is present.
- Sender IP Address: 217.18.161.43. From the scan on AbuseIPDB, it shows that the sender’s IP address has been reported a total of 3 times from 2 distinct sources. It was reported under the following categories; Brute-Force, Phishing and Email Spam.



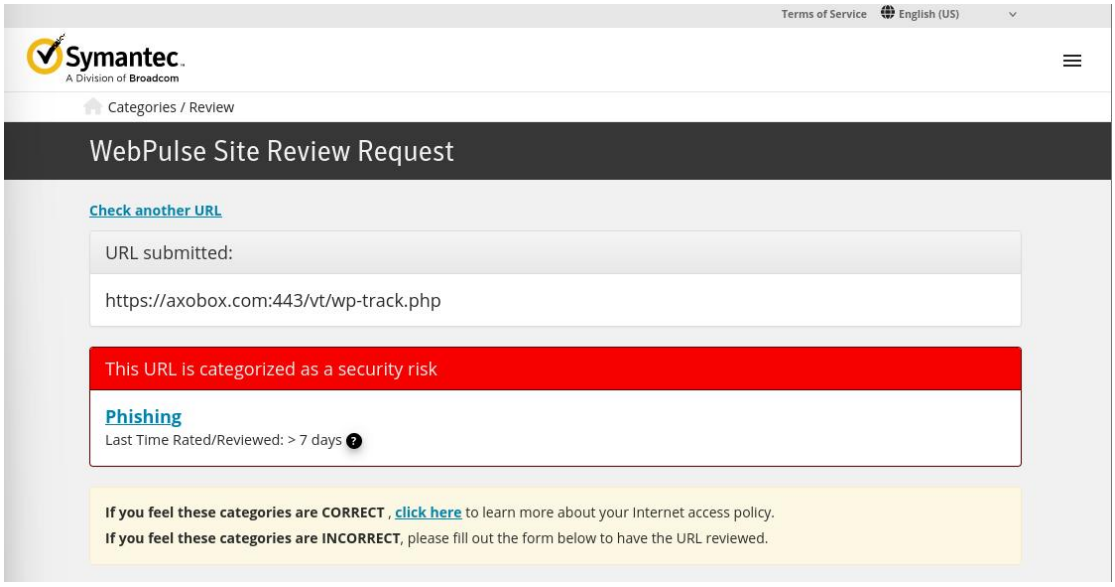
- DKIM / DMARC: Not configured and ineffective

Conclusion: The email header shows multiple signs of spoofing and poor sender domain security.

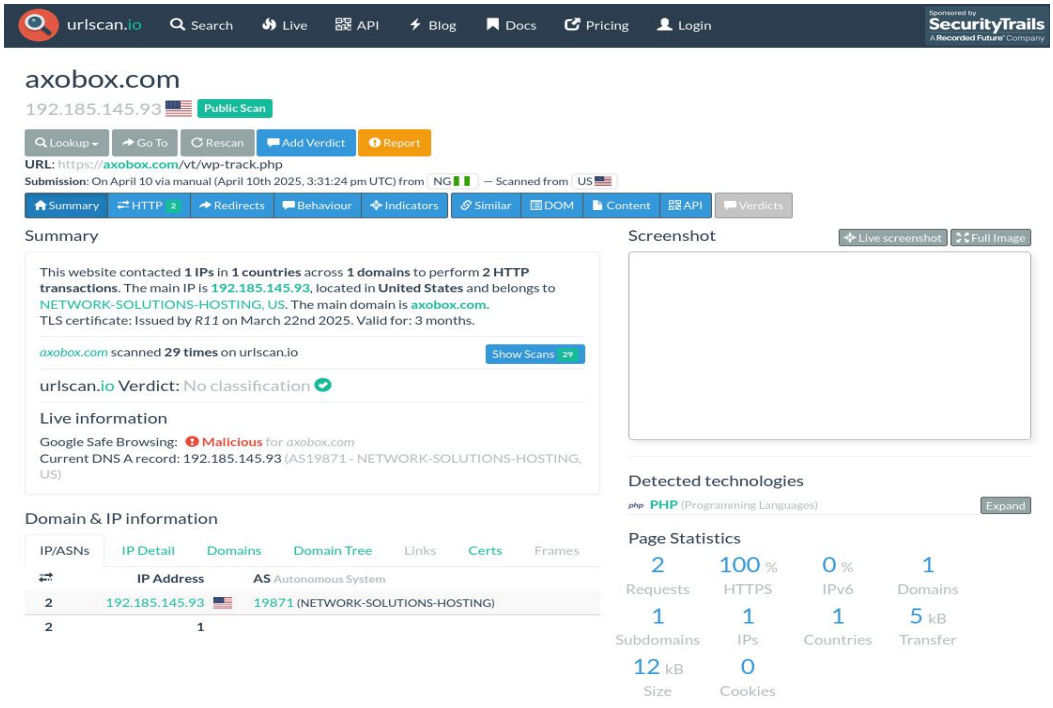
URL Analysis

The embedded URL which is : https://axobox.com/vt/wp-track.php was tested using the tools listed above .

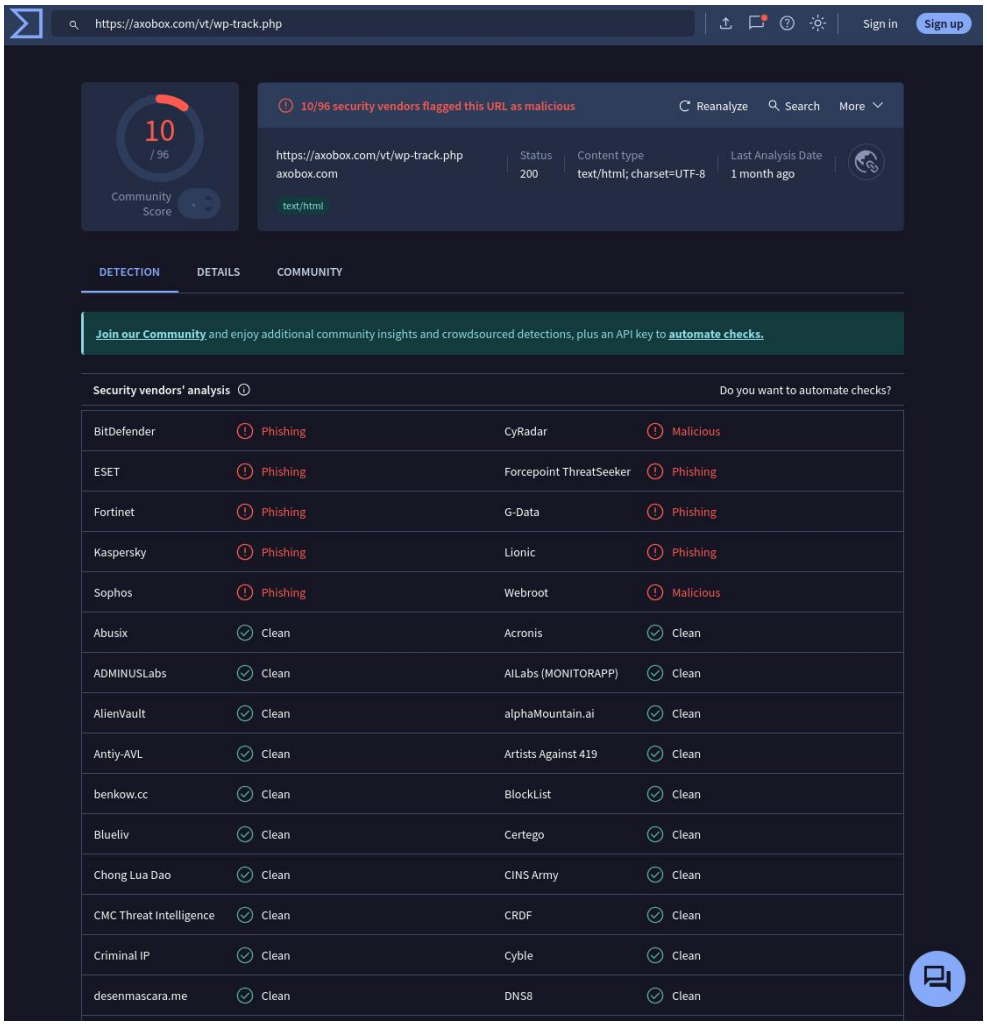
Symantec Bluecoat: This tool classified the URL as a security risk under “Phishing” category.



URLScan.io: It was classified as Malicious by Google Safe Browsing but was not given any classification by URLScan.io.



VirusTotal: 10 out of 96 security vendors flagged it as malicious.



Conclusion: The URL was clearly malicious and designed to harvest user information.

Key Indicators of Phishing

- Urgent language promting immediate response
- Email came from an unverified source pretending to be a legitimate organization.
- Technical indicators (SPF, IP, Return Path) failed verification.

Recommendations

- Always verify URLs before clicking, especially those prompting login or sensitive actions.
- Enable SPF, DKIM, and DMARC on organizational domains.
- Train users to recognize phishing tactics and report suspicious emails.
- Implement IP reputation checks and enhanced spam filtering.

Conclusion

The analyzed email demonstrated common phishing characteristics, including domain spoofing, malicious links, and deceptive sender metadata. With the help of security tools, this email was identified as a phishing attempt, underlining the need for continued vigilance and proper email authentication practice.