PREPARED BY: MUHAMMAD ABDUL REHMAN KHAN

What is an Email?

Email or Electronic Mail is a system for sending and receiving messages electronically over the internet. It allows individuals and organizations to communicate quickly and efficiently, sending messages that may include text, files, images, and other media. Email has become a fundamental tool in personal and professional communication.

What is Spam & Phishing Email?

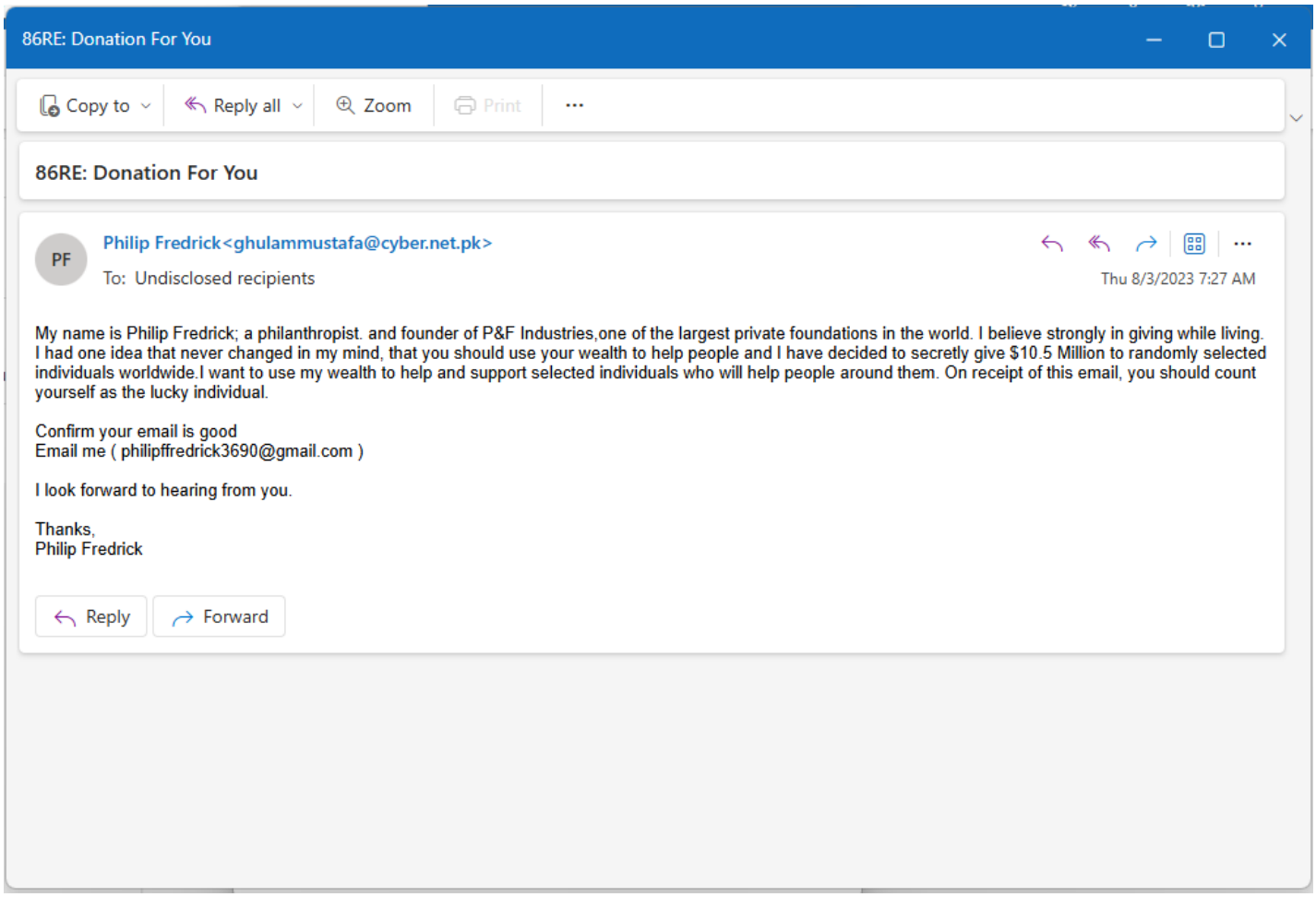
Spam refers to unwanted, bulk emails usually sent for advertising, while phishing is a more harmful type of scam where attackers impersonate legitimate entities to steal sensitive information like passwords or credit card details. While spam clutters inboxes, phishing poses a serious security risk by deceiving users into revealing personal data.

How to Detect Spam or Phishing Email?

1. Email as Received in Mailbox

This screenshot showcases the email as it appears in the recipient's inbox. Key details include:

- The sender appears to be offering a $10.5 million donation.
- The email subject and preview use generic and vague language, which is a hallmark of phishing campaigns.

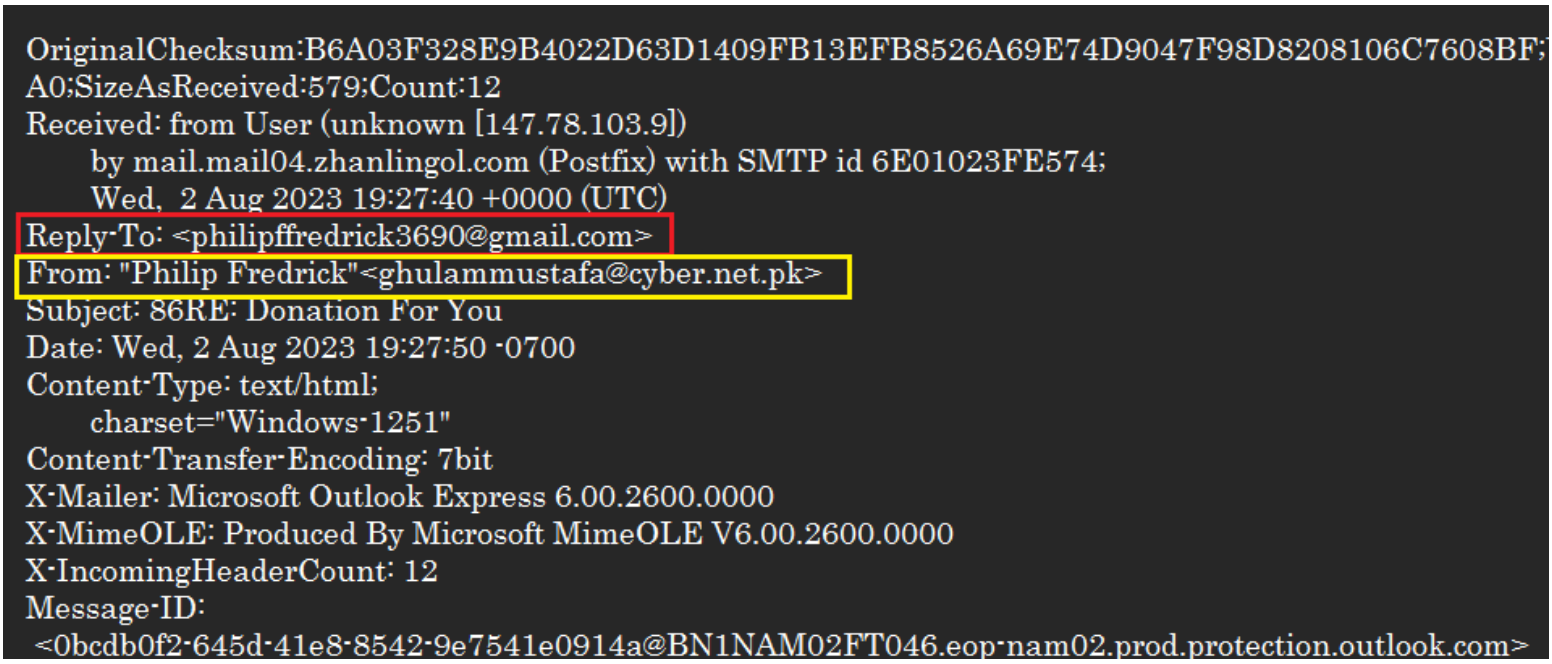


2. Raw Email Headers Highlighting Sender Discrepancies

Key discrepancies highlighted:

- **From Address (Yellow Box):** *ghulammustafa@cyber.net.pk* – Attempts to impersonate a legitimate organization.
- **Reply-To Address (Red Box):** *philipffredrick3690@gmail.com* – A free email address, unassociated with the sender's domain.

This mismatch is indicative of spoofing or an attempt to redirect replies to a phishing inbox.



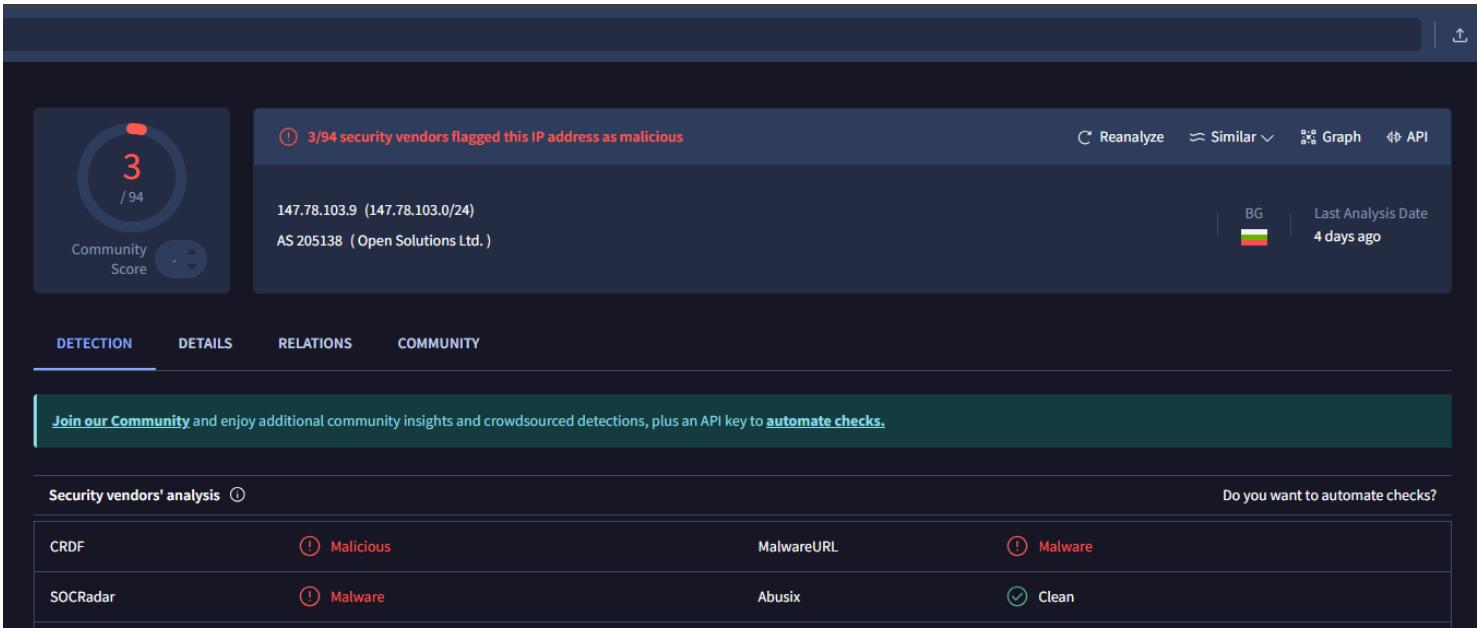
3. Received Header Highlighting Originating IP (147.78.103.9)

- **Marked in Red:** The originating IP address 147.78.103.9 is unrelated to the claimed sender domain cyber.net.pk. This suggests that the email originated from a potentially compromised or malicious server.

```
OriginalChecksum:B6A03F328E9B4022D63D1409FB13EFB8526A69E74D9047F98D8208106C7608BF;
A0;SizeAsReceived:579;Count:12
Received: from User (unknown [147.78.103.9])
      by mail.mail04.zhanlingol.com (Postfix) with SMTP id 6E01023FE574;
      Wed,  2 Aug 2023 19:27:40 +0000 (UTC)
Reply-To: <philipffredrick3690@gmail.com>
From: "Philip Fredrick"<ghulammustafa@cyber.net.pk>
Subject: 86RE: Donation For You
Date: Wed, 2 Aug 2023 19:27:50 -0700
Content-Type: text/html;
      charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-IncomingHeaderCount: 12
Message-ID:
 <0bcdb0f2-645d-41e8-8542-9e7541e0914a@BN1NAM02FT046.eop-nam02.prod.protection.outlook.com>
```

4. Virus Total Analysis for IP (147.78.103.9)

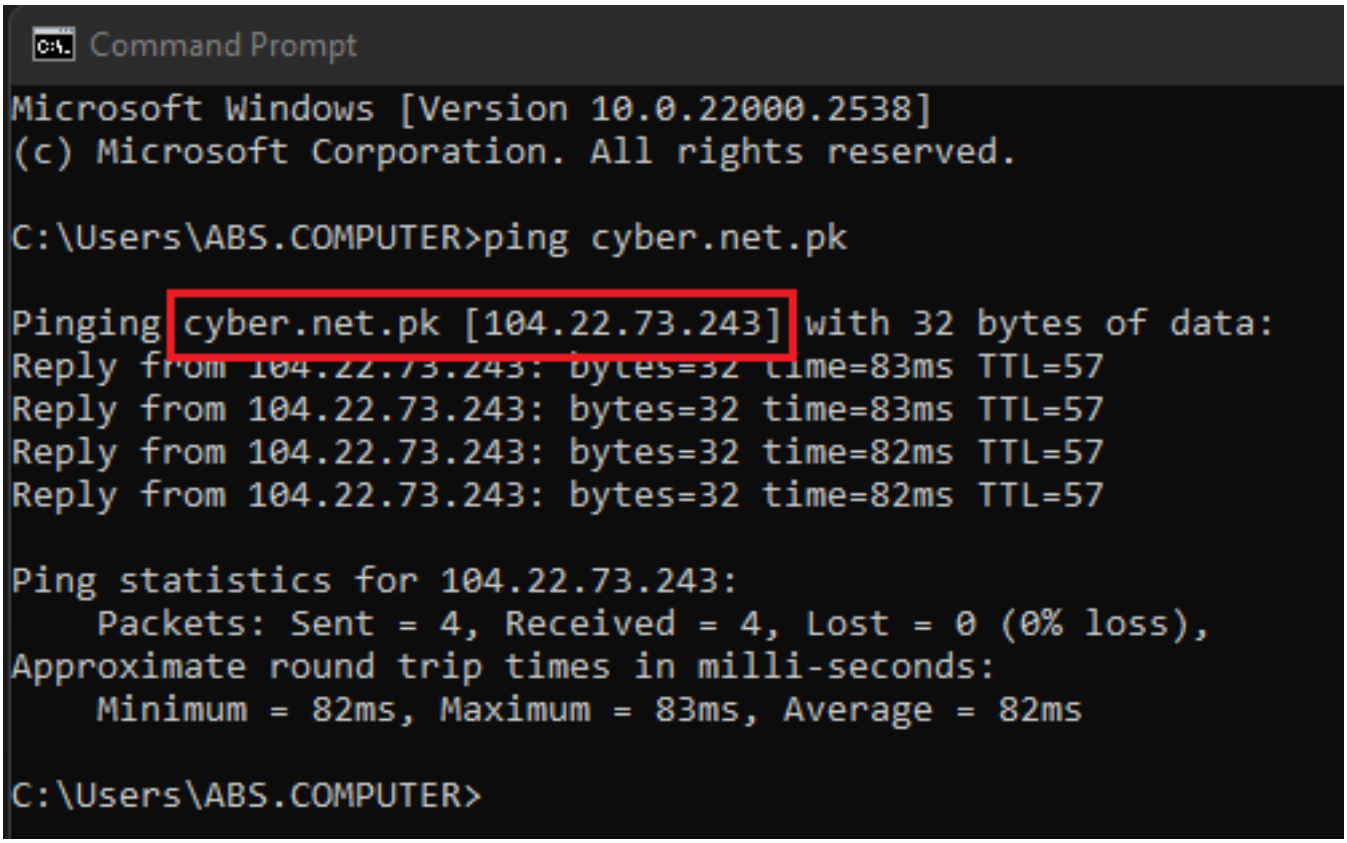
- **Result:** The IP is flagged as **malicious**.
- **Location:** Origin traced to **Bulgaria**.
- **Reputation Score:** A low score of 3 confirms its association with malicious activity.



5. Pinging the Domain (cyber.net.pk)

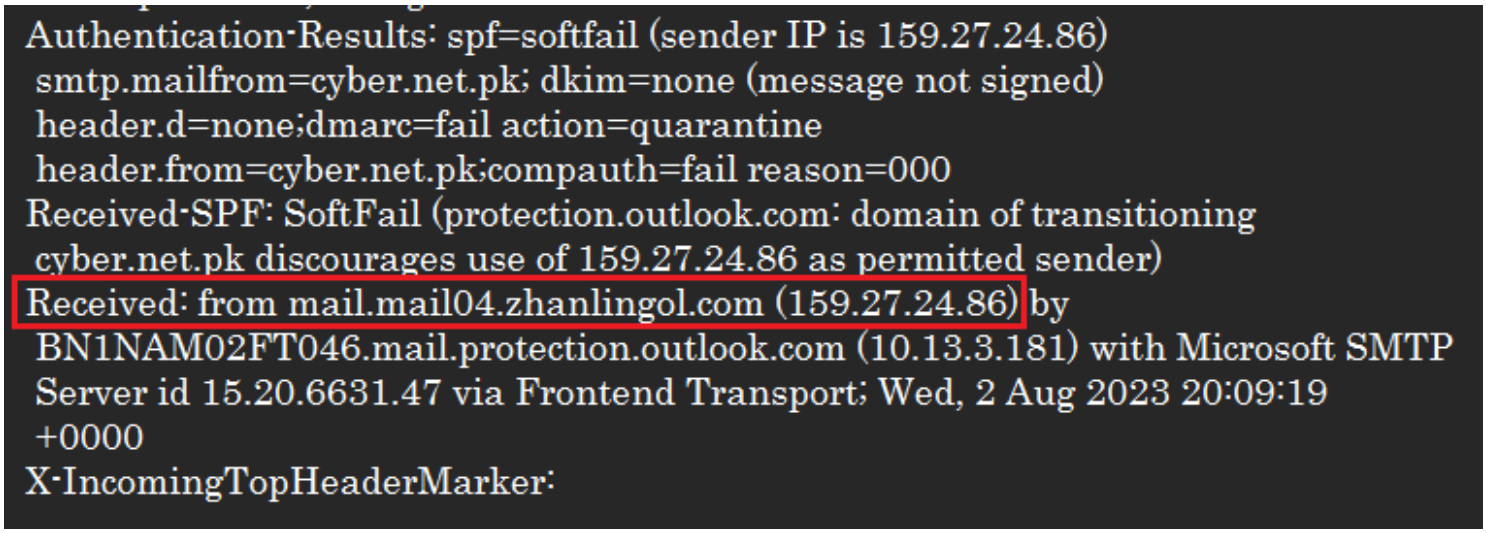
The legitimate domain cyber.net.pk was pinged to verify its actual IP.

- **Marked in Red:** The resolved IP does not match the originating IPs in the email headers, further confirming the email did not originate from the claimed sender.



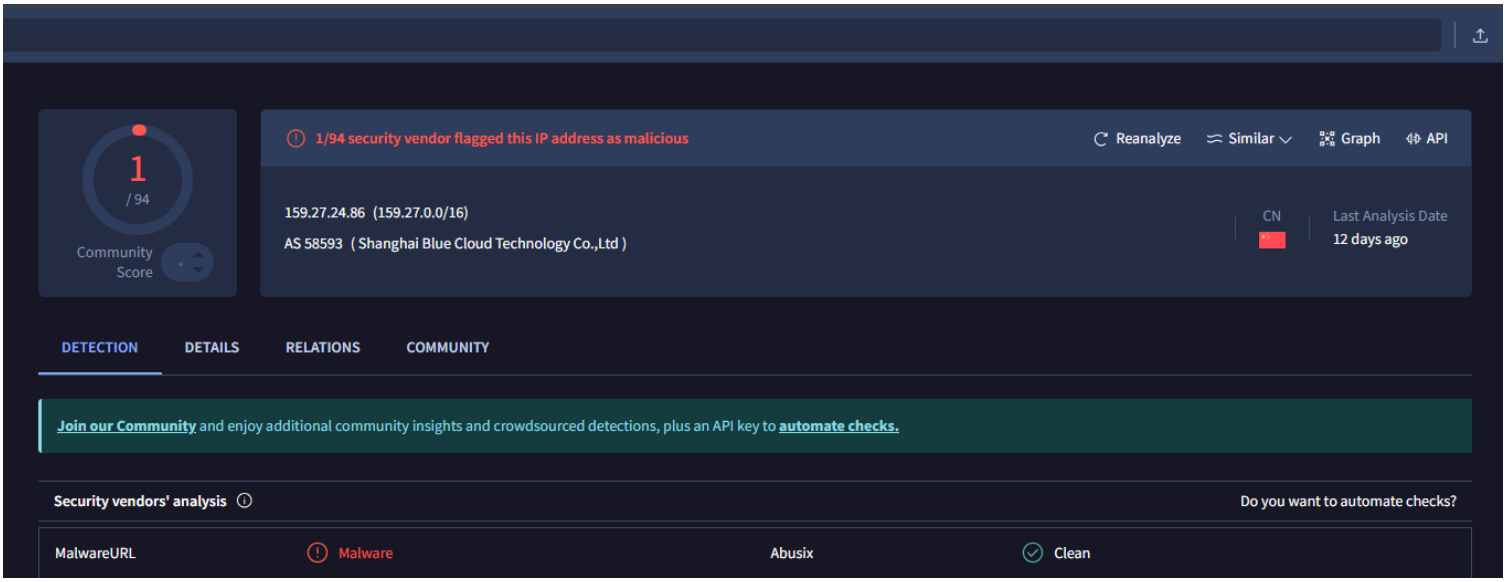
6. Raw Email Headers Highlighting Suspicious Server (mail.mail04.zhanlingol.com)

- **Marked in Red:** The mail server (mail.mail04.zhanlingol.com) with IP (159.27.24.86) is unrelated to the domain cyber.net.pk. This strongly suggests the use of a malicious intermediary to send the email.



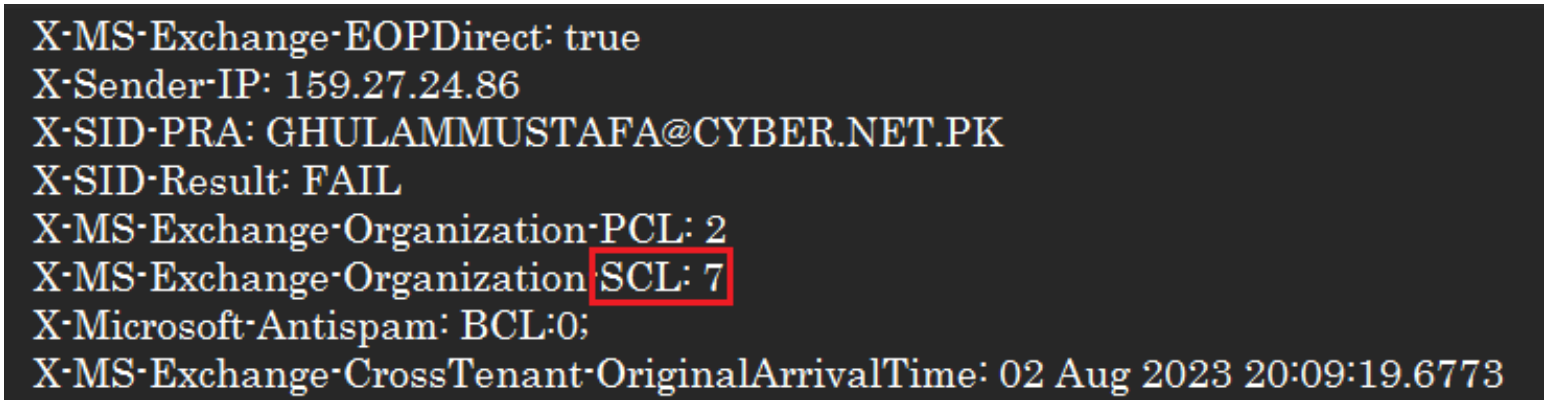
7. Virus Total Analysis for IP 159.27.24.86

- **Result:** The IP is flagged as **malicious**.
- **Location:** Origin traced to **China**.
- **Reputation Score:** A very low score of 1 confirms its use in malicious activities.



8. Raw Email Header Highlighting Spam Confidence Level (SCL)

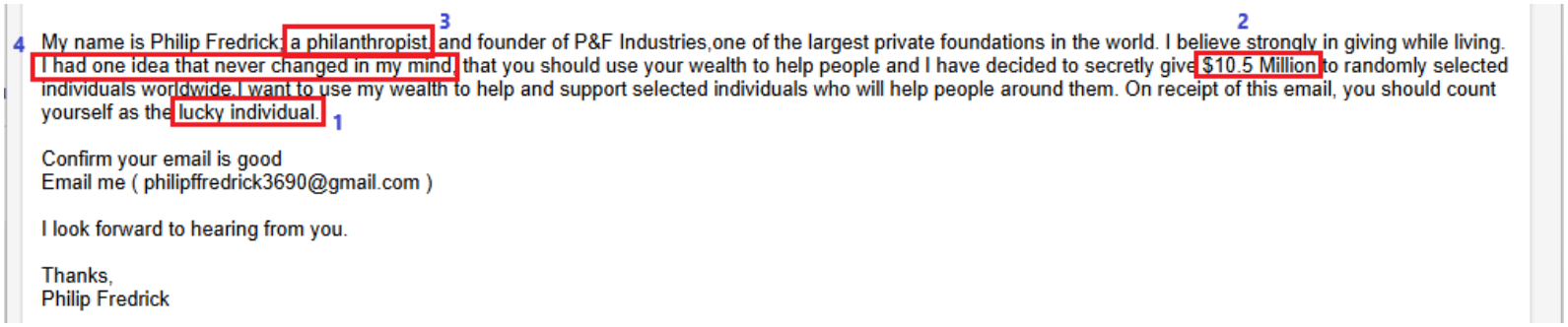
- **Marked in Red:** The Spam Confidence Level (SCL) is set to **7**, indicating a high likelihood of spam as per Microsoft Exchange filtering systems.



9. Email Body Highlighting Suspicious Content

Key phrases in the email body are marked and numbered for reference:

1. **“Lucky individual” (Red Box 1):** Generic phrasing without personalization, typical of phishing.
2. **“$10.5 Million” (Red Box 2):** Unrealistic promises of large sums of money to entice the recipient.
3. **“A philanthropist” (Red Box 3):** Vague claims used to establish false credibility.
4. **“I had one idea that never changed in my mind” (Red Box 4):** Poorly constructed sentence indicative of a scam.



10. Raw Email Header Highlighting Undisclosed Recipients

- **Marked in Red:** The email was addressed to "Undisclosed Recipients," indicating a bulk phishing attempt targeting multiple users.

```
Content-Transfer-Encoding: 7bit
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-IncomingHeaderCount: 12
Message-ID:
 <0bcdb0f2-645d-41e8-8542-9e7541e0914a@BN1NAM02FT046.eop-nam02.prod.protection.outlook.com>
To: Undisclosed recipients:;
Return-Path: ghulammustafa@cyber.net.pk
X-MS-Exchange-Organization-ExpirationStartTime: 02 Aug 2023 20:09:20.5054
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
```

Analysis Summary

The following factors confirm that the email is a phishing attempt and likely fraudulent:

1. **Sender Authentication Failures:**
    - SPF shows a SoftFail indicating the sending IP is not authorized to send on behalf of cyber.net.pk.
    - DKIM is missing, and DMARC fails, flagging the email as unauthenticated.
2. **Spoofing Indicators:**
    - The **From** and **Reply-To** addresses mismatch, with replies directed to a suspicious Gmail account.
3. **Use of Malicious Infrastructure:**
    - Two IPs (147.78.103.9 and 159.27.24.86) linked to malicious activity were used in email transmission.
    - Both IPs are flagged as malicious by VirusTotal and traced to **Bulgaria** and **China**, respectively.
4. **Suspicious Content:**
    - The email uses generic language, unrealistic promises, and vague claims to deceive the recipient.
5. **Spam Classification:**
    - A Spam Confidence Level (SCL) of 7 corroborates the email's classification as likely spam/phishing.

Conclusion

This email is a confirmed phishing attempt with evidence of spoofed sender details, use of malicious infrastructure, and fraudulent content. Immediate action is recommended to mitigate any potential risks.