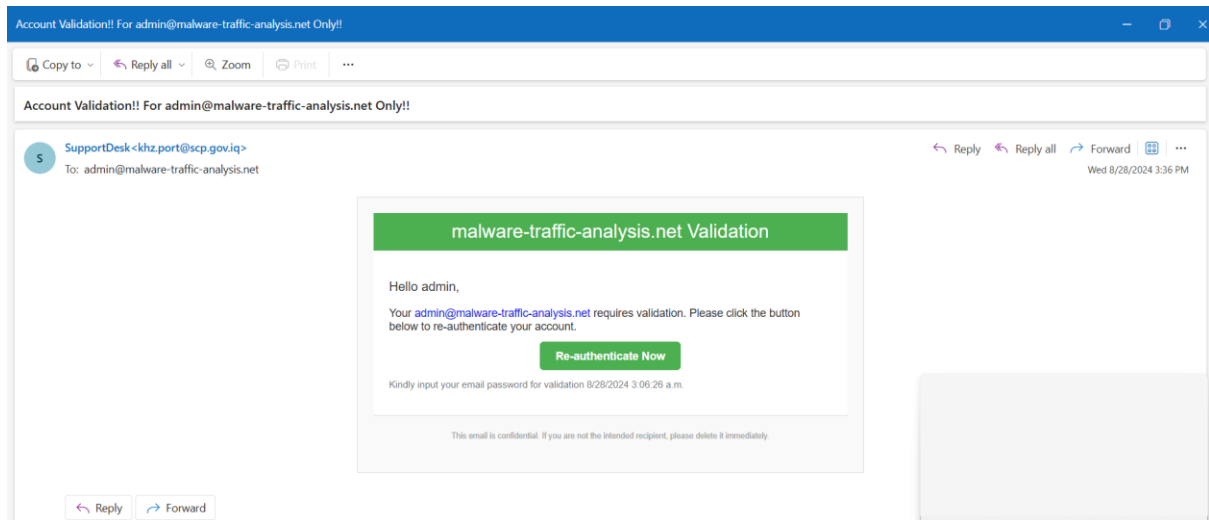# Task-2

Phishing Email Analysis

Here is the Phishing Email that I took for analysis.

From the phishing email, identify the links in buttons or text format. Check the Sender domain or IP address.


First thing we do is header analysis. We will get the email header from our mail box or mail client we are using in. Then we will use the tools like MX toolbox for Header Analysis.

Then check for the sender domain name in the Virus Total. After that we check any links & attachments that are in the received email. In that mail the Re-authenticate Now button hides a malicious URL. Scanning the Domain address.
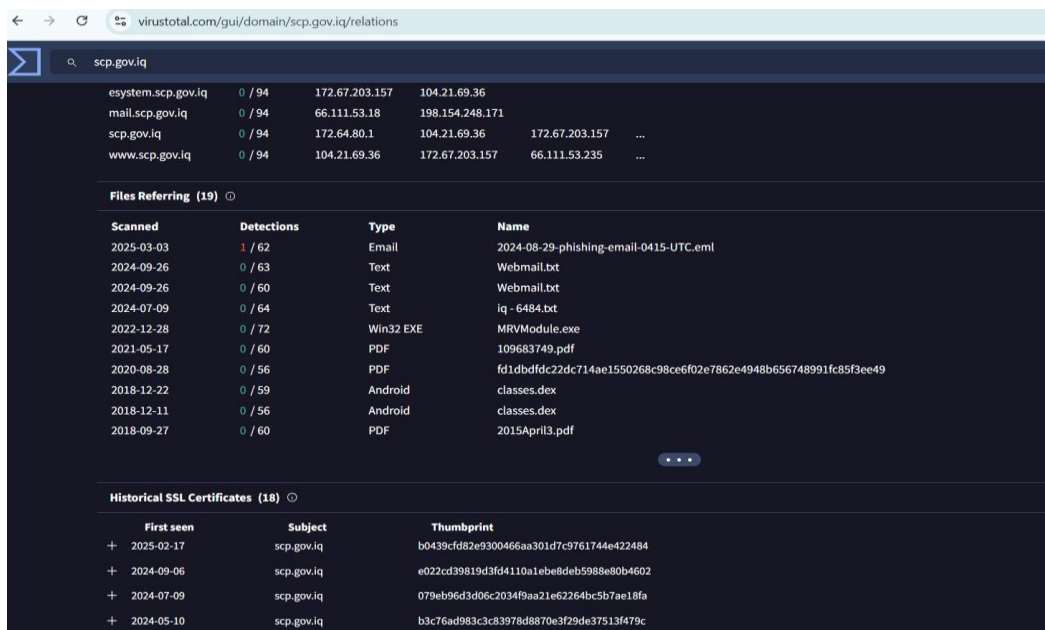
In the above screenshot it gives details about the Domain details such as it is reputation it shows it is malicious, phishing, suspicious or clean.
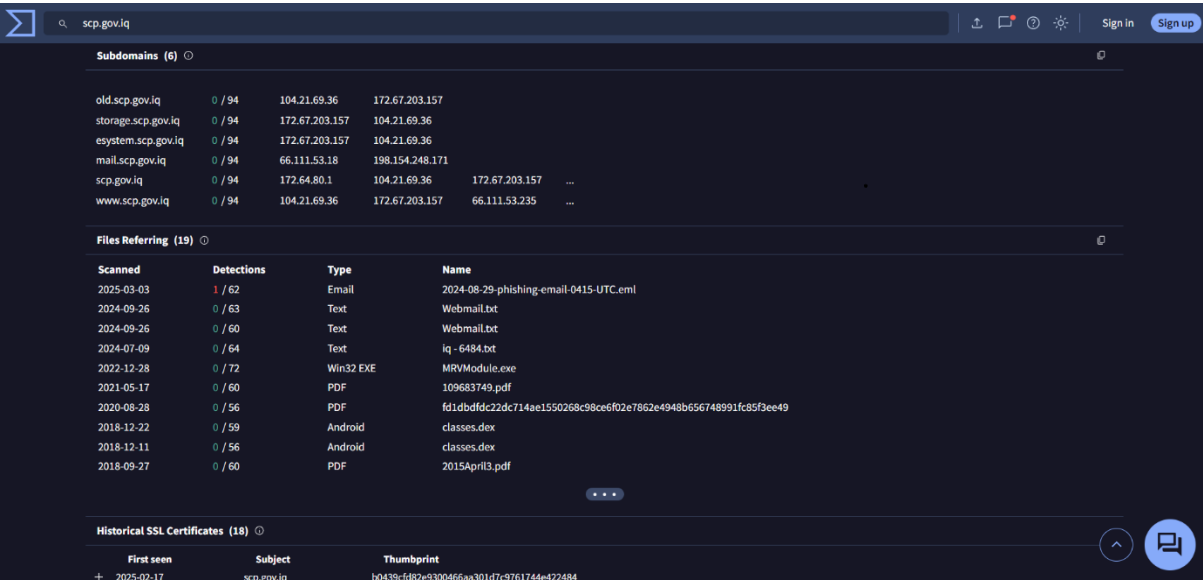

These are the sub domains of that domain. Below it shows the files referring to and there is the phishing email.

In that email if there is an attachment, we have to download that attachment in a secure isolated environment like Virtual Machine or Sandbox. Next we will open the Virus Total and we will upload the attachment or file in it. It will give us the details of the attachment whether it is genuine or any malware is present or not.
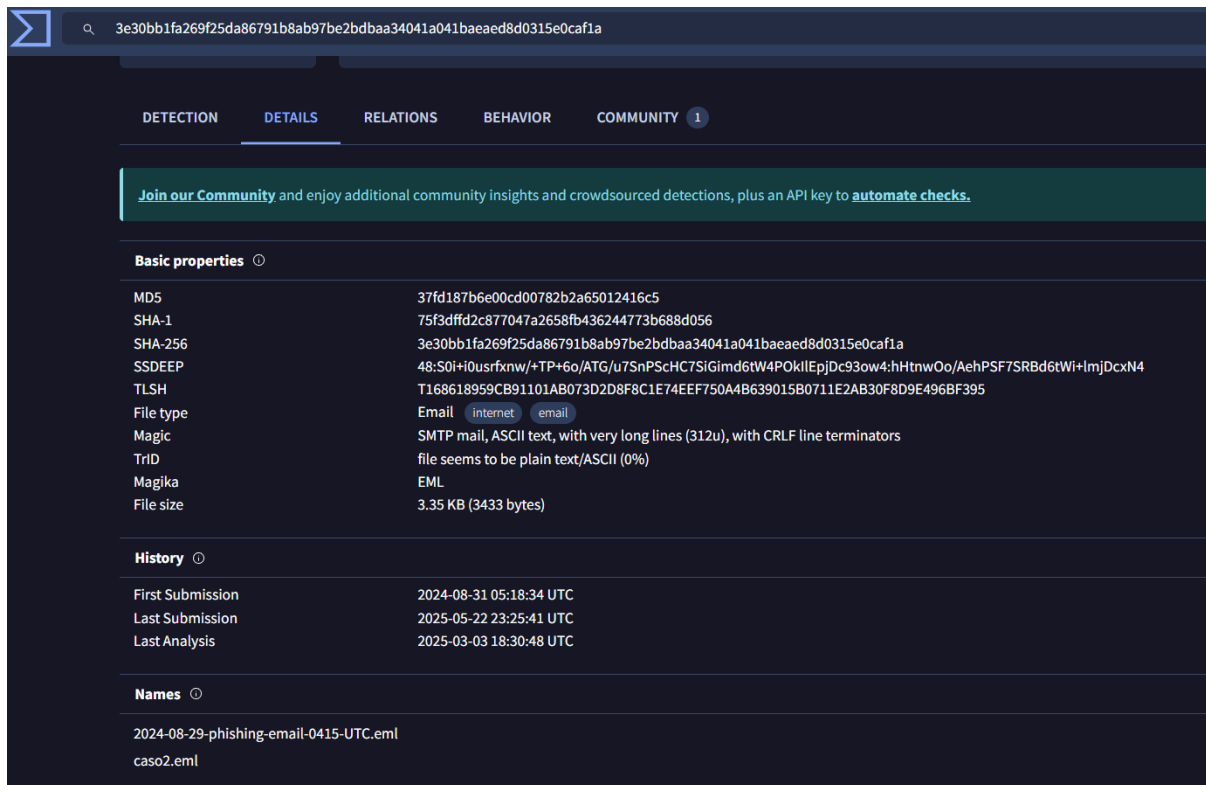
After copying the link from that email, we will paste that link in Virus Total. It will the give the results about it. It showed that the link is malicious.

Here's the Screenshot:
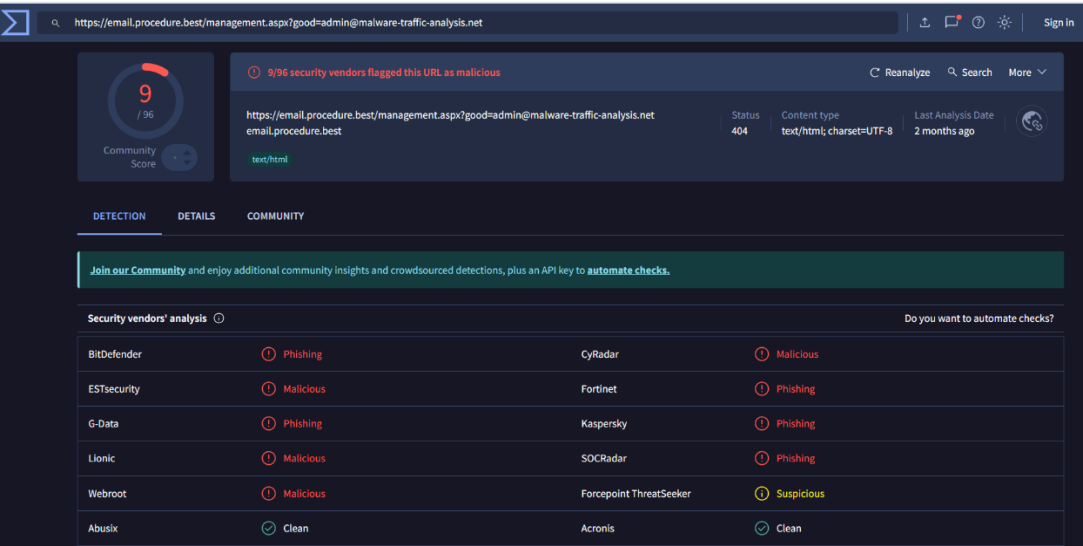
After copying the link from that mail, we will paste it in the virus total. It will give us the details about that link. Here it is showed that 9 security vendors are flagged as Malicious URL.

After clicking on that it shows about the full details of the email that was malicious email it contains the trojan in it will execute the different commands.

After that next step is look at the body of the email it mentioned about the Account Validation that you should authenticate now which is suspicious and it asks for a password.

We should check for malicious payloads in that email attachments by using tools like Virus Total. Then check for links that are attached in that email by using tools like Urlscan.io or Virus Total it will give the results of that link.

If you click on that link by mistake the attacker will get the access, he will exploit the system and he will install the backdoor for access and then he will get the full access like command-and-control C2.

email.procedure.best

172.67.202.104 Public Scan

URL: https://email.procedure.best/management.aspx?=
Submission: On May 29 via manual (May 29th 2025, 8:45:01 am UTC) from IN — Scanned from CH

Summary | HTTP 1 | Redirects | Behaviour | Indicators | Similar | DOM | Content | API | Verdicts

Summary

This website contacted **2 IPs** in **1 countries** across **1 domains** to perform **1 HTTP transactions**. The main IP is **172.67.202.104**, located in **Ascension Island** and belongs to CLOUDFLARENET, US. The main domain is **email.procedure.best**.
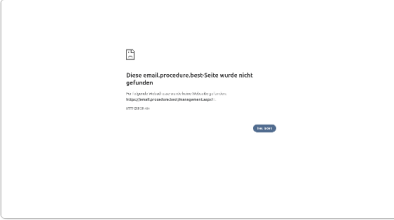TLS certificate: Issued by *WE1* on April 6th 2025. Valid for: 3 months.

email.procedure.best scanned **9 times** on urlscan.io   Show Scans 9

urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *email.procedure.best*
Current DNS A record: 104.21.37.14 (AS13335 - CLOUDFLARENET, US)
Domain created: August 13th 2024, 13:24:52 (UTC)
Domain registrar: SAV.COM, LLC

Screenshot   Live screenshot | Full Image

Page Title

email.procedure.best

We can see that the link is not working at present. This Domain was created in the 2024 August.

Based on this spoofed domain in the header and the malicious link this is confirmed to be a phishing attempt targeting the user credentials.

Tips:

Never open links/attachments on your real machine.

Always use sandbox or VM