

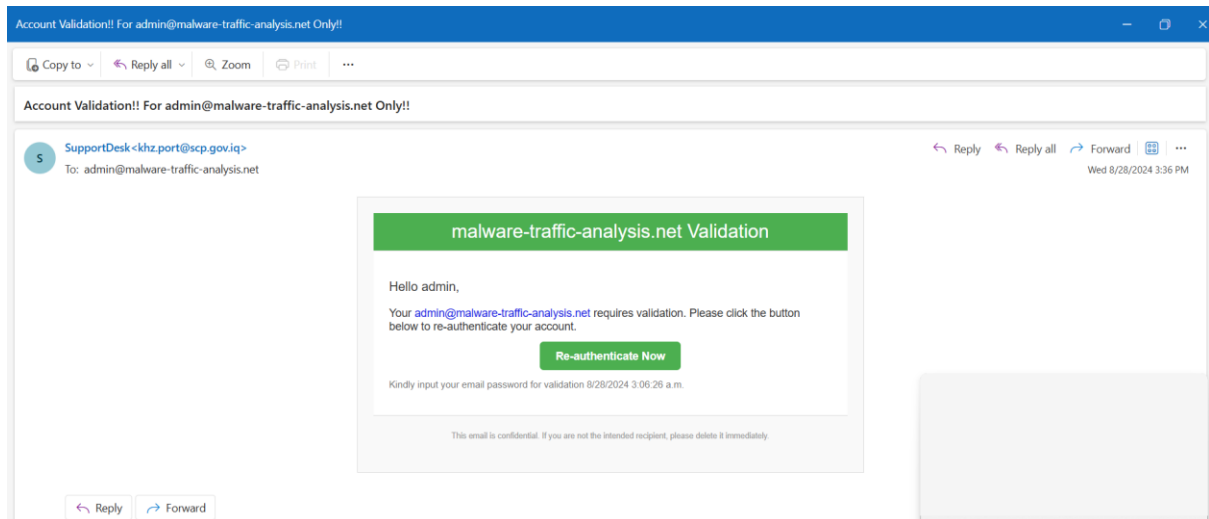
Task-2

Phishing Email Analysis

Here is the Phishing Email that I took for analysis.

I am planning to start the investigation and analysis in 3 steps.

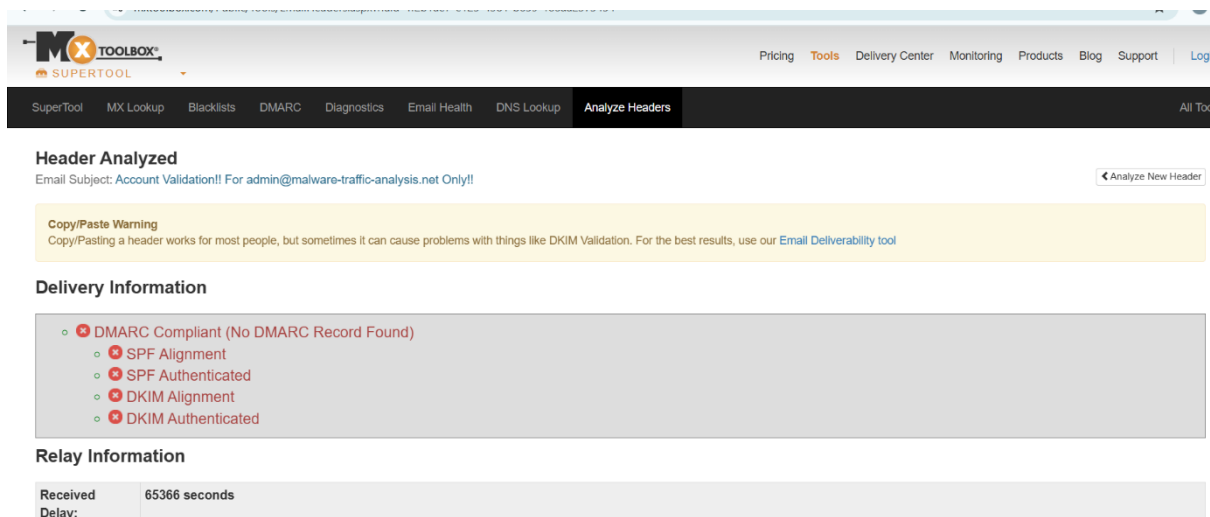
Step-by-step process for Analysing Phishing Email



Step-1: Header Analysis

I extracted and reviewed the full email header using tools like MX toolbox and I checked the return path and the received fields to trace the source IP.

Screenshot:



Here it showed that the Authentication checks are failed which are SPF Alignment, SPF Authenticated, DKIM Alignment, DKIM Authenticated are failed. In the MX

toolbox it showed that there is no record on that SPF and DMARC data. Below I have attached the screenshot of that details.

SPF and DKIM Information

dmARC:scp.gov.iq

Hide

Solve Email Delivery Problems

Test	Result	
<div>✖</div> DMARC Record Published	No DMARC Record found	<div>More Info</div>

Reported by ns01.trs-dns.com on 5/30/2025 at 5:06:20 AM (UTC 0), just for you.

Transcript

SPF:scp.gov.iq:188.127.247.252

Hide

Solve Email Delivery Problems

Test	Result	
<div>✖</div> SPF Record Published	No SPF Record found	<div>More Info</div>
<div>✖</div> DMARC Record Published	No DMARC Record found	<div>More Info</div>
<div>✖</div> DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	<div>More Info</div>

Reported by nsp-anycast.cmc.iq on 5/30/2025 at 5:06:26 AM (UTC 0), just for you.

Transcript

DKIM Signature Error:

No DKIM-Signature header found - [more info](#)

DKIM Signature Error:

There must be at least one aligned DKIM-Signature for the message to be considered aligned. - [more info](#)

I checked the sender domain details in the Virus Total. It showed the details of that domain and its sub domain. Below are the screenshots of that details. It shows the details of files referring to and SSL certificate details.

scp.gov.iq

Subdomains (6)

old.scp.gov.iq	0 / 94	104.21.69.36	172.67.203.157
storage.scp.gov.iq	0 / 94	172.67.203.157	104.21.69.36
esystem.scp.gov.iq	0 / 94	172.67.203.157	104.21.69.36
mail.scp.gov.iq	0 / 94	66.111.53.18	198.154.248.171
scp.gov.iq	0 / 94	172.64.80.1	104.21.69.36
www.scp.gov.iq	0 / 94	104.21.69.36	172.67.203.157

Files Referring (18)

Scanned	Detections	Type	Name
2025-03-03	1 / 62	Email	2024-08-29-phishing-email-0415-UTC.eml
2024-09-26	0 / 63	Text	Webmail.txt
2024-09-26	0 / 60	Text	Webmail.txt
2024-07-09	0 / 64	Text	iq - 6484.txt
2022-12-28	0 / 72	Win32 EXE	MRVModule.exe
2021-05-17	0 / 60	PDF	109683749.pdf
2020-08-28	0 / 56	PDF	fd1dbdfdc2dc714ae1550268c38ceff02e7862e4948b656748991f685f3ee49
2018-12-22	0 / 59	Android	classes.dex
2018-12-11	0 / 56	Android	classes.dex
2018-09-27	0 / 60	PDF	2015Apr13.pdf

Historical SSL Certificates (18)

First seen	Subject	Thumbprint
2025-03-17	scp.gov.iq	10429c607c2300566e30147c3761749e472456

3e30bb1fa269f25da86791b8ab97be2bdbaa34041a041baeaed8d0315e0caf1a

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	37fd187b6e00cd00782b2a65012416c5
SHA-1	75f3dffd2c877047a2658fb436244773b688d056
SHA-256	3e30bb1fa269f25da86791b8ab97be2bdbaa34041a041baeaed8d0315e0caf1a
SSDEEP	48:S0+I0usrfxnw/+TP+6o/ATG/uTSnPScHCT5iGimd6tW4PQkIEpJDC93ow4:hHtnwOo/AehPSF7SRBd6tWi+lmjDcxN4
TLSH	T168618959CB91101AB07302D8f8C1E74EEF750A4B639015B0711E2AB30F8D9E496BF395
File type	Email internet email
Magic	SMTP mail, ASCII text, with very long lines (312u), with CRLF line terminators
TrID	file seems to be plain text/ASCII (0%)
Magika	EML
File size	3.35 KB (3433 bytes)

History

First Submission	2024-08-31 05:18:34 UTC
Last Submission	2025-05-22 23:25:41 UTC
Last Analysis	2025-03-03 18:30:48 UTC

Names

2024-08-29-phishing-email-0415-UTC.eml

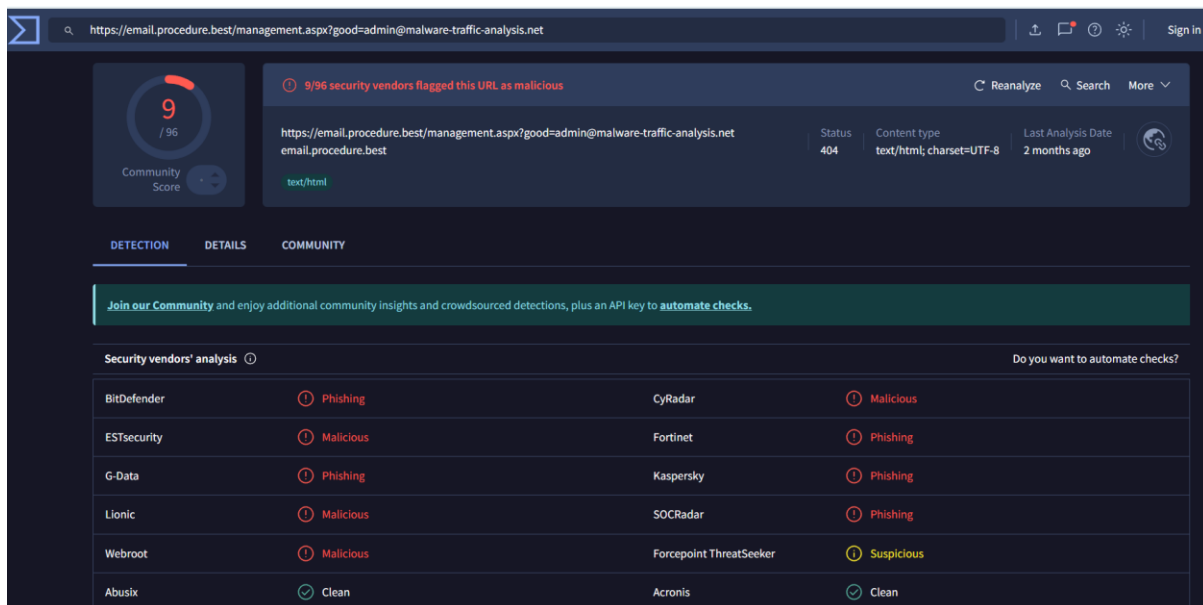
caso2.eml

In that mail the Re-authenticate Now button hides a malicious URL. In the below screenshot it gives details about the Domain details such as its reputation it shows the malicious, phishing, suspicious or clean.

My first stage is completed it failed the Header analysis check.

Step-2: Check any attachments or links are available in that email

I have checked that email and consists a link so I hovered over all hyperlinks to compare the displayed text with the actual URL. Then I copied that URL and pasted it on the Virus Total which is used to check any suspicious URLs are present. Then it started checking that URL. It showed the results that 9 security vendors flagged this URL as malicious.

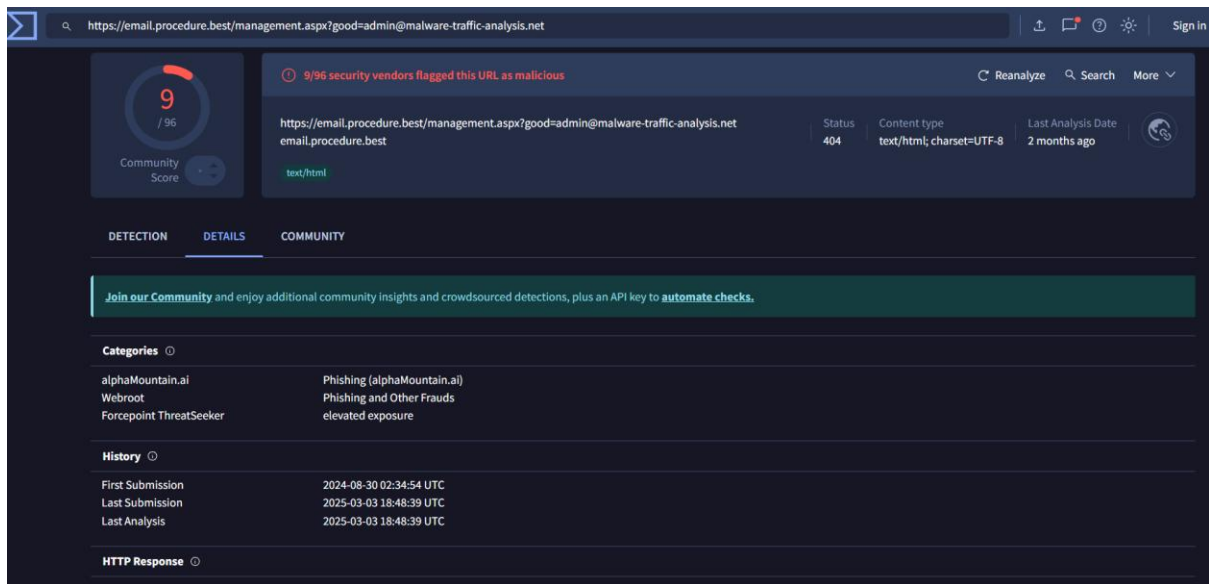


The screenshot shows the VirusTotal interface for the URL `https://email.procedure.best/management.aspx?good=admin@malware-traffic-analysis.net`. The Community Score is 9/96. A banner indicates that 9/96 security vendors flagged this URL as malicious. The status is 404, content type is text/html, and the last analysis was 2 months ago. Below the tabs (DETECTION, DETAILS, COMMUNITY), there is a link to join the community. The 'Security vendors' analysis' table shows the following results:

Security vendors' analysis		Do you want to automate checks?	
BitDefender	Phishing	CyRadar	Malicious
ESTsecurity	Malicious	Fortinet	Phishing
G-Dat	Phishing	Kaspersky	Phishing
Lionic	Malicious	SOCradar	Phishing
Webroot	Malicious	Forcepoint ThreatSeeker	Suspicious
Abusix	Clean	Acronis	Clean

In that email if there is an attachment, we have to download that attachment in a secure isolated environment like Virtual Machine or Sandbox. 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. This helped me identify whether the links redirected to known phishing or malicious sites.

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. Below mentioned the details of that URL.



Step-3: Body of the Email

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.

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

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](#)
[Redirects](#)
[Behaviour](#)
[Indicators](#)
[Similar](#)
[DOM](#)
[Content](#)
[API](#)
[Verdicts](#)

[Lookup](#) [Go To](#) [Rescan](#)

[Add Verdict](#) [Report](#)

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](#)

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 form analysis it showed that the URL was not working at present.

 urlscan.io [Home](#) [Search](#) [Live](#) [API](#) [Blog](#) [Docs](#) [Pricing](#) [Login](#)

email.procedure.best [Back to summary](#)

104.21.37.14 [Unlisted Scan](#)

URL: <https://email.procedure.best/management.aspx?good=admin@malware-traffic-analysis.net>

Submission: On May 30 via manual (May 30th 2025, 6:11:49 am UTC) from [IN](#) — Scanned from [US](#)

Form analysis 0 forms found in the DOM

Text Content

THIS EMAIL.PROCEDURE.BEST PAGE CAN'T BE FOUND

No webpage was found for the web address:
<https://email.procedure.best/management.aspx?good=admin@malware-traffic-analysis.net>

HTTP ERROR 404
Reload

No webpage was found for the web address:
<https://email.procedure.best/management.aspx?good=admin@malware-traffic-analysis.net>

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