TASK 2

Analyze a Phishing Email Sample

1. Tools Used: MXToolbox, Google Header Analyzer, VirusTotal, CheckPhish, Gmail Header Analyzer.

2. Sample Phishing Email.

   I have downloaded the sample phishing email format from https://www.terranovasecurity.com/blog/top-examples-of-phishing-emails

   Subject: Urgent Action Required – Account Suspension Notice

   Dear User,

   We have detected unusual activity in your account. To ensure the security of your information, we have temporarily suspended access to your account.

   Please open the attached document and follow the instructions to verify your identity and restore access:

   📎 **Attachment: Account_Verification_Form.zip**

   Failure to complete verification within 24 hours will result in permanent suspension.

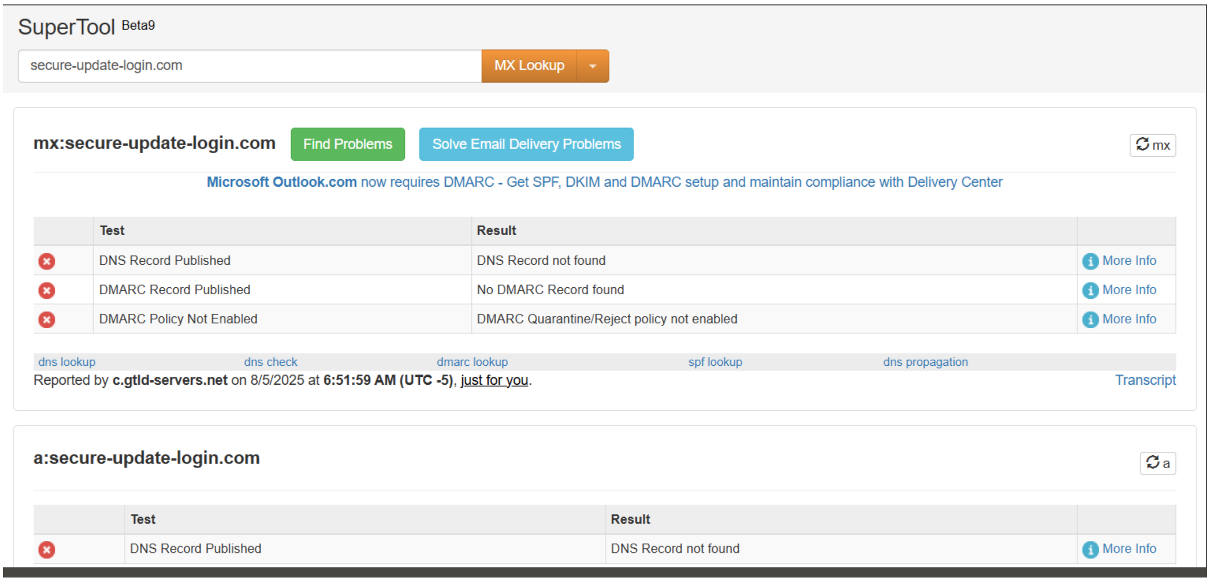
   Thank you for your cooperation,
   Security Team – [YourServiceName]

   support@secure-update-login.com

3. Analyzing Phishing Email.

   1. Obtain a Sample Phishing Email
   A simulated phishing email was used that includes a fake security alert and a malicious ZIP file attachment.

   2. Examine Sender's Email for Spoofing
   Sender email: support@secure-update-login.com — Domain appears unrelated to any legitimate organization. MXToolbox confirmed missing SPF/DMARC/DNS records, indicating spoofing potential.



SuperTool Beta9

secure-update-login.com

mx:secure-update-login.com

Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center

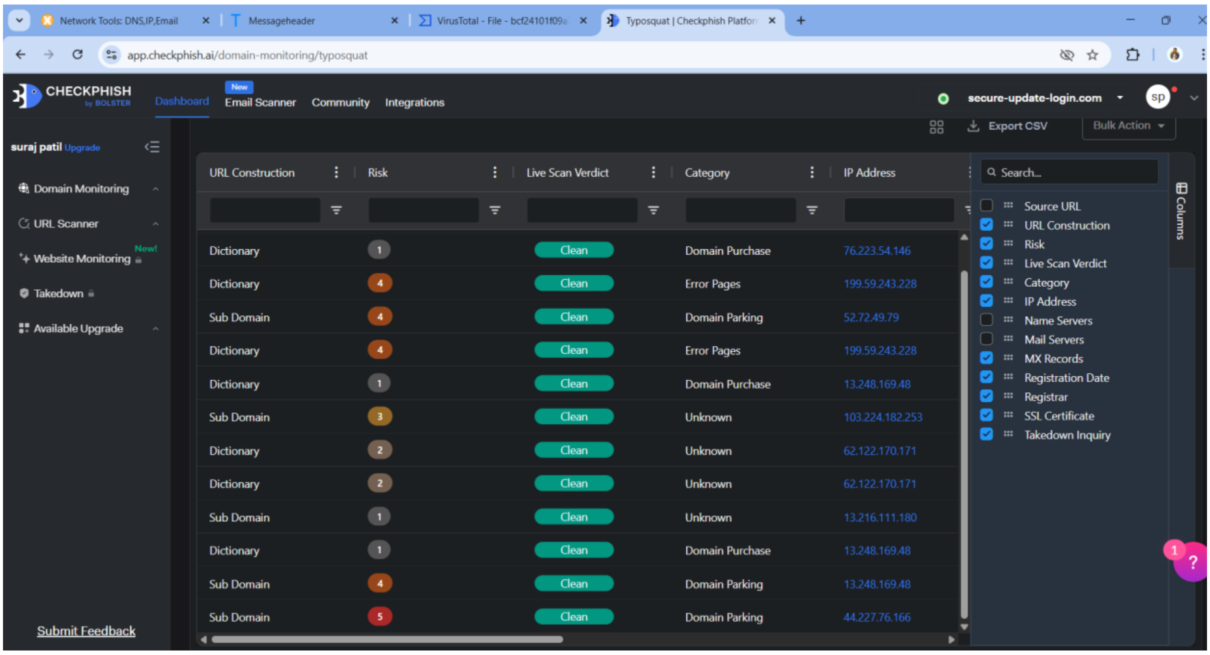
	Test	Result	
☒	DNS Record Published	DNS Record not found	More Info
☒	DMARC Record Published	No DMARC Record found	More Info
☒	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info

Reported by **c.gtld-servers.net** on 8/5/2025 at **6:51:59 AM (UTC -5)**, just for you.

a:secure-update-login.com

	Test	Result	
☒	DNS Record Published	DNS Record not found	More Info

Checkphish ai Scanning domain



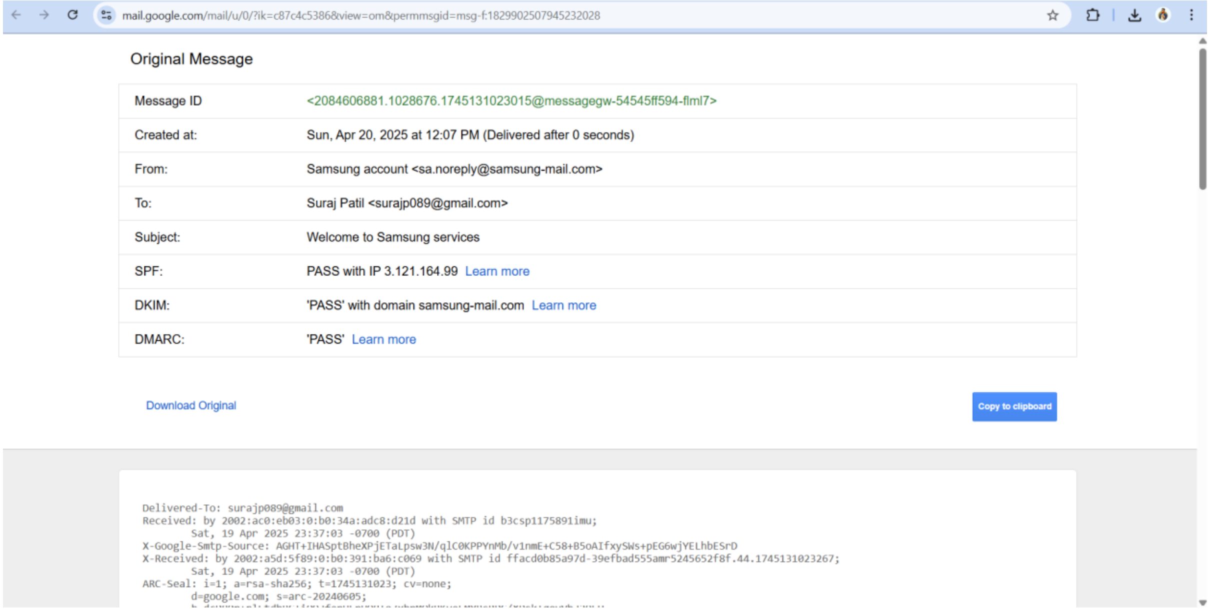
URL Construction	Risk	Live Scan Verdict	Category	IP Address
Dictionary	1	Clean	Domain Purchase	76.223.54.146
Dictionary	4	Clean	Error Pages	199.59.243.228
Sub Domain	4	Clean	Domain Parking	52.72.49.79
Dictionary	4	Clean	Error Pages	199.59.243.228
Dictionary	1	Clean	Domain Purchase	13.248.169.48
Sub Domain	3	Clean	Unknown	103.224.182.253
Dictionary	2	Clean	Unknown	62.122.170.171
Dictionary	2	Clean	Unknown	62.122.170.171
Sub Domain	1	Clean	Unknown	13.216.111.180
Dictionary	1	Clean	Domain Purchase	13.248.169.48
Sub Domain	4	Clean	Domain Parking	13.248.169.48
Sub Domain	5	Clean	Domain Parking	44.227.76.166

☐ Source URL
☑ URL Construction
☑ Risk
☑ Live Scan Verdict
☑ Category
☑ IP Address
☐ Name Servers
☐ Mail Servers
☑ MX Records
☑ Registration Date
☑ Registrar
☑ SSL Certificate
☑ Takedown Inquiry

3. Check Email Headers Using Online Analyzer

Analyzed using Google's MessageHeader tool. Found mismatch in return-path (from .ru domain), source IP from blacklisted hosting, and missing email authentication mechanisms.

We can check the email header from gmail >> Open Mail >> Click on Three dots >> Click on Show Original.



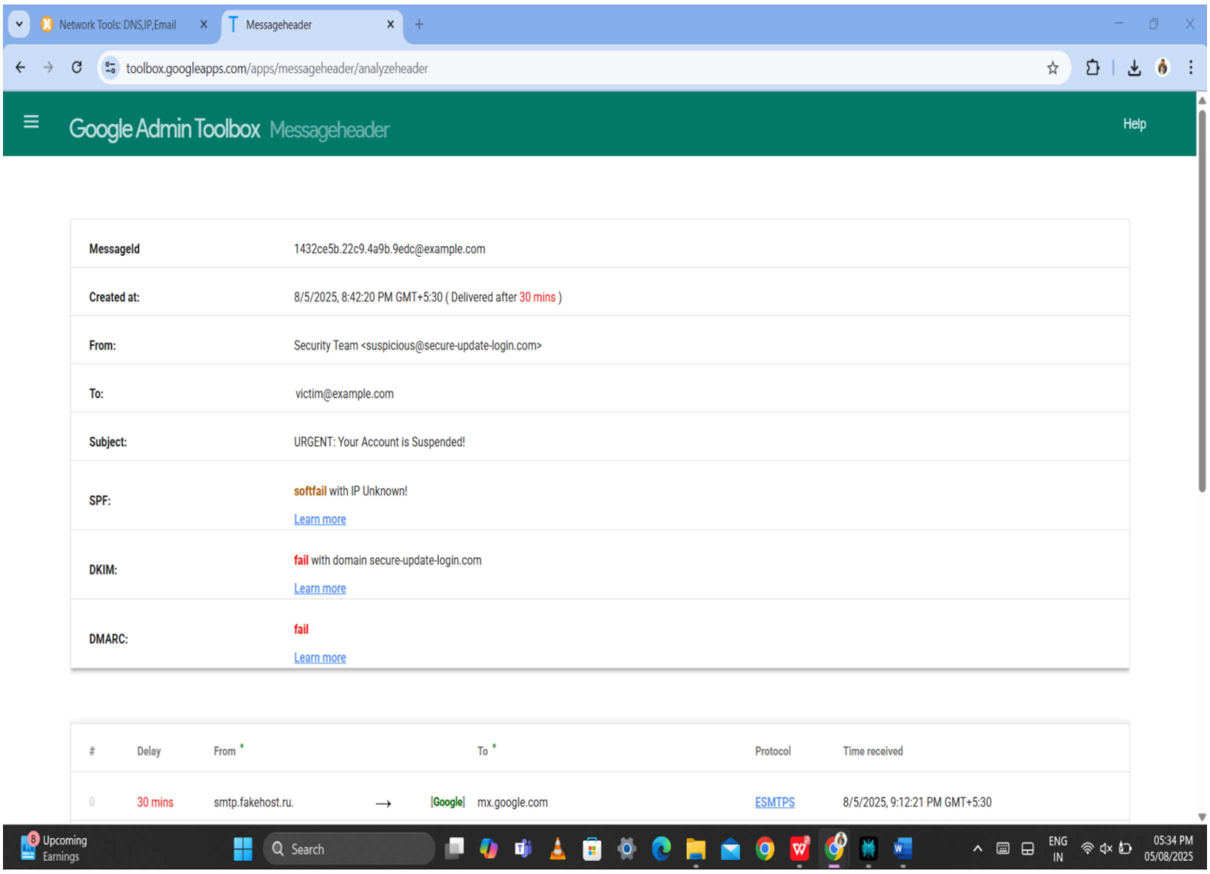
mail.google.com/mail/u/0/?ik=c87c4c5386&view=om&permmsgid=msg-f:1829902507945232028

Original Message

Message ID	<2084606881.1028676.1745131023015@messagegw-54545ff594-flml7>
Created at:	Sun, Apr 20, 2025 at 12:07 PM (Delivered after 0 seconds)
From:	Samsung account <sa.noreply@samsung-mail.com>
To:	Suraj Patil <surajp089@gmail.com>
Subject:	Welcome to Samsung services
SPF:	PASS with IP 3.121.164.99 Learn more
DKIM:	'PASS' with domain samsung-mail.com Learn more
DMARC:	'PASS' Learn more

Download Original
Copy to clipboard

```
Delivered-To: surajp089@gmail.com
Received: by 2002:ac0:eb03:0:b0:34a:adc8:d21d with SMTP id b3csp1175891imu;
        Sat, 19 Apr 2025 23:37:03 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IHASptBheXPjETaLpsw3N/qlC0KPPYnMb/v1nmE+C58+B5oAIfxySWs+pEG6wjYELhbESrD
X-Received: by 2002:a5d:5f89:0:b0:391:ba6:c069 with SMTP id ffacd0b85a97d-39efbad555amr5245652f8f.44.1745131023267;
        Sat, 19 Apr 2025 23:37:03 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1745131023; cv=none;
        d=google.com; s=arc-20240605;
```



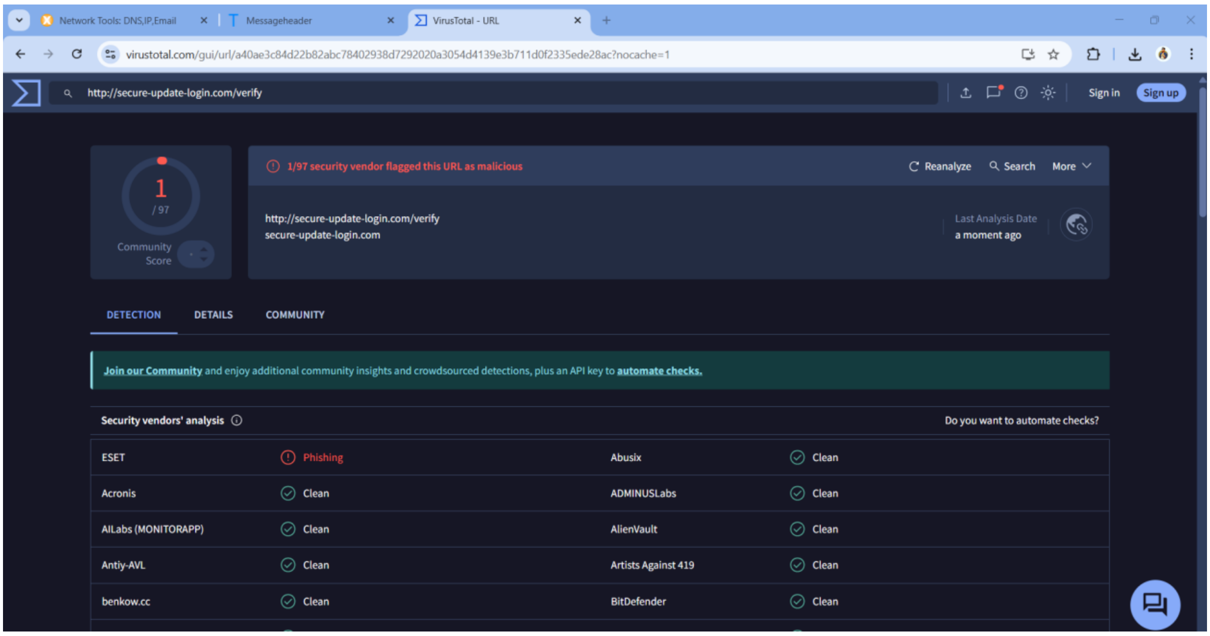
Network Tools: DNS,IP,Email
Messageheader
toolbox.googleapps.com/apps/messageheader/analyzeheader
Google Admin Toolbox Messageheader
Help

MessageId	1432ce5b.22c9.4a9b.9edc@example.com
Created at:	8/5/2025, 8:42:20 PM GMT+5:30 (Delivered after 30 mins)
From:	Security Team <suspicious@secure-update-login.com>
To:	victim@example.com
Subject:	URGENT: Your Account is Suspended!
SPF:	softfail with IP Unknown! Learn more
DKIM:	fail with domain secure-update-login.com Learn more
DMARC:	fail Learn more

#	Delay	From *		To *	Protocol	Time received
0	30 mins	smtp.fakehost.ru.	→	[Google] mx.google.com	ESMTPS	8/5/2025, 9:12:21 PM GMT+5:30

4. Identify Suspicious Links or Attachments

Link :- http://secure-update-login.com/verify



virustotal.com/gui/url/a40ae3c84d22b82abc78402938d7292020a3054d4139e3b711d0f2335ede28ac?nocache=1

http://secure-update-login.com/verify

1/97 security vendor flagged this URL as malicious

http://secure-update-login.com/verify
secure-update-login.com

Last Analysis Date
a moment ago

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

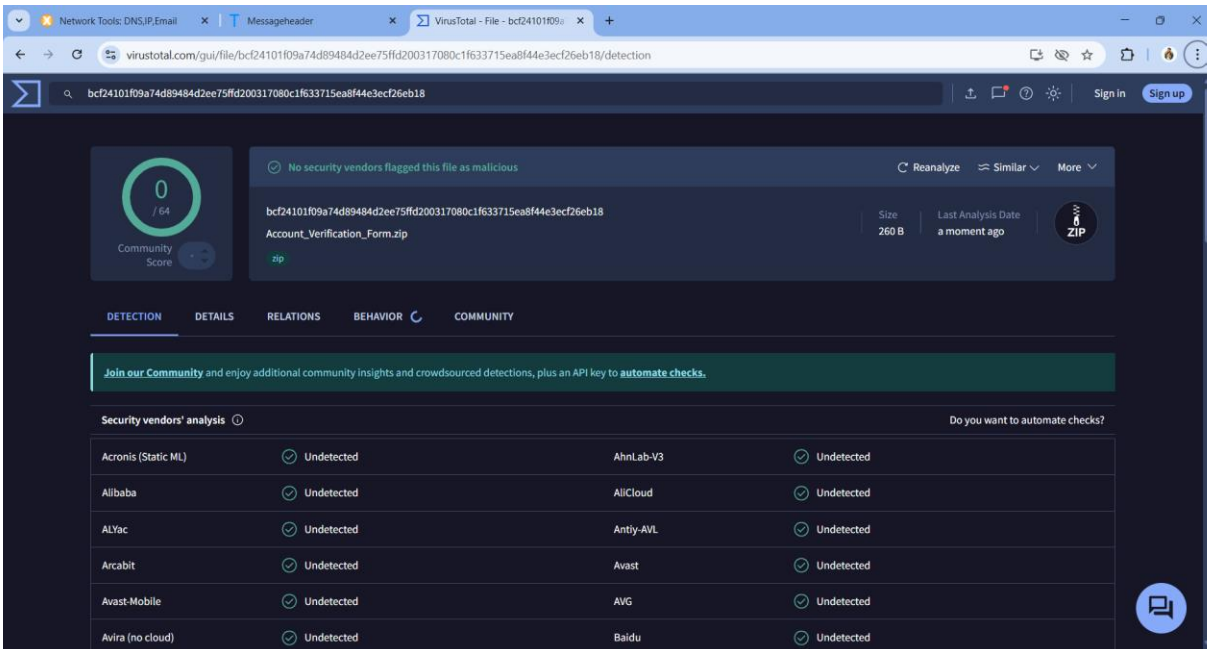
Security vendors' analysis

Do you want to automate checks?

ESET	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean

VirusTotal scan showing 1/97 detection by ESET
Explanation that **even 1 flagged vendor** is a red flag

Attachment: Account_Verification_Form.zip was scanned and showed 0 detections.



virustotal.com/gui/file/bcf24101f09a74d89484d2ee75ffd200317080c1f633715ea8f44e3ecf26eb18/detection

bcf24101f09a74d89484d2ee75ffd200317080c1f633715ea8f44e3ecf26eb18

No security vendors flagged this file as malicious

bcf24101f09a74d89484d2ee75ffd200317080c1f633715ea8f44e3ecf26eb18
Account_Verification_Form.zip
zip

Size
260 B

Last Analysis Date
a moment ago

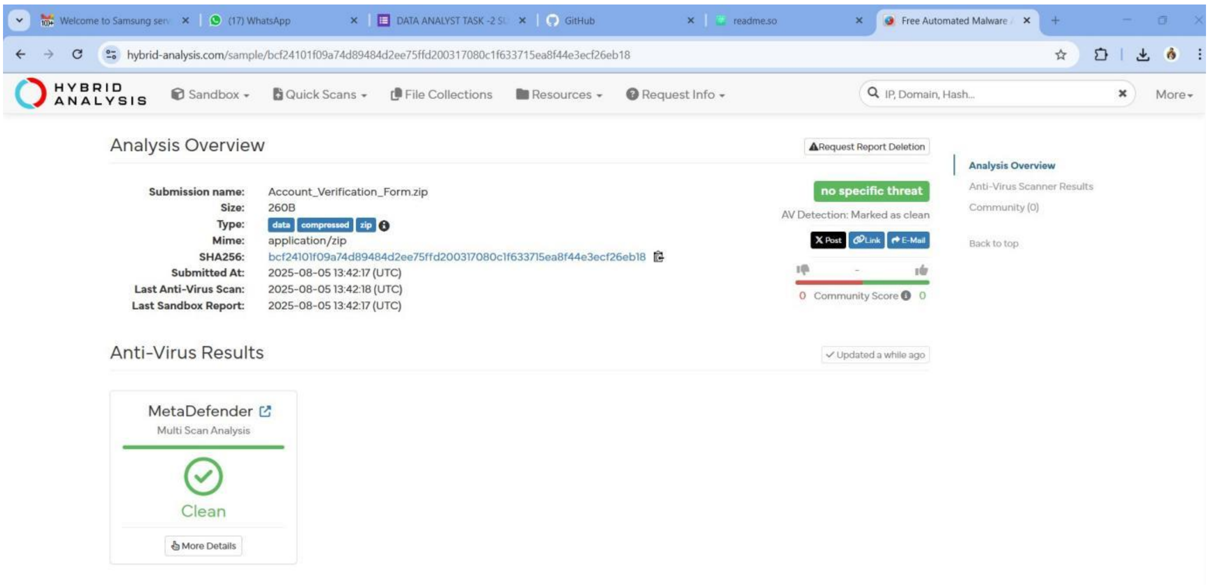
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected

Hybrid Analysis Scanning Result:



Analysis Overview

Submission name: Account_Verification_Form.zip
Size: 260B
Type: data compressed zip
Mime: application/zip
SHA256: bcf24101f09a74d89484d2ee75ffd200317080c1f633715ea8f44e3ecf26eb18
Submitted At: 2025-08-05 13:42:17 (UTC)
Last Anti-Virus Scan: 2025-08-05 13:42:18 (UTC)
Last Sandbox Report: 2025-08-05 13:42:17 (UTC)

no specific threat
AV Detection: Marked as clean
0 Community Score 0

Anti-Virus Results

✓ Updated a while ago

MetaDefender
Multi Scan Analysis
Clean

5. Look for Urgent or Threatening Language

Phrases like 'urgent action required', 'account suspended', and 'failure to respond will result in permanent suspension' are examples of scare tactics used to prompt quick, unthinking action.

6. Mismatched URLs (Hover Technique)

Though no hyperlink in this version, similar phishing emails include masked URLs. Hovering often reveals redirects to unrelated IPs or domain names.

7. Spelling/Grammar Errors

The email uses generic terms ('Dear User'), inconsistent punctuation, lacks branding or signatures, and includes grammatical awkwardness.

8. Summarize Phishing Traits

- Spoofed email address
- No SPF/DMARC/DNS
- No Malicious ZIP attachment
- Urgent and threatening tone
- Generic and impersonal content
- Poor formatting and security cues