

CYBER SECURITY LAB-3 PHISHING EMAILS

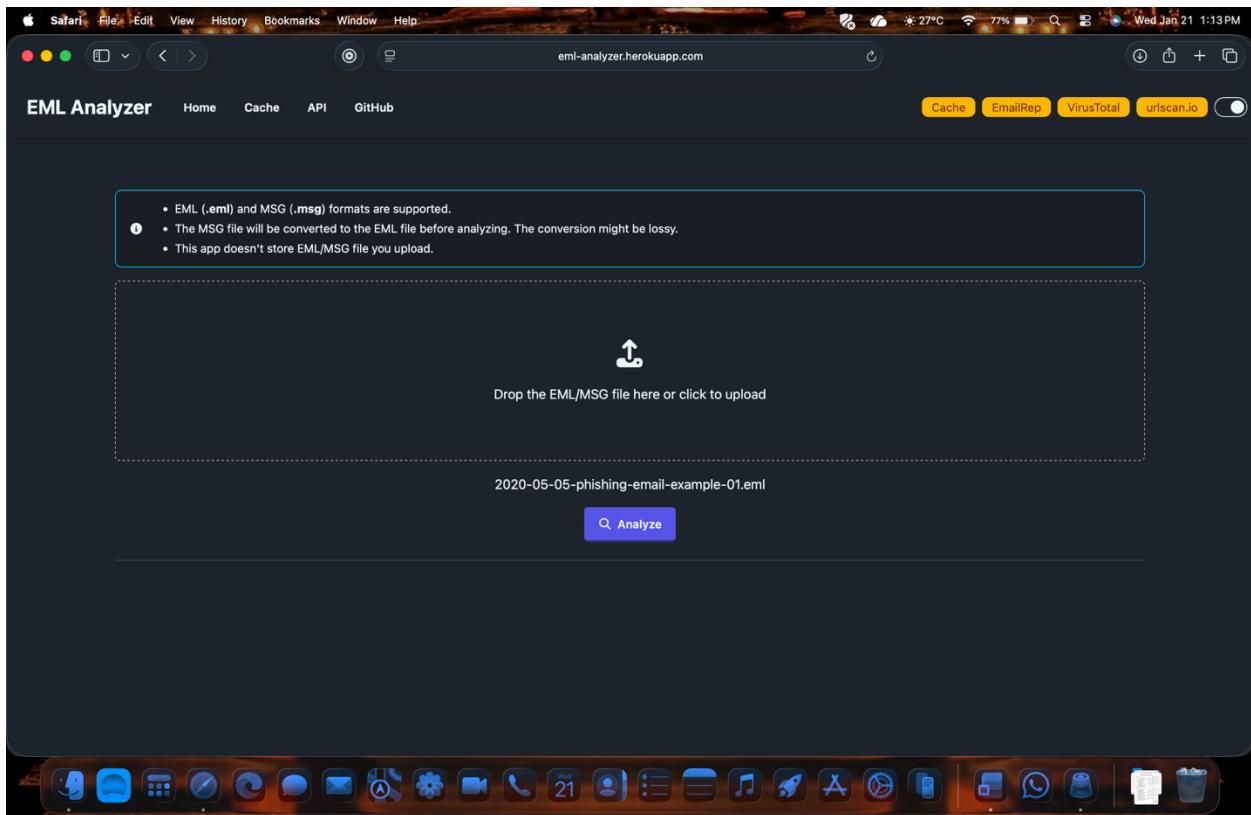
23BD1A052Q HARI VIGNESH RAO

Experiment: Analyzing Phishing Emails

To analyze a suspicious email using EML Analyzer and VirusTotal and identify whether it is phishing based on technical indicators.

Part A: EML Analyzer Results

The file 2020-05-05-phishing-email-example-01.eml was uploaded to the EML Analyzer.



EML Analyzer Results:

Key Observations:

- Subject: Warning: Final Notice
- From: sues@nnwifi.com
- To: brad@malware-traffic-analysis.net
- Content Type: text/html
- Message-ID: Missing

Basic headers	
Message ID	N/A
Subject	⚠ Warning: ✅ Final notice : malware-traffic-analysis.net™
Date (UTC)	2020-05-05T14:58:44Z
From	sues@nnwifi.com
To	brad@malware-traffic-analysis.net
Other headers	
content-transfer-encoding	quoted-printable
content-type	text/html; charset="iso-8859-1"

Header Analysis:

- Sender IP: 94.100.31.27
- Reverse DNS: 94-100-31-27.static.hvvc.us
- Mail Server: mail.nnwifi.com

Verdicts										
oleid	N/A									
There is no suspicious OLE file in attachments.										
N/A										
Headers										
Hops										
Hop	From	By	With	Date (UTC)	Delay					
1	94.100.31.27, 94-100-31-27.static.hvvc.us, nnwifi.com	mail.nnwifi.com	esmtpa id 900ebc20064a	2020-05-05T07:20:19Z	N/A					
2	127.0.0.1, mail.nnwifi.com	127.0.0.1, mail.nnwifi.com	esmtp id acdb6zuvbnrn	2020-05-05T09:58:55Z	3 hours					
3	127.0.0.1	mail.nnwifi.com	esmtp id 58618c1d3543	2020-05-05T09:58:55Z	N/A					
4	127.0.0.1, mail.nnwifi.com	127.0.0.1, mail.nnwifi.com	esmtp id jgwpvva6ppj_9	2020-05-05T12:44:32Z	3 hours					
5	127.0.0.1	mail.nnwifi.com	esmtp id 29423c1d2bf3	2020-05-05T12:44:33Z	a few seconds					
6	173.46.174.49, mail.nnwifi.com			2020-05-05T13:30:50Z	an hour					

Safari File Edit View History Bookmarks Window Help

virustotal.com

G VirusTotal - IP address - 94.100.31.27

EML Analyzer

Σ 94.100.31.27

Did you intend to search across the file corpus instead? Click here

1/92 security vendor flagged this IP address as malicious

94.100.31.27 (94.100.28.0/22)
AS 29802 (HVC-AS)

NI Last Analysis Date 3 days ago

Detection Details Relations Community

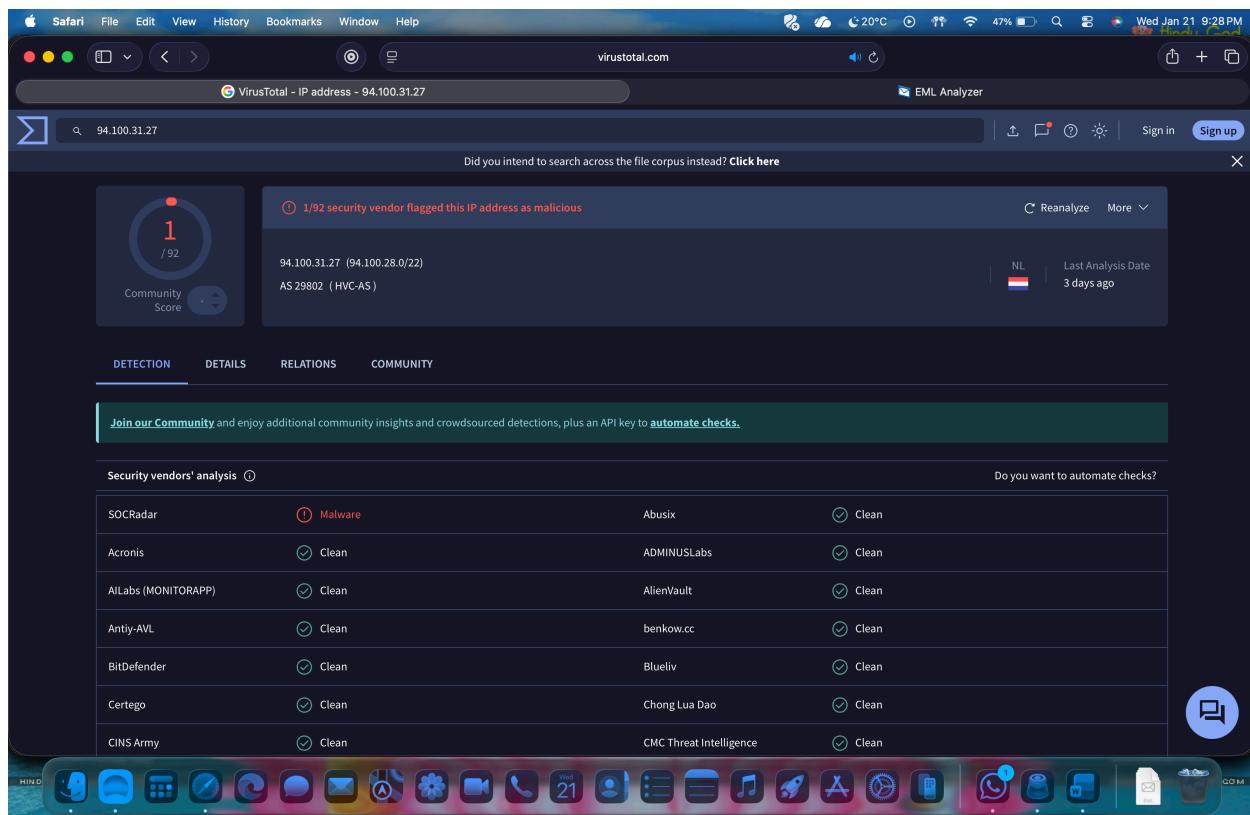
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

SOCRadar	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
All Labs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean

Do you want to automate checks?

HIND



Safari File Edit View History Bookmarks Window Help

eml-analyzer.herokuapp.com

EML Analyzer

Home Cache API GitHub

Cache EmailRep VirusTotal urlscan.io

• EML (.eml) and MSG (.msg) formats are supported.
• The MSG file will be converted to the EML file before analyzing. The conversion might be lossy.
• This app doesn't store EML/MSG file you upload.

Drop the EML/MSG file here or click to upload

Updates to how privacy settings work on Play.eml

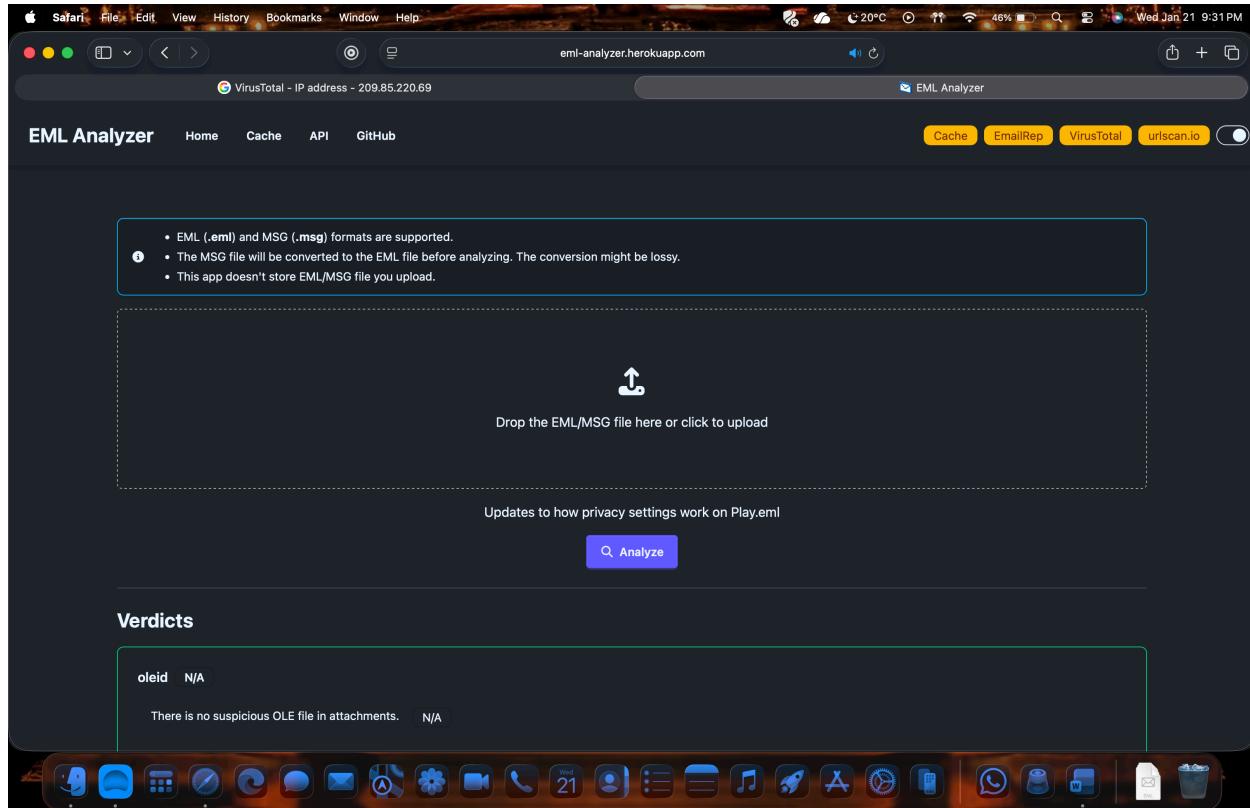
Analyze

Verdicts

oleid N/A

There is no suspicious OLE file in attachments. N/A

HIND



Safari File Edit View History Bookmarks Window Help

VirusTotal - IP address - 209.85.220.69 eml-analyzer.herokuapp.com

Verdicts

oleid N/A
There is no suspicious OLE file in attachments. N/A

DKIM N/A
DKIM signature verification failed or no valid signature found N/A

Headers

Hops

Hop	From	By	With	Date (UTC)	Delay
1	209.85.220.69, mail-sor-f69.google.com	mx.google.com	smtps id 006d021491bc7-65f48bb819asor10186409eaf.1.2026.0 1.13.17.40.05	2026-01-14T01:40:05Z	N/A
2		2002:a05:6124:8484:10b0:42b:cdf3:f21f	smtp id w4-nicsp4128233vld	2026-01-14T01:40:05Z	N/A

Basic headers

Message ID <9598d104ec0e2f48253923a5e46d9e66e08a1b19-20382279-987377478@google.com>

Subject Updates to how privacy settings work on Play

Safari File Edit View History Bookmarks Window Help

virustotal.com

VirusTotal - IP address - 209.85.220.69

Community Score 95

0 / 92

10+ detected files embedding this IP address

209.85.220.69 (209.85.128.0/17)
AS 15169 (GOOGLE)

US Last Analysis Date 6 hours ago

Detection Details Relations Community 57

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

Security vendors' analysis

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AI Labs (MONITORAPP)	Clean
AlienVault	Clean	AlphaSOC	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean

Part B: VirusTotal Analysis

The sender IP 94.100.31.27 was checked on VirusTotal.

VirusTotal Result:

- Detection Ratio: 1 / 92 vendors flagged as malicious
- Location: Netherlands
- ASN: AS29802 (HVC-AS)

This means the IP is not widely blacklisted but has suspicious reputation.

The screenshot shows the VirusTotal website interface. At the top, it says "1 / 92 security vendor flagged this IP address as malicious". Below this, it provides the IP address (94.100.31.27), its location (AS 29802 (HVC-AS)), and the last analysis date (3 days ago). A "Community Score" icon shows a red "1" over a blue circle with "92". Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A green banner encourages joining the community. The main content area is titled "Security vendors' analysis" and lists 14 vendors, each with their name, analysis result (either Malware or Clean), and a "Clean" status indicator. A "Do you want to automate checks?" button is visible on the right. The bottom of the screen shows the Mac OS X dock with various application icons.

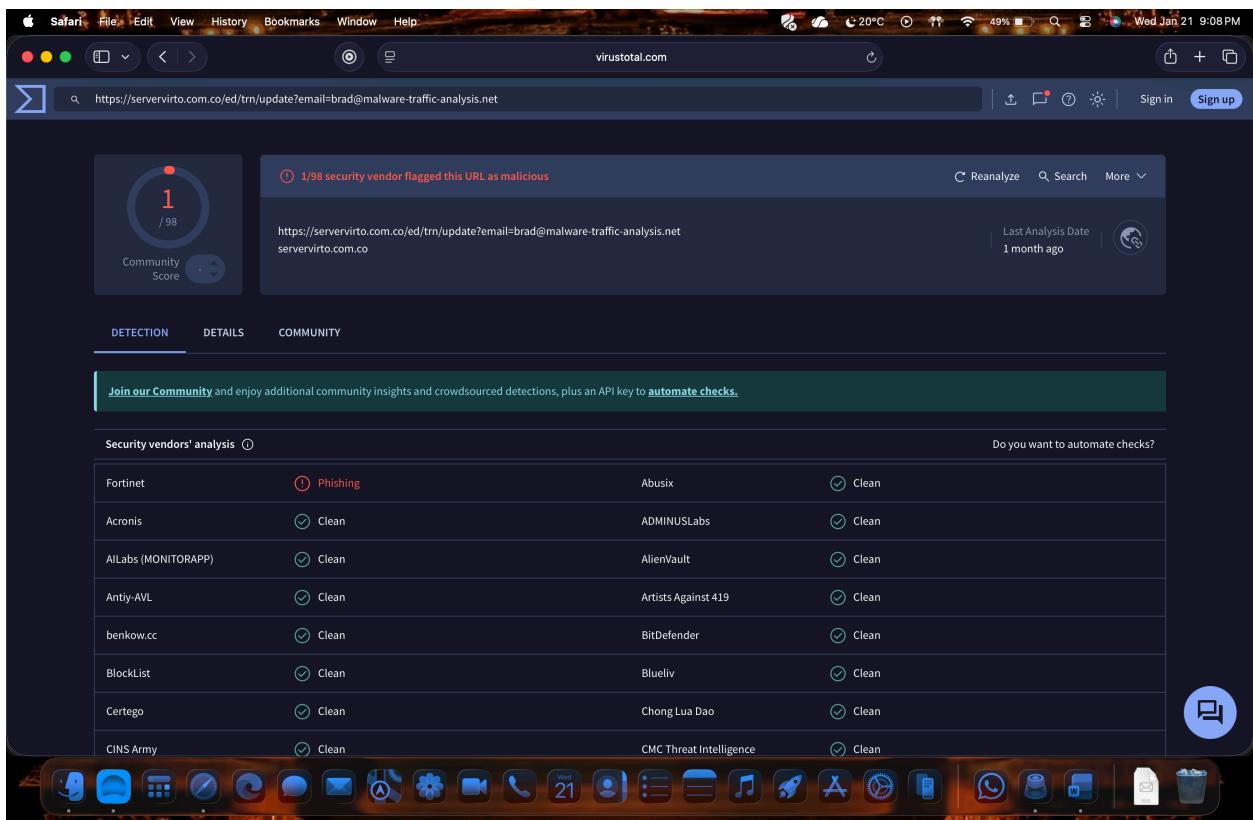
Suspicious Link Identified

From EML Analyzer, the following URL was extracted:

<https://servervirtocom.co/ed/trn/update?email=brad@malware-traffic-analysis.net>

Reasons it is suspicious:

- Does not match sender domain (nnwifi.com)
- Uses foreign domain (.com.co)
- Requests confirmation of ownership (credential harvesting pattern)



Not Suspicious Ip Address

The screenshot shows a VirusTotal analysis page for the IP address 38.68.46.250. The main interface displays a large green circle with a '0' and the text 'Community Score / 92'. It also states '3 detected files embedding this IP address'. Below this, it lists the IP as 38.68.46.250 (38.68.46.0/23) and its Autonomous System (AS) number as 396073 (MAJESTIC-HOSTING-01). A small American flag icon indicates the analysis was performed in the US, with a 'Last Analysis Date' of '1 month ago'. The page includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY, with the DETECTION tab selected. A green banner at the bottom encourages users to 'Join our Community' and automate checks. On the right side, there's a 'Do you want to automate checks?' button and a blue circular icon with a white speechmark symbol. The bottom of the screen shows the Mac OS X dock with various application icons.

Not Suspicious Link

No security vendors flagged this URL as malicious

https://myaccount.google.com/security
myaccount.google.com

Status 200 | Content type text/html; charset=utf-8 | Last Analysis Date 1 day ago

text/html external-resources

Community Score 1

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

Security vendor	Analysis result	Action
Abusix	Clean	Clean
ADMINUSLabs	Clean	Clean
AlienVault	Clean	Clean
Artists Against 419	Clean	Clean
BitDefender	Clean	Clean
Blueliv	Clean	Clean
Chong Lua Dao	Clean	Clean
Acronis	Clean	Clean
AI Labs (MONITORAPP)	Clean	Clean
Antiy-AVL	Clean	Clean
benkow.cc	Clean	Clean
BlockList	Clean	Clean
Certego	Clean	Clean
CINS Army	Clean	Clean