CYBER SECURITY LAB-3 PHISHING EMAILS

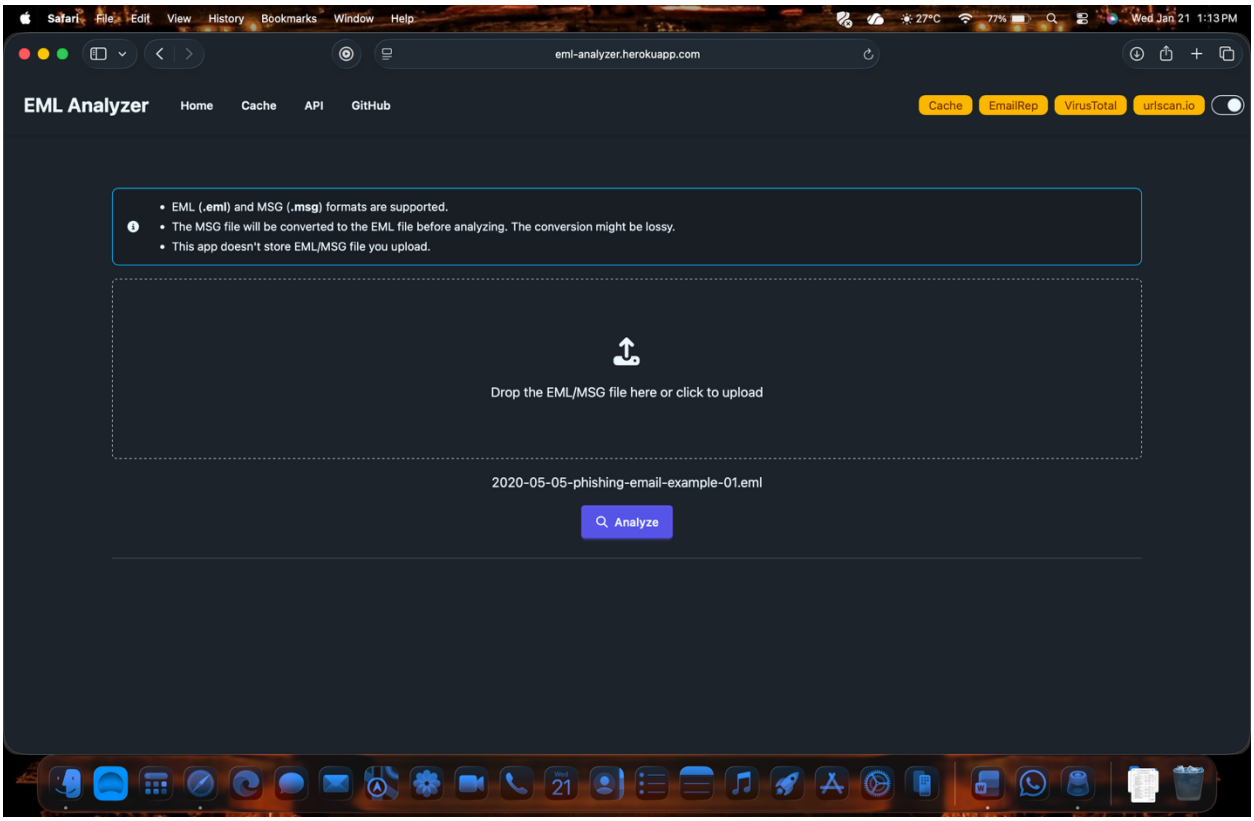
23BD1A052Q HARI VIGNESH RAO

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

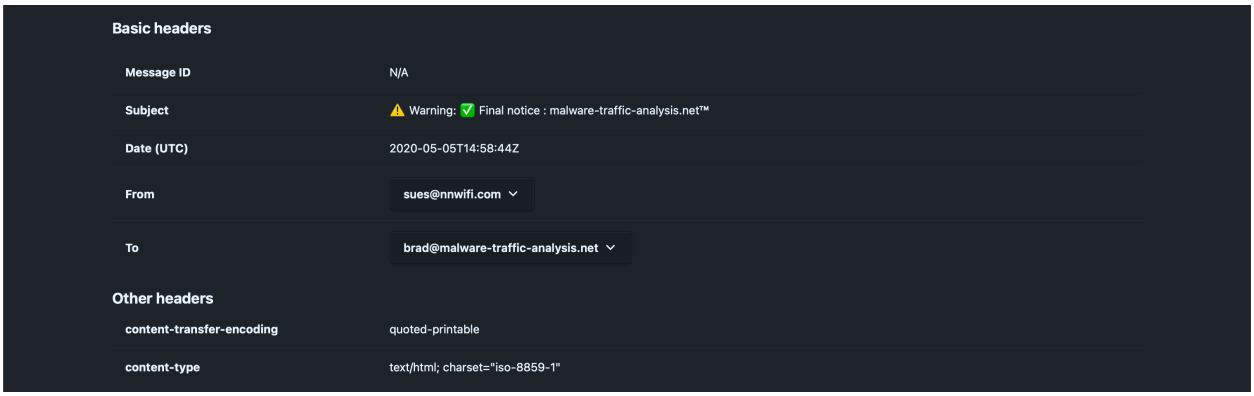
The file 2020-05-05-phishing-email-example-01.eml was uploaded to the EML Analyzer.



EML Analyzer Results:

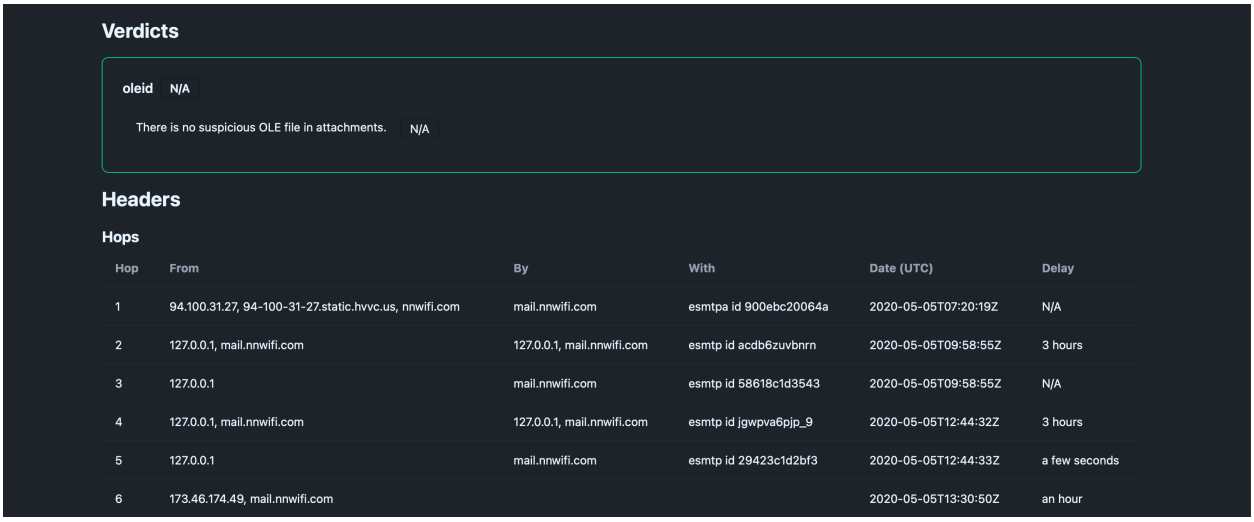
Key Observations:

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

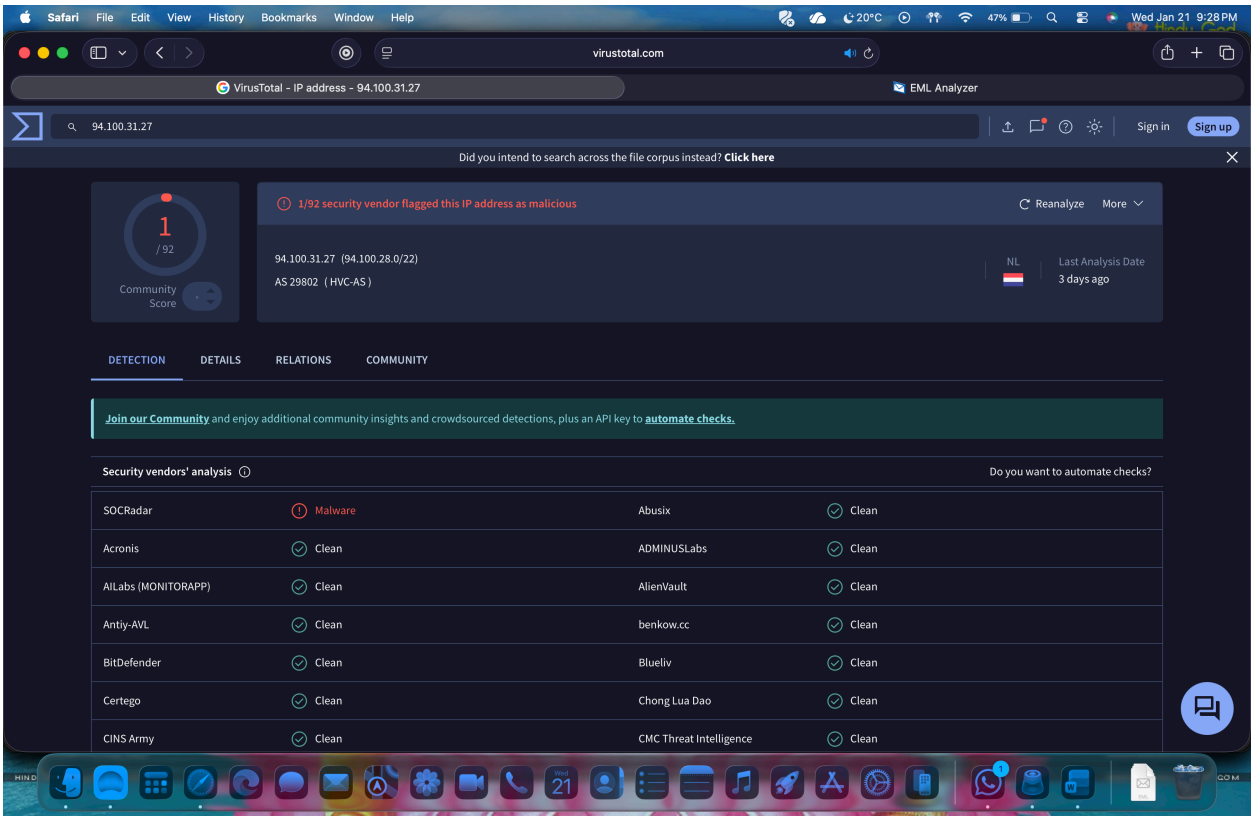


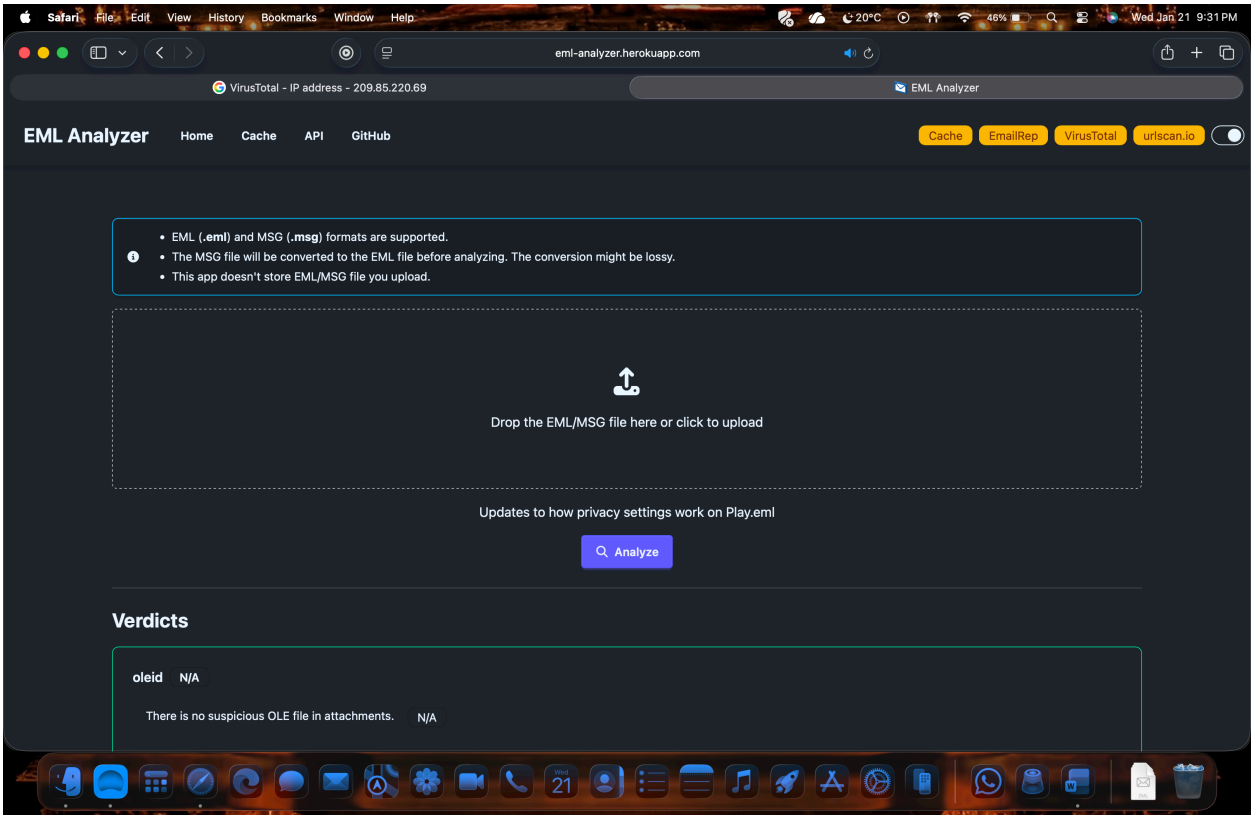
Header Analysis:

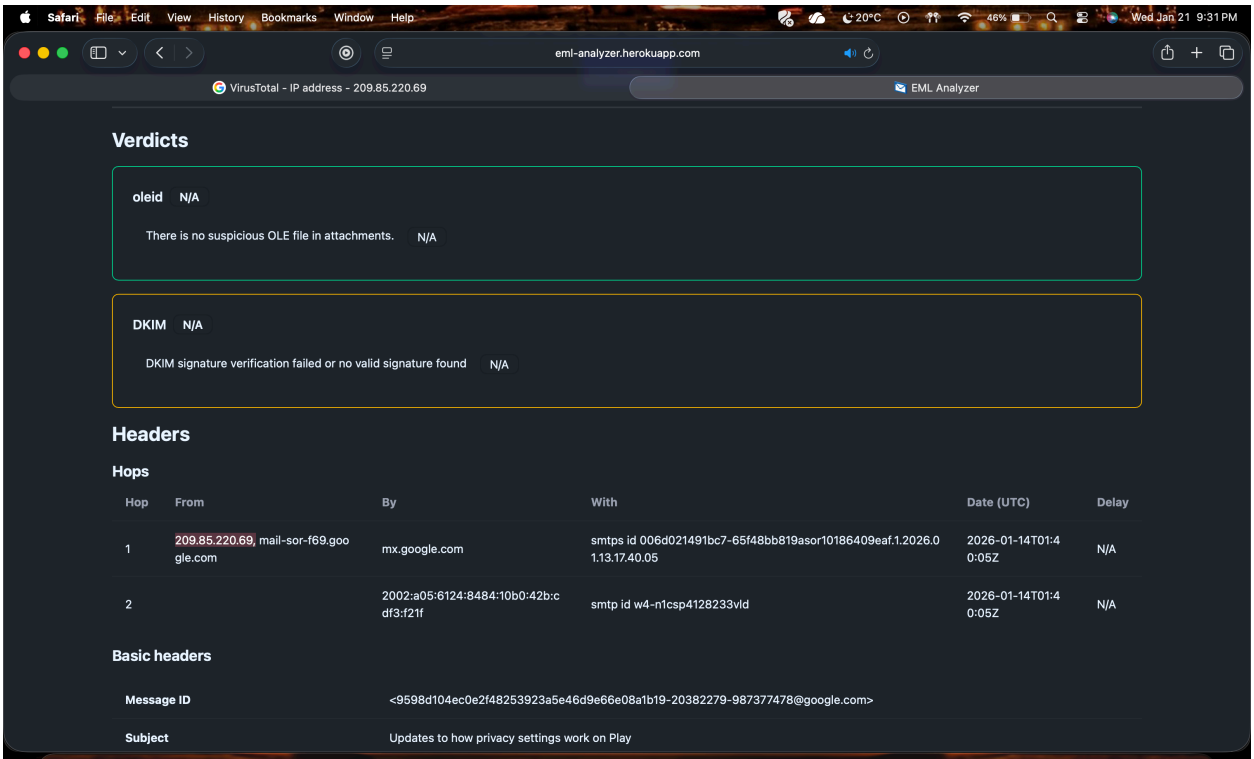
- Sender IP: 94.100.31.27
- Reverse DNS: 94-100-31-27.static.hvvc.us
- Mail Server: mail.nnwifi.com

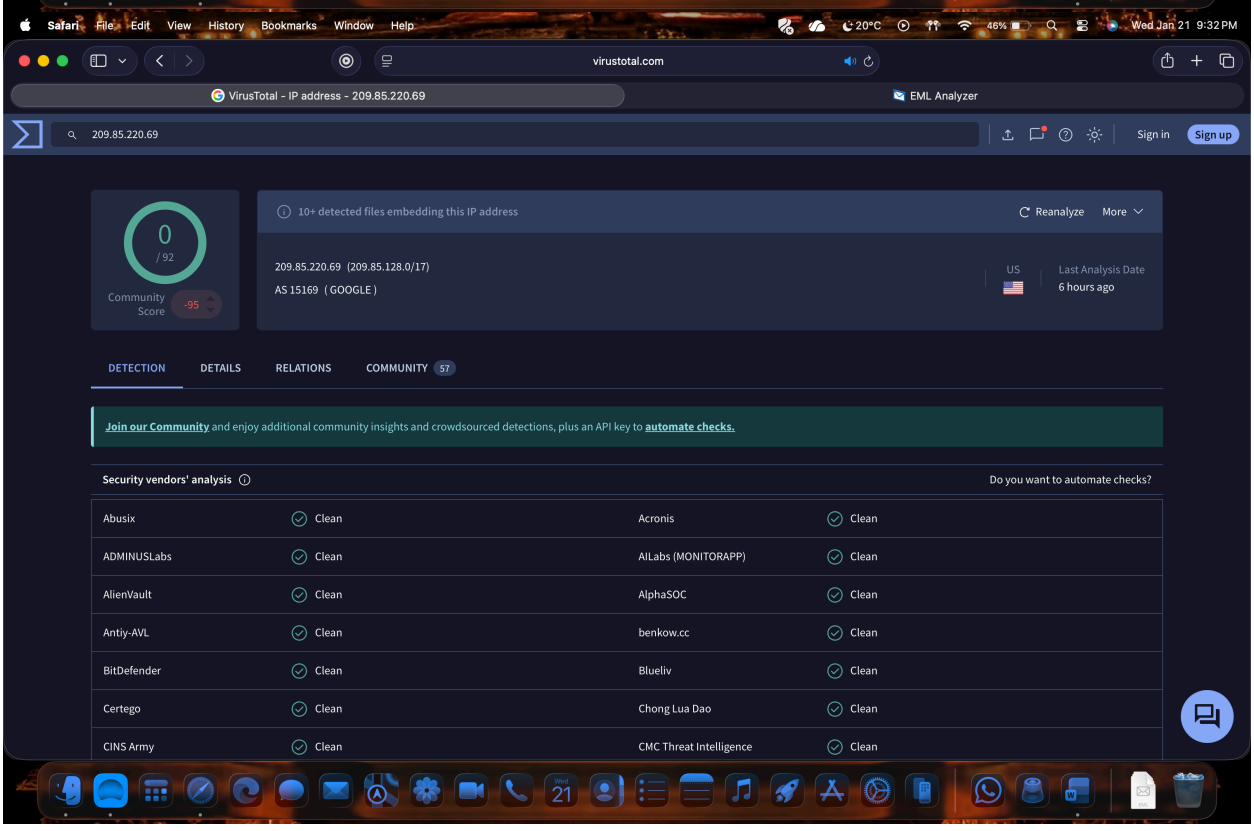


Hop	From	By	With	Date (UTC)	Delay
1	94.100.31.27, 94-100-31-27.static.hvvc.us, nnwifi.com	mail.nnwifi.com	esmtpa id 900ebc20064a	2020-05-05T07:20:19Z	N/A
2	127.0.0.1, mail.nnwifi.com	127.0.0.1, mail.nnwifi.com	esmtp id acdb6zuvbnrn	2020-05-05T09:58:55Z	3 hours
3	127.0.0.1	mail.nnwifi.com	esmtp id 58618c1d3543	2020-05-05T09:58:55Z	N/A
4	127.0.0.1, mail.nnwifi.com	127.0.0.1, mail.nnwifi.com	esmtp id jgwpva6pjp_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
VirusTotal - IP address - 94.100.31.27
EML Analyzer
94.100.31.27
Sign in
Sign up
Did you intend to search across the file corpus instead? Click here
1 / 92
Community Score
1/92 security vendor flagged this IP address as malicious
Reanalyze
More
94.100.31.27 (94.100.28.0/22)
AS 29802 (HVC-AS)
NL
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
Do you want to automate checks?
SOCRadar Malware
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (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

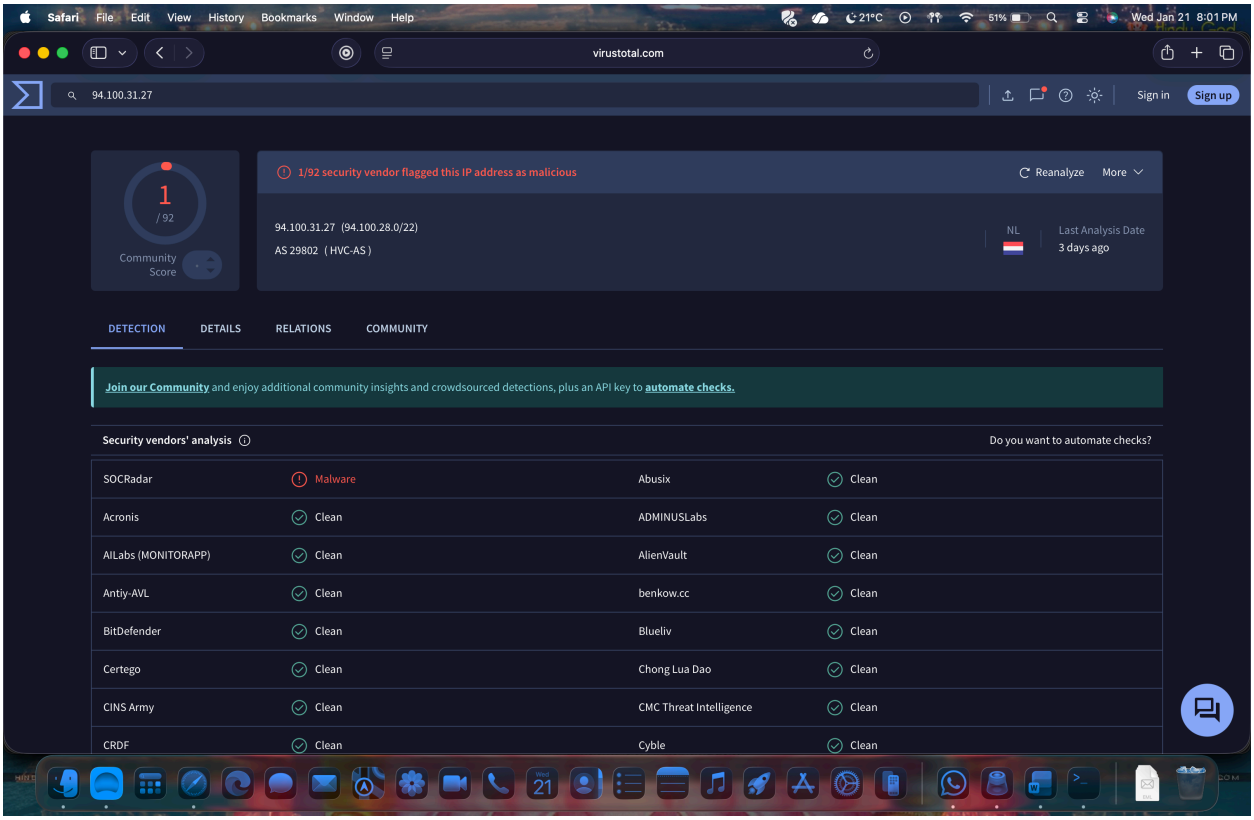

Safari File Edit View History Bookmarks Window Help
eml-analyzer.herokuapp.com
VirusTotal - IP address - 209.85.220.69
EML Analyzer
EML Analyzer
Home
Cache
API
GitHub
Cache
EmailRep
VirusTotal
urlscan.io
EML (.eml) and MSG (.msg) formats are supported.
The MSG file will be converted to the EML file before 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


Safari File Edit View History Bookmarks Window Help
Wed Jan 21 9:31 PM
eml-analyzer.herokuapp.com
VirusTotal - IP address - 209.85.220.69
EML Analyzer
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.1.2026.01.13.17.40.05 2026-01-14T01:40:05Z N/A
2 2002:a05:6124:8484:10b0:42b:cdf3:f21f smtp id w4-n1csp4128233vld 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
Wed Jan 21 9:32 PM
virustotal.com
VirusTotal - IP address - 209.85.220.69
EML Analyzer
209.85.220.69
Sign in
Sign up
0 / 92
Community Score -95
10+ detected files embedding this IP address
Reanalyze
More
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
Do you want to automate checks?
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (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

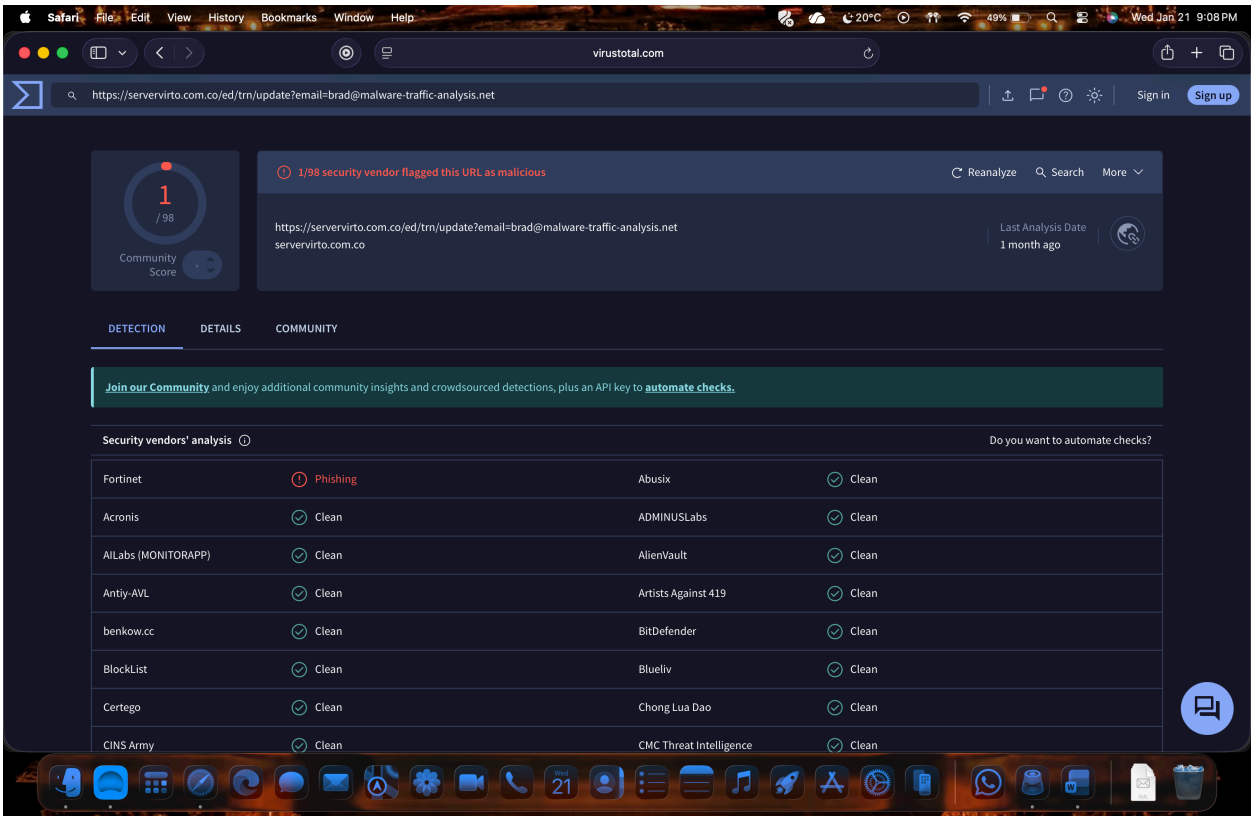
Part B: VirusTotal Analysis

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.

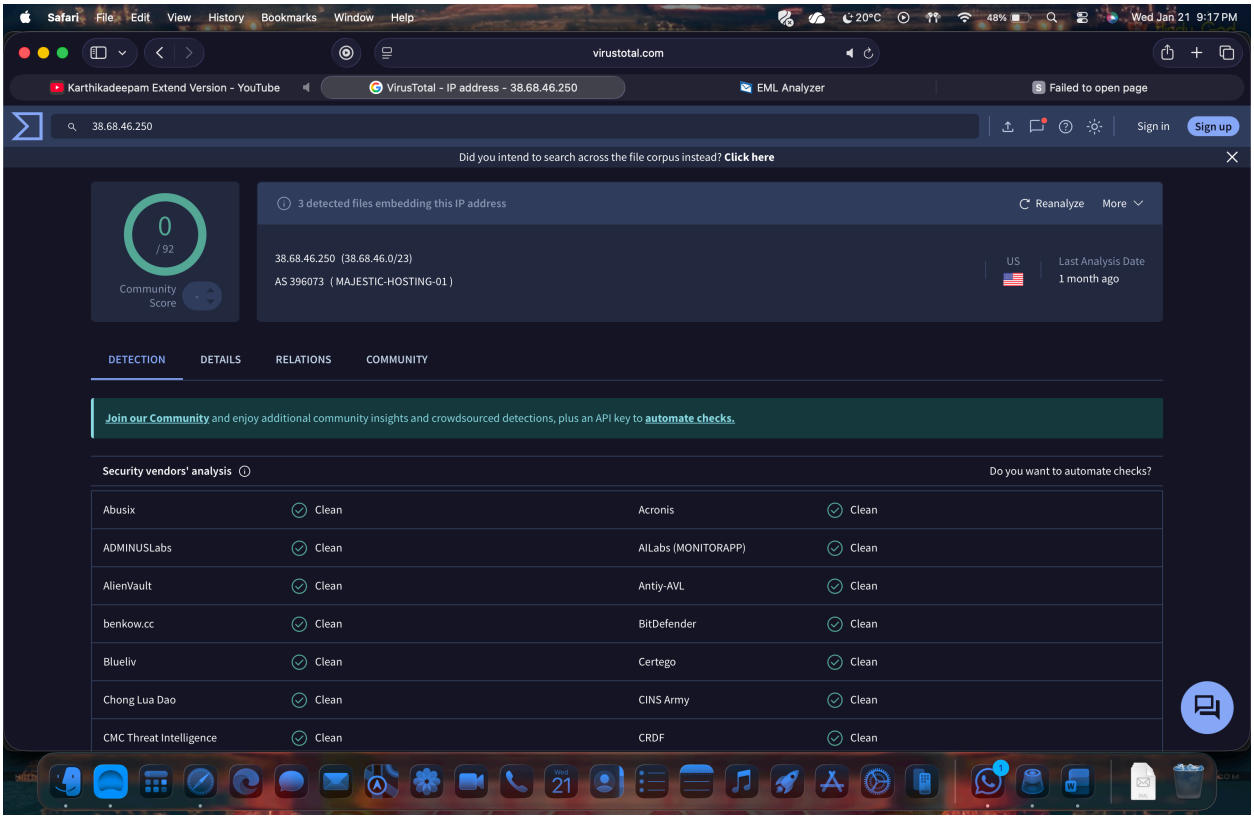


Suspicious Link Identified

From EML Analyzer, the following URL was extracted:
https://servervirto.com.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)


Safari File Edit View History Bookmarks Window Help
20°C 49% Wed Jan 21 9:08 PM
virustotal.com
https://servervirto.com.co/ed/trn/update?email=brad@malware-traffic-analysis.net
Sign in
Sign up
1
/ 98
Community Score
1/98 security vendor flagged this URL as malicious
Reanalyze
Search
More
https://servervirto.com.co/ed/trn/update?email=brad@malware-traffic-analysis.net
servervirto.com.co
Last Analysis Date
1 month ago
DETECTION
DETAILS
COMMUNITY
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?
Fortinet Phishing
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
Antiy-AVL Clean
Artists Against 419 Clean
benkow.cc Clean
BitDefender Clean
BlockList Clean
Blueliv Clean
Certego Clean
Chong Lua Dao Clean
CINS Army Clean
CMC Threat Intelligence Clean

Not Suspicious Ip Address



Not Suspicious Link