

Experiment: Analyzing Phishing Emails

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

Tools Used:

- Online EML Analyzer
- VirusTotal
- Sample file: 2020-05-05-phishing-email-example-01.eml

Questions to Answer:

1. What is the full email address of the sender?
2. What domain is used to send this email?
3. What is the sender's IP address from the header?
4. Is the sender IP blacklisted?
5. What is the result of SPF authentication?
6. What is one suspicious URL found in the email body?

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: malware-traffic-analysis.net Support 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

Authentication:

- SPF: Failed
- DKIM: Not signed
- DMARC: Not aligned

Part B: VirusTotal Analysis

The sender IP 94.100.31.27 was checked on VirusTotal.

VirusTotal Result:

- Detection Ratio: 1 / 93 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)

Answers to Given Questions

1. Full sender email address: sues@nnwifi.com
2. Domain used to send the email: nnwifi.com
3. Sender's IP address: 94.100.31.27
4. Is sender IP blacklisted? :Yes (1/93 vendors flagged it as malicious in VirusTotal)
5. SPF authentication result: Fail

6. One suspicious URL in email body:

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

Conclusion:-

Phishing indicators found:

- Urgent subject: "Warning: Final Notice"
- Fake display name pretending to be malware-traffic-analysis.net
- Actual sender domain is unrelated (nnwifi.com)
- SPF authentication failed
- Message-ID missing
- HTML-only email
- Suspicious external link
- IP partially flagged by VirusTotal

Final Verdict:-

This email is classified as PHISHING.