Phishing Email Investigation & IOC Analysis

Project Overview

This project demonstrates a real-world phishing email investigation workflow followed by a Security Operations Center (SOC) analyst.
The objective is to identify malicious indicators, analyze email authentication failures, uncover hidden URL redirections, and validate threats using industry-standard security tools — without directly interacting with malicious content.

This mirrors how phishing alerts are triaged, investigated, and escalated in an operational SOC environment.

Objectives

- Detect phishing characteristics based on email content and urgency
- Extract and analyze email headers
- Identify authentication failures (SPF, DKIM, DMARC)
- Safely analyze URLs without visiting them
- Detect hidden redirections
- Validate indicators of compromise (IOCs) using threat intelligence platforms
- Produce SOC-ready findings and documentation

Tools & Platforms Used

Category	Tools
➢ Email Client	✓ Microsoft Outlook
➢ Raw Email Analysis	✓ Notepad++
➢ Header Analysis	✓ mailheader.org
➢ URL Screenshot	✓ URL2PNG
➢ URL Redirection & Behavior	✓ urlscan.io
➢ Threat Intelligence	✓ VirusTotal

Investigation Methodology

Step 1: Initial Email Review (Outlook)

- Opened the email only to review the content
- Observed the following suspicious characteristics:
    - Spelling and grammatical mistakes
    - Urgent language demanding immediate action
    - Psychological pressure tactics commonly used in phishing emails
- No links or attachments were clicked during this phase

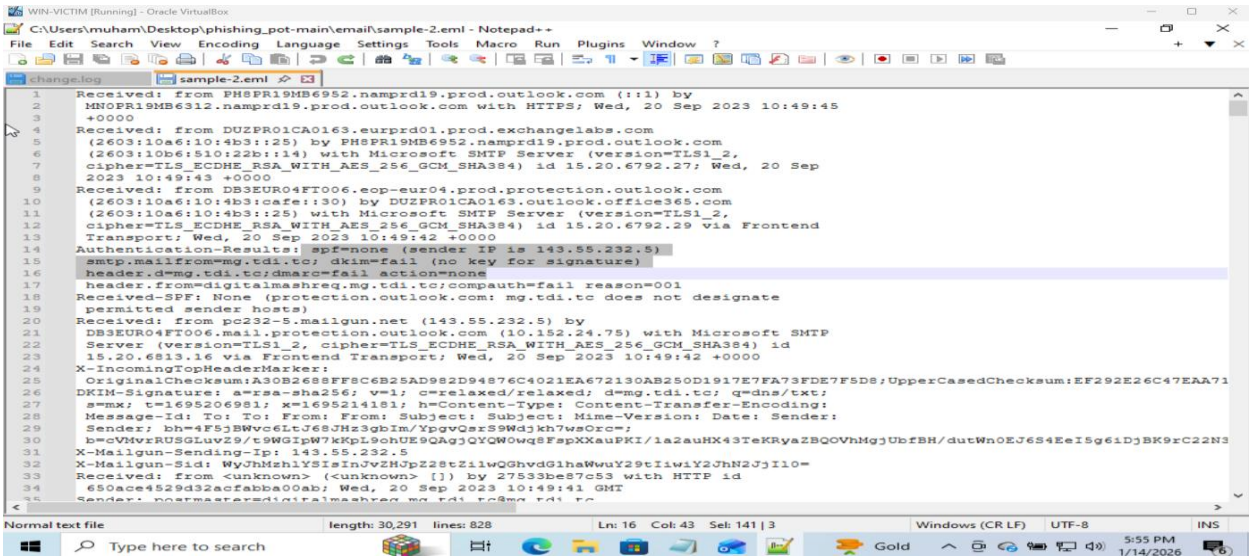
Initial suspicion of phishing was raised due to urgency and poor language quality.

Step 2: Raw Email Examination (Notepad++)

- Opened the raw email source using Notepad++
- Identified multiple email authentication failures:

SPF: none (FAIL)
DKIM: fail (no key for signature)
DMARC: fail
CompAuth: fail

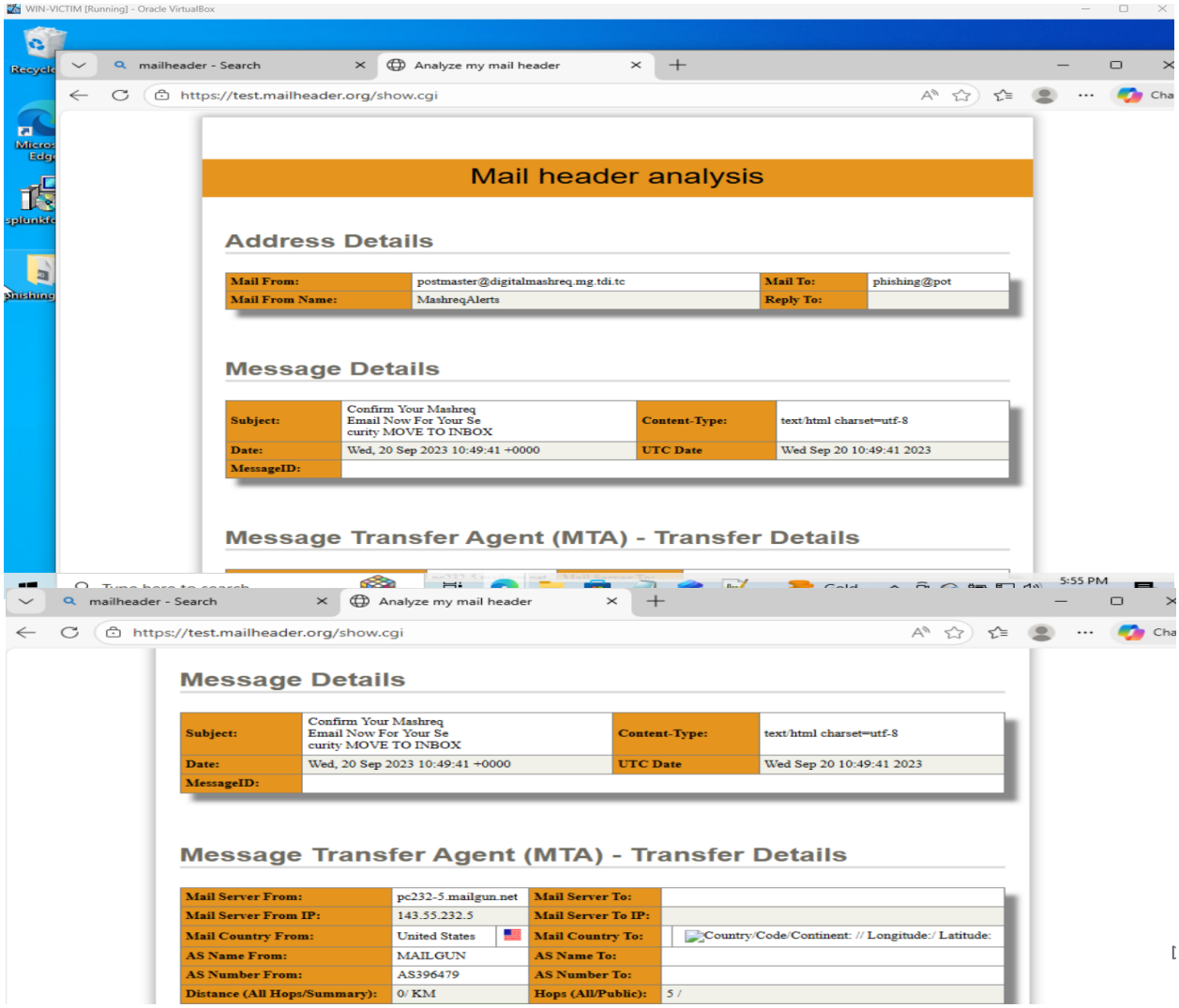
Multiple authentication failures strongly indicate email spoofing or unauthorized sending infrastructure.



Step 3: Email Header Analysis

- Uploaded the complete email headers to mailheader.org
- Extracted and analyzed:
    - Sender IP address
    - Sending mail server information
    - Geolocation of the sender IP
    - Full mail routing path

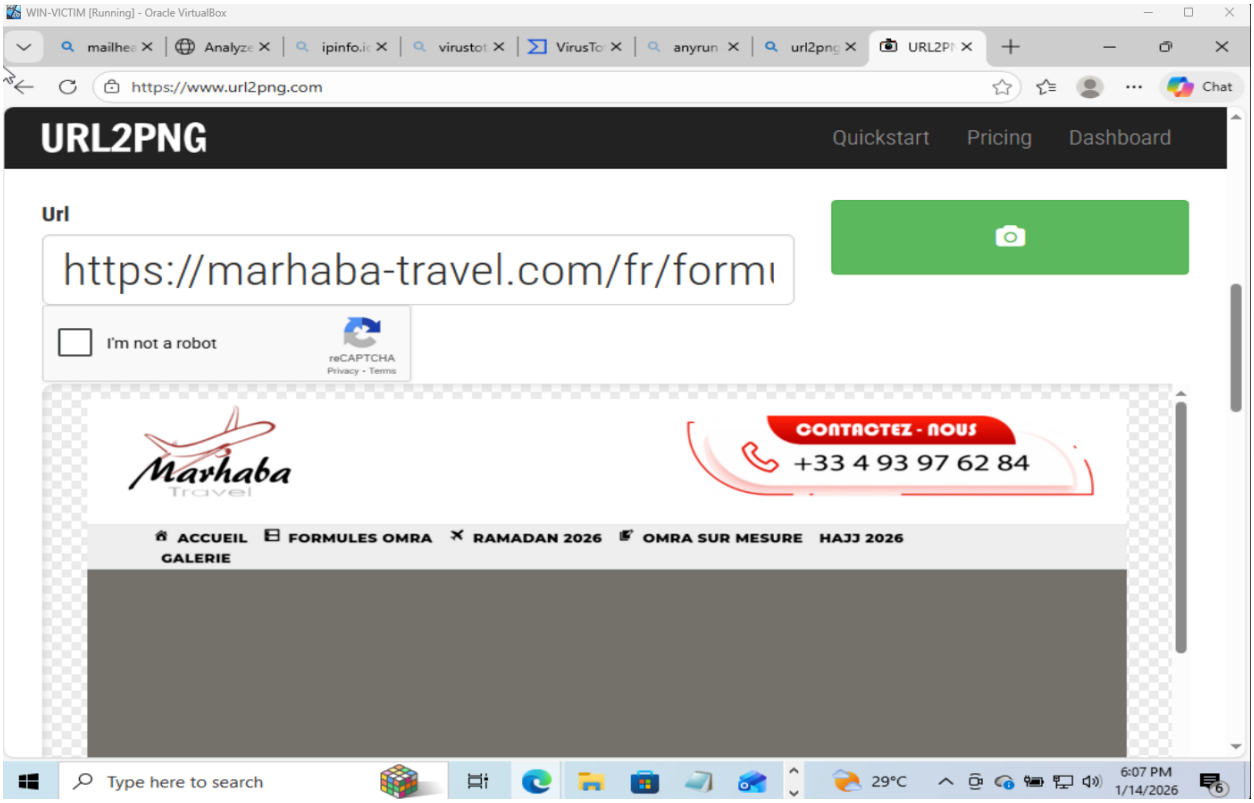
The sender IP origin did not align with the organization claimed in the email, further confirming spoofing.



Step 4: URL Safety Preview (URL2PNG)

- Used URL2PNG to capture a screenshot of the suspicious webpage
- Ensured:
    - No direct interaction with the live website
    - Visual inspection only

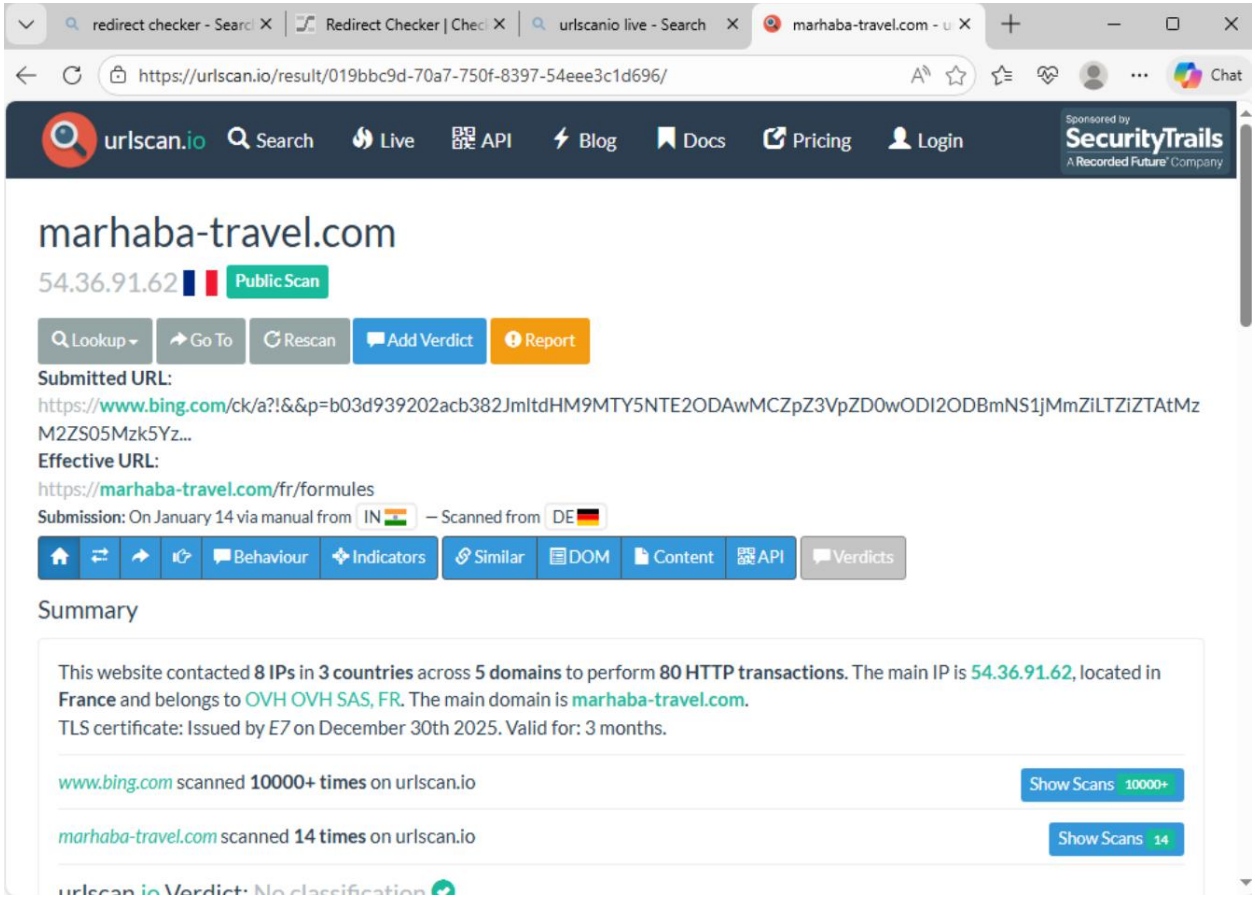
The webpage appearance suggested impersonation or a non-legitimate service.



Step 5: Redirect and Behavior Analysis (urlscan.io)

- Submitted the suspicious URL to urlscan.io
- Observed:
    - A hidden redirection chain
    - Final landing domain unrelated to the claimed sender
    - Suspicious JavaScript and redirect behavior

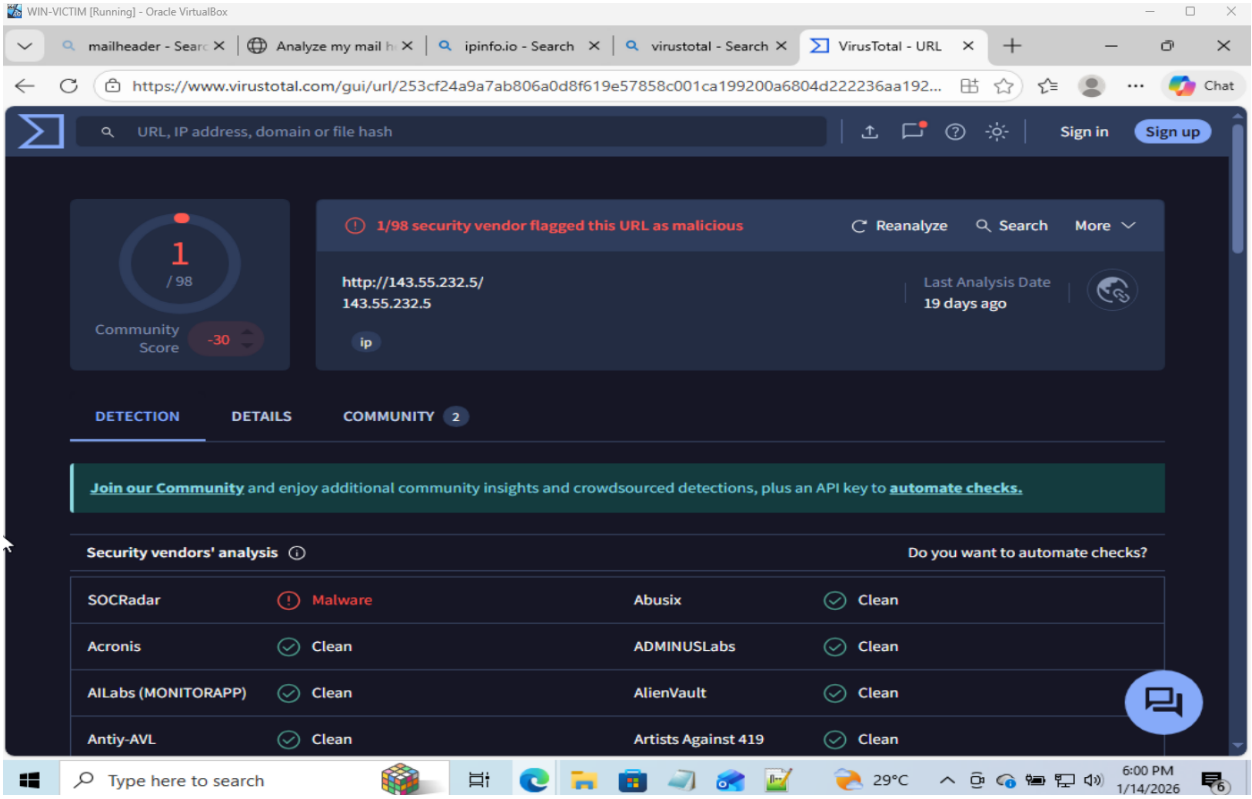
This confirmed that URL redirection was used to disguise the final malicious destination.

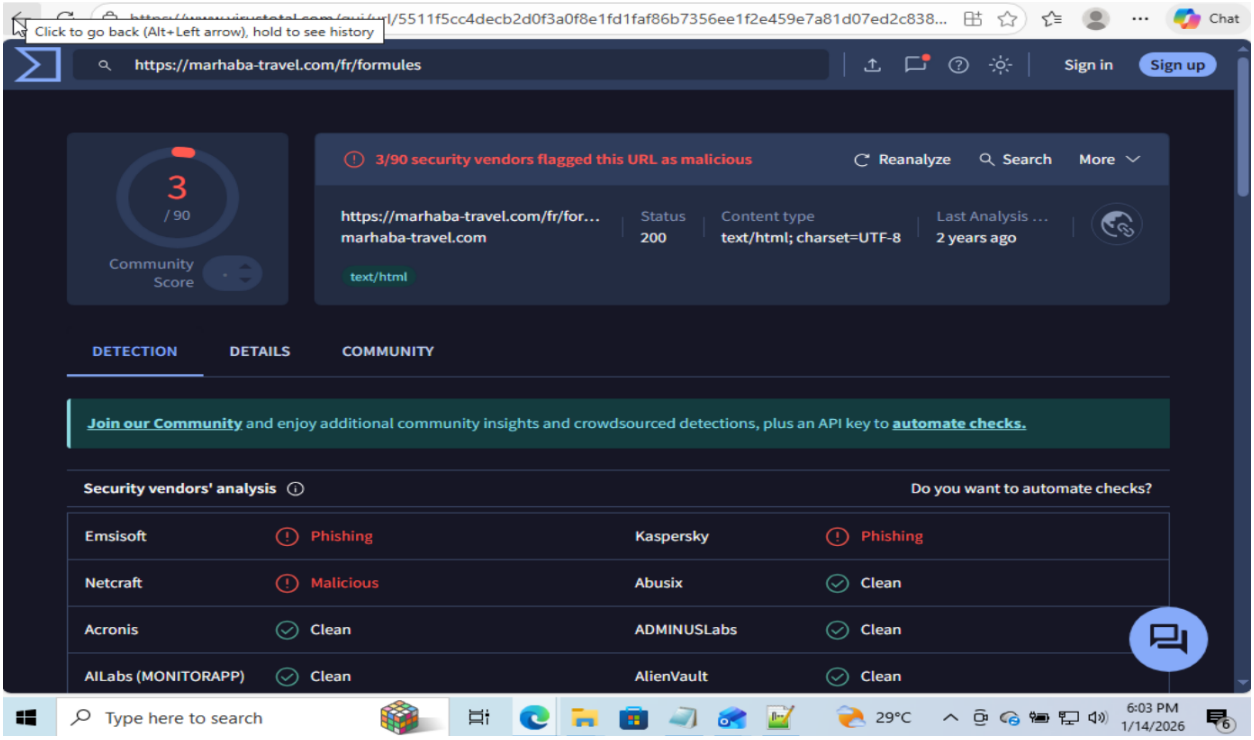


Step 6: Threat Intelligence Validation (VirusTotal)

- Analyzed:
    - Sender IP reputation
    - Redirected and final destination URLs
- Results showed:
    - Multiple detections from security vendors
    - Classification as malicious or phishing

Threat activity was confirmed using external threat intelligence sources.





💉 Indicators of Compromise (IOCs) —

🌐 Network & Infrastructure IOCs

Type	Value
➢ Sender IP	✓ 143.55.232.5
➢ Sending Host	✓ pc232-5.mailgun.net
➢ Mail Service	✓ Mailgun

🌎 Domain IOCs

Type	Value
➢ Spoofed From Domain	✓ digitalmashreq.mg.tdi.tc
➢ Mail Domain	✓ mg.tdi.tc
➢ Redirect Domain	✓ bing.com
➢ Final Malicious Domain	✓ marhaba-travel.com

🔗 URL IOCs

Type	Value
➢ Malicious URL	✓ http://marhaba-travel.com/fr/formules

📧 Email Header IOCs

Type	Value
➢ From Address	✓ postmaster@digitalmashreq.mg.tdi.tc
➢ Return-Path	✓ bounce+…@mg.tdi.tc
➢ Message-ID	✓ 20230920104941.05fa86daa715a6e3@mg.tdi.tc

Final Assessment

Threat Type: Phishing
Risk Level: High

Attack Techniques Identified

- Email spoofing
- Redirect-based URL obfuscation
- Social engineering using urgency

Potential Impact

- Credential harvesting
- Account takeover
- Possible malware delivery

SOC Response & Recommendations

- Block sender IP address and domains at the email gateway
- Blacklist malicious URLs and redirect domains
- Conduct user awareness training on urgency-based phishing attacks
- Enforce strict SPF, DKIM, and DMARC policies
- Monitor for similar phishing indicators and patterns within the SIEM

Disclaimer

All analysis was performed using passive investigation techniques in a controlled environment. No malicious links, attachments, or payloads were executed.