

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:

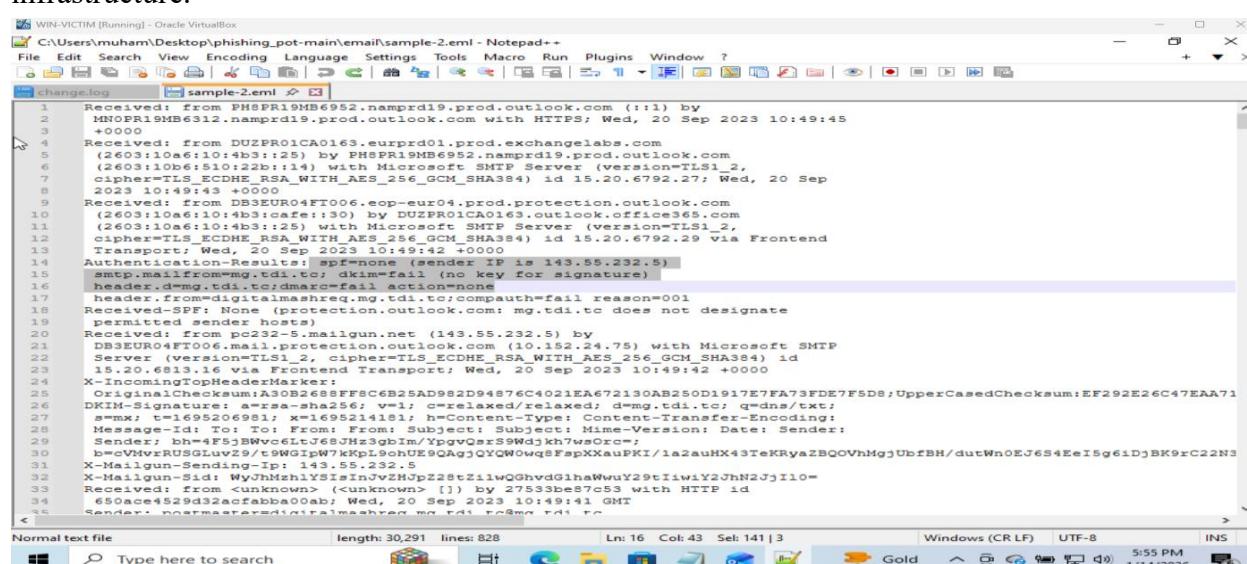
SPF: none (FAIL)

DKIM: fail (no key for signature)

DMARC: fail

CompAuth: fail

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



```
WIN-VICTIM [Running] - Oracle VirtualBox
C:\Users\muham\Desktop\phishing_pot-main\email\sample-2.eml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
[File] [Edit] [Search] [View] [Encoding] [Language] [Settings] [Tools] [Macro] [Run] [Plugins] [Window]
sample-2.eml
change.log
Received: from PHSPR19MB6952.namprd19.prod.outlook.com (:) by
 20 Sep 2023 10:49:45 +0000
Received: from DUZPRO1CA0163.eurprd01.prod.exchangelabs.com
  (2603:10a6:10:4b3::25) by PHSPR19MB6952.namprd19.prod.outlook.com
  (2603:10b6:510:22b::114) with Microsoft SMTP Server (version=TLS1_2,
  cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.27; Wed, 20 Sep
  2023 10:49:45 +0000
Received: from D83EURO4FT006.ecp-euro04.prod.protection.outlook.com
  (2603:10a6:10:4b3::130) by D83EURO4FT006.ecp-euro04.prod.protection.outlook.com
  (2603:10a6:10:4b3::25) with Microsoft SMTP Server (version=TLS1_2,
  cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.29 via Frontend
  Transport; Wed, 20 Sep 2023 10:49:42 +0000
Transport-Results: :spf:none (sender IP is 143.55.232.5)
smtp.mailfrom=mg.tdi.td; dkim=fail (no key for signature)
X-Header-Name: mg.tdi.td
header_from=digitalmashreq.mg.tdi.td; compauth=fail reason=001
Received-SPF: None (protection.outlook.com: mg.tdi.td does not designate
  permitted sender hosts)
Received: from pc32-5.mailgun.net (143.55.232.5) by
  DB3EURO4FT006.mail.protection.outlook.com (10.152.24.75) with Microsoft SMTP
  Server (version=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
  15.20.6813.1; via Frontend Transport; Wed, 20 Sep 2023 10:49:42 +0000
X-IncomingTopHeaderMarker:
OriginalChecksum:A30B2687FF8C6B25AD982D94876C4021EA672130AB250D1917E7FA73FDE7F5D8;UpperCasedChecksum:EF292E26C47EAA71
DKIM-Signature: a=xrsa-sha256; v=1; c=relaxed/relaxed; d=mg.tdi.td; q=dns/txt;
s=mx; t=1695206981; x=1695214181; h=Content-Type: Content-Transfer-Encoding:
Message-ID: To: From: Subject: Subject: Mime-Version: Date: Sender:
Subject: X-Mailer: X-Mailgun-Sending-IP: 143.55.232.5
X-Mailgun-Sid: WyJhMzhlySISinJvZHUpZ2stZ1lwQghvdG1haWwUY29tIlwiY2JhN2JjI10-
Received: from <unknown> (<unknown>) [] by 27533be87c53 with HTTP id
650ace529d32acfbabao0ab; Wed, 20 Sep 2023 10:49:41 GMT
Sender: postmaster@digitalmashreq.mg.tdi.td
```

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.

The image displays two side-by-side screenshots of the mailheader.org analysis interface. Both screenshots show the same three sections: Address Details, Message Details, and Transfer Details.

Address Details:

Mail From:	postmaster@digitalmashreq.mg.tdi.tc	Mail To:	phishing@pot
Mail From Name:	MashreqAlerts	Reply To:	

Message Details:

Subject:	Confirm Your Mashreq Email Now For Your Security MOVE TO INBOX	Content-Type:	text/html charset=utf-8
Date:	Wed, 20 Sep 2023 10:49:41 +0000	UTC Date:	Wed Sep 20 10:49:41 2023
MessageID:			

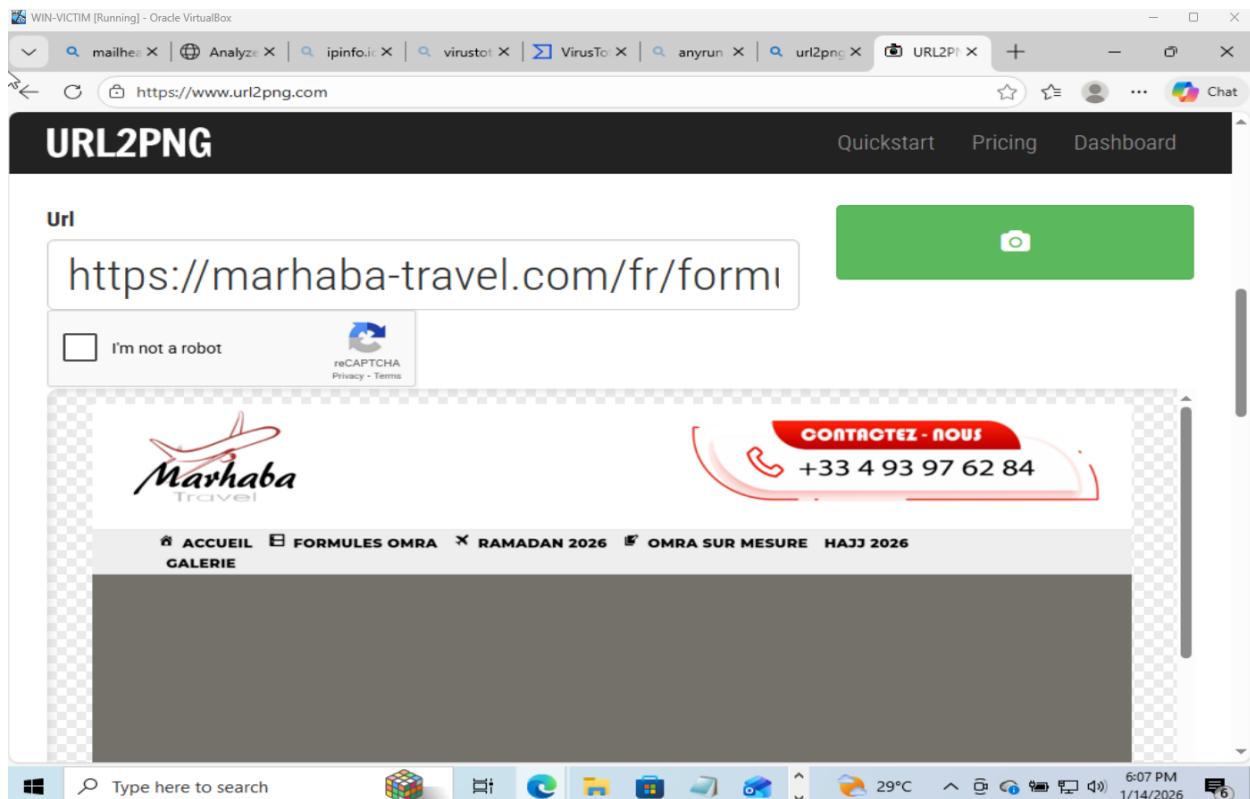
Transfer Details:

Mail Server From:	pc232-5.mailgun.net	Mail Server To:	
Mail Server From IP:	143.55.232.5	Mail Server To IP:	
Mail Country From:	United States	Mail Country To:	Country/Code/Continent: // Longitude: / Latitude:
AS Name From:	MAILGUN	AS Name To:	
AS Number From:	AS396479	AS Number To:	
Distance (All Hops/Summary):	0/ KM	Hops (All/Public):	5 /

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.

The screenshot shows the urlscan.io analysis page for the domain marhaba-travel.com. The main header displays the IP address 54.36.91.62 and the status Public Scan. Below the header, there are several navigation and action buttons: Lookup, Go To, Rescan, Add Verdict, and Report. The page displays the submitted URL (<https://www.bing.com>) and the effective URL (<https://marhaba-travel.com/fr/formules>). It also shows the submission details: On January 14 via manual from India (IN) and scanned from Germany (DE). A summary section indicates that the website contacted 8 IPs in 3 countries across 5 domains to perform 80 HTTP transactions. The main IP is 54.36.91.62, located in France and belongs to OVH OVH SAS, FR. The main domain is marhaba-travel.com. The TLS certificate was issued by E7 on December 30th 2025, valid for 3 months. Below this, two specific scans are listed: www.bing.com scanned 10000+ times and marhaba-travel.com scanned 14 times. The urlscan.io Verdict is No classification.

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.

The screenshot shows the VirusTotal URL analysis interface. At the top, there's a navigation bar with tabs for 'mailheader - Search', 'Analyze my mail', 'ipinfo.io - Search', 'virustotal - Search', and 'VirusTotal - URL'. The 'VirusTotal - URL' tab is active. Below the bar, the URL <https://www.virustotal.com/gui/url/253cf24a9a7ab806a0d8f619e57858c001ca199200a6804d222236aa192...> is displayed. The main content area shows a summary card with a 'Community Score' of 1 / 98 and a 'Last Analysis Date' of 19 days ago. A message indicates that 1/98 security vendor flagged the URL as malicious. Below this, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'COMMUNITY' tab is selected, showing a call-to-action to 'Join our Community'. Under 'Security vendors' analysis', the following results are listed:

Vendor	Result	Action
SOCRadar	Malware	Do you want to automate checks?
Acronis	Clean	Do you want to automate checks?
AI Labs (MONITORAPP)	Clean	Do you want to automate checks?
Antiy-AVL	Clean	Do you want to automate checks?
Abusix	Clean	Do you want to automate checks?
ADMINUSLabs	Clean	Do you want to automate checks?
AlienVault	Clean	Do you want to automate checks?
Artists Against 419	Clean	Do you want to automate checks?

At the bottom of the screen, the Windows taskbar shows the search bar, pinned icons for File Explorer, Edge, and File History, and system status indicators for battery level (6%), temperature (29°C), and date/time (6:00 PM, 1/14/2026).

Click to go back (Alt+Left arrow), hold to see history

https://marhaba-travel.com/fr/formules

3/90 security vendors flagged this URL as malicious

Community Score 3 / 90

Status 200 | Content type text/html; charset=UTF-8 | Last Analysis ... 2 years 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?	
Emsisoft	Phishing	Kaspersky	Phishing
Netcraft	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
Allabs (MONITORAPP)	Clean	AlienVault	Clean

Type here to search 6:03 PM 1/14/2026 6:03 PM 1/14/2026 6:03 PM 1/14/2026

💡 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.