Phishing Email Analysis BY P3NGU1N

Introduction to Phishing:

- type of attack to steal personal information
- phishing lies in delivery phase of CKC
- phishing is done by sending malicious content to victim using links
- Attacker gets the victim to click on links in mail by using tricky phrases and tricks user into thinking link is legitimate
- most common initial attack vector
- first step to infiltrate systems

Information Gathering:

Spoofing:

- because no authentication mechanisms
- protocols SPF, DKIM, DMARC have been created to prevent mail spoofing
- smtp address of mail should first be identifiable
- domains record can be obtained using tools MXtoolbox
- spoofing isnt the only way
- hacking mails of trusted companies and using them to send harmful files can also be done

E-mail Traffic Analysis

The following parameters can give us an idea of the size of the attack and the target audience if we perform a search on the mail gateway.

- Sender Address(info@letsdefend.io)
- SMTP IP Address(127.0.0.1)

- @letsdefend.io (domain base)
- letsdefend (In addition to the Gmail account, the attacker may have sent from the Hotmail account)
- Subject (sender address and SMTP address may be constantly changing)

- it is necessary to know the recipients' addresses and time information in the search results
- If malicious emails are constantly being forwarded to the same users, their email addresses may have somehow been leaked and shared on sites such as Paste Bin.
- Attackers can find email addresses using the Harvester tool on Kali Linux.

What is an Email Header?

contain info:

- sender
- recipient
- date
- reply-to
- received by

- allows u to identify the sender and receiver of a mail “to” and “From” fields
- this prevents people from receiving spam mails
- track mail route to see if it came from a legitimate server. email header information confirms the legitimacy of a server

Important Fields:

- FROM: name and address of sender
- TO: name and address of recipient also CC and BCC

- DATE: timestamp of when mail was sent

in gmail format used for date is: day dd mm yyyy hh:mm:ss

- SUBJECT: topic of email
- RETURN-PATH: (aka REPLY-TO)when u reply to a mail it returns to the mail in REPLY-TO field
- DOMAIN KEY & DKIM: (Domain key identifiable mail) : are email signatures that authenticate mails , helps email service providers identify the authenticity like SPF (SENDER POLICY FRAMEWORK)
- MESSAGE-ID: used to identify mail. its like a hash. every mail has a different message id which is a combination of number and letters
- MIME-VERSION (MULTIPURPOSE INTERNET MAIL EXTENTION): it is an internet coding standard. which converts non text content like videos, pics etc into text so it can be sent as an attachment via (smtp)
- RECEIVED: contains each mail server that email passed through in order to reach destination

it is in reverse chronological order means

Destination server

last-server before destination

-

-

first server (where mail originated from)

- X-SPAM STATUS: shows u the spam score of message

if SPAM: it will show spam score and threshold

if below threshold (normal email)

if it exceeds spam threshold (sent to spam folder)

How to access ur mail header:

1- open mail

2- download mail

3- open with notepad

Outlook

1- Open the email in question

2- File → Info → Properties → Internet headers

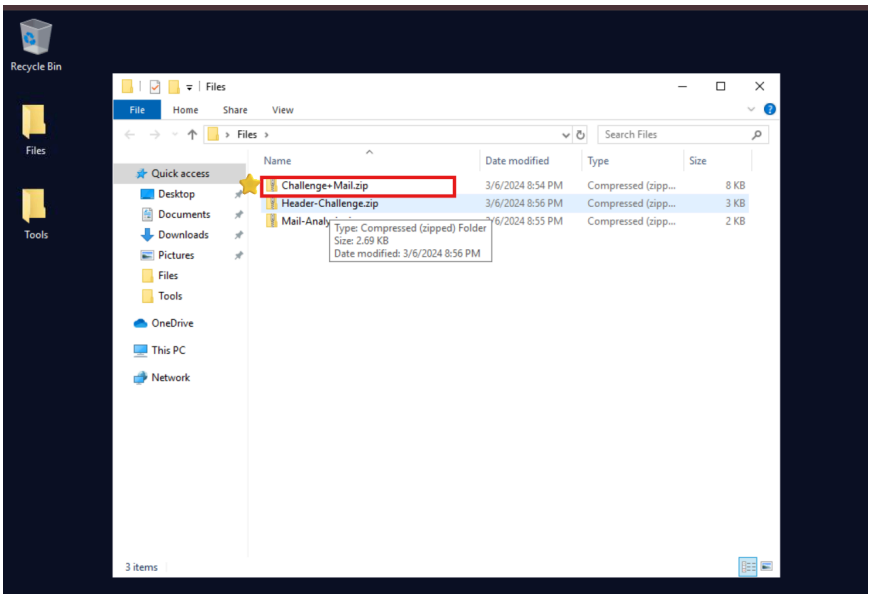
Note:

Use the "C:\Users\LetsDefend\Desktop\Files\Challenge+Mail.zip" file to solve the questions below.

File Password:

infected

STEP 1: OPEN this file with notepad++



🎯 **Question:**

If we wanted to respond to this email, what would be the recipient's address?

ANSWER: info@letsdefend.io

🎯 QUESTION:

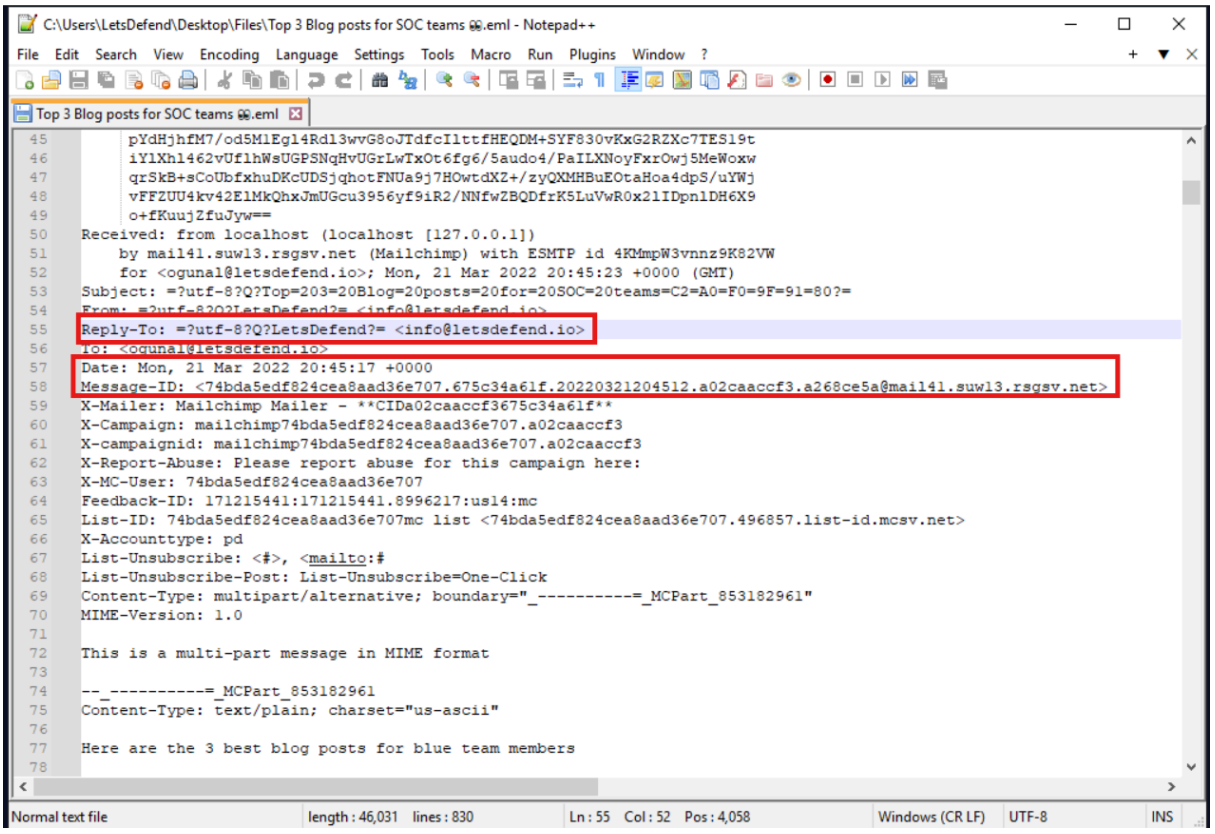
What year was the email sent?

ANSWER: 2022

🎯 QUESTION:

What is the Message-ID? (without > <)

ANSWER: 74bda5edf824cea8aad36e707.675c34a61f



Above Screenshot shows message id ,date, and reply-to mail address

Email Header Analysis

we need to able to analyze an email in order to mark it as phishing or safe

- smtp address?
- are ‘FROM’ & ‘REPLY-TO / RETURN-PATH’ same?

was email sent from correct smtp server:

- we will check received for that
- check legitimacy of ip and server
- us mxtoolbox.com

Are the 'From' and 'Return-Path / Reply-To' details the same?

- compare ‘from’ and ‘reply-to’ fields

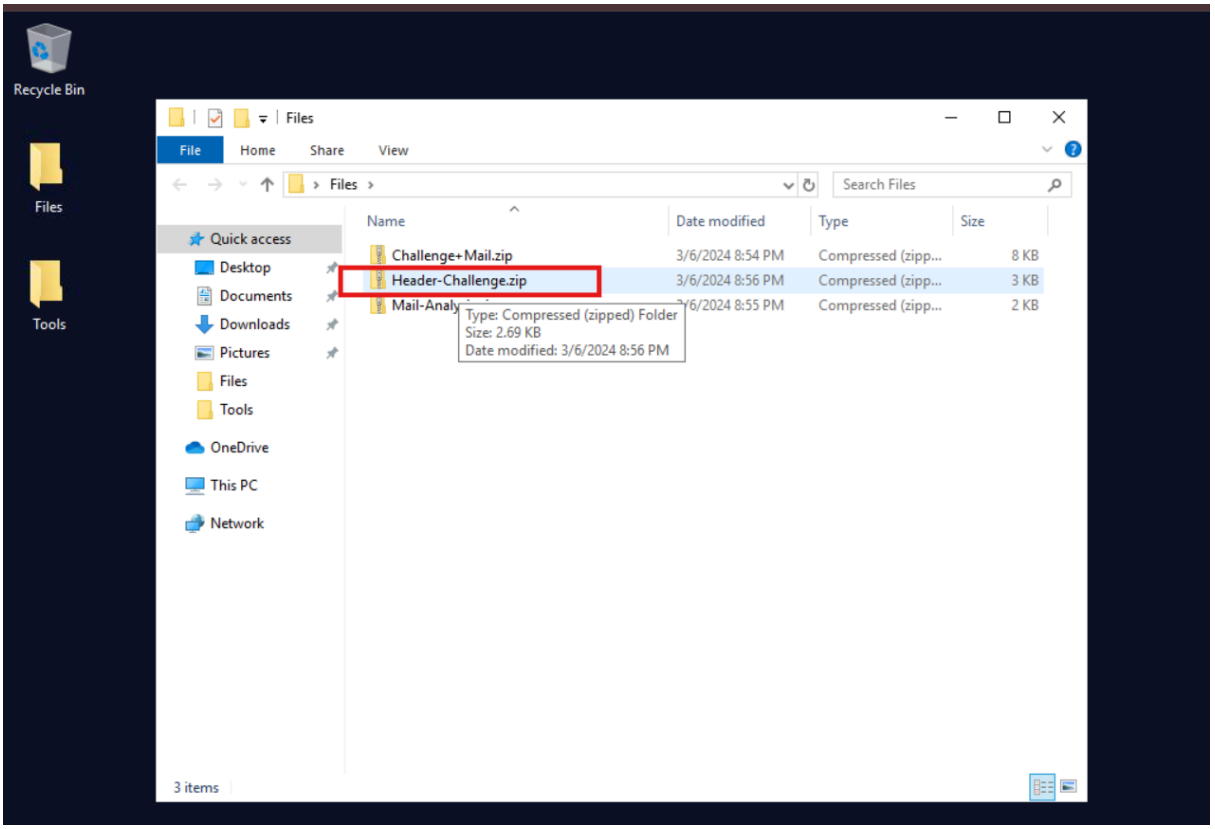
if they dont match might be phishing but not always

Note:

Use the "C:\Users\LetsDefend\Desktop\Files\Header-Challenge.zip" file to solve the questions below.

File Password:

infected



🎯 **Question:**

Are the sender’s address and the address in the “Reply-To” area different?

Answer :Y

🎯 **Question:**

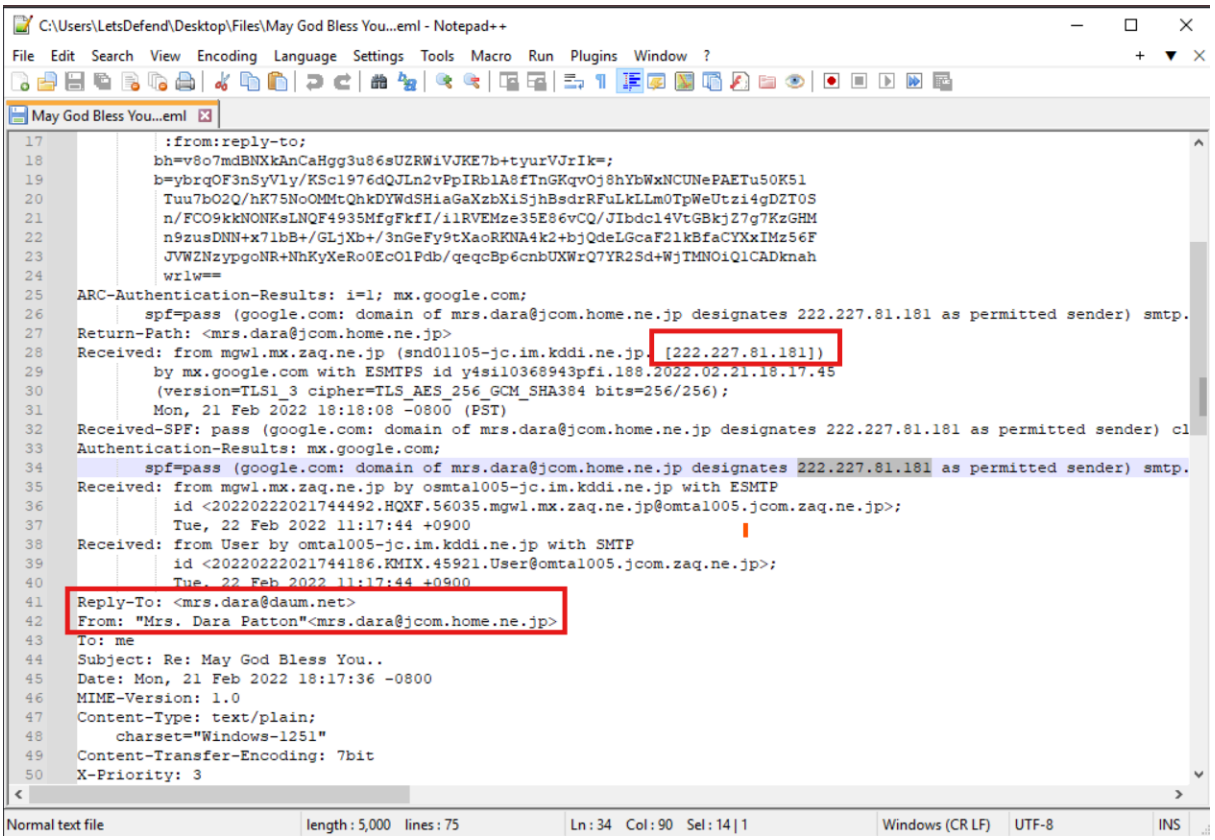
If I want to reply to this email, which address will it be sent to?

ANSWER: mrs.dara@daum.net

🎯 **Question:**

What IP address was the email sent from?

ANSWER: 222.227.81.181



- Above screenshot shows from and reply to mails are not same
- the ip of sender
- also the mail will be sent to the address in reply-to field

---

Static Analysis

- attacker could hide malicious sites behind buttons in html mails
- look for that and scan those urls using
- virus total and cisco talos intelligence

Dynamic Analysis

- inorder to see what those url do u need to check those urls in a safe environment like a sandbox

---

QUIZ

1.**At what stage of the Cyber Kill Chain are phishing attacks carried out?**

ANSWER: DELIVERY

2.**Where should you check to see if an email is spoofed?**

ANSWER: EMAIL HEADER

3.**Which protocol does not help you to determine whether an e-mail has been spoofed or not?**

ANSWER: UDP

4.**What does SMTP stand for?**

ANSWER: SIMPLE MAIL TRANSFER PROTOCOL

5.**Which of these are not part of the header of an e-mail?**

ANSWER: CHECK

6.**Which of the following cannot be achieved through a phishing attack?**

ANSWER: SQL INJECTION
