

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

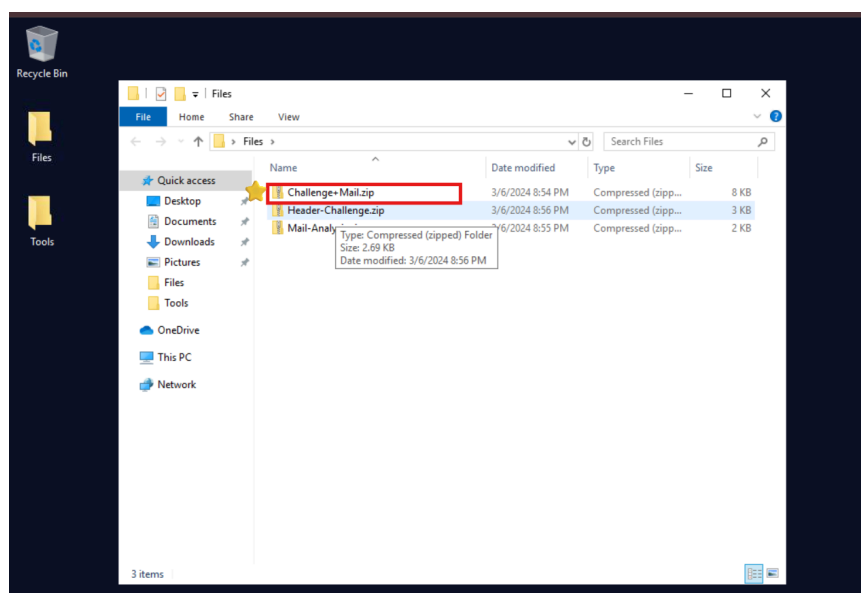
Note:

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

```
C:\Users\LetsDefend\Desktop\Files\Top 3 Blog posts for SOC teams .eml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Top 3 Blog posts for SOC teams .eml
45 pYdHjhFM7/od5M1Egl4Rdl3wvG8oJTdfcIlttfHEQDM+SYF830vKxG2R2Xc7TES19t
46 iYlXh1462vUf1hWuUGPSNqHvUGrLwTxOt6fg6/5audo4/PaILXNoyFxrOwj5MeWoxw
47 qrSkB+sCoUbfxhuDKcUDSjghotFNUa9j7H0wtdXZ+/zyQXMHBUeOtaHoa4dpS/uYWj
48 vFFZUU4kv42ElMkQhxJmUGcu3956yf9iR2/NNfwZBQDfrK5LuVwR0x2lIDpnlDH6X9
49 o+fKuuJZfuJyw==
50 Received: from localhost (localhost [127.0.0.1])
51 by mail41.suw13.rsgsv.net (Mailchimp) with ESMTP id 4KMmpW3vnnz9K82VW
52 for <ogunal@letsdefend.io>; Mon, 21 Mar 2022 20:45:23 +0000 (GMT)
53 Subject: =?utf-8?Q?Top=203=20Blog=20posts=20for=20SOC=20teams=C2=A0=F0=9F=91=80?=
54 From: =?utf-8?Q?LetsDefend?= <info@letsdefend.io>
55 Reply-To: =?utf-8?Q?LetsDefend?= <info@letsdefend.io>
56 To: <ogunal@letsdefend.io>
57 Date: Mon, 21 Mar 2022 20:45:17 +0000
58 Message-ID: <74bda5edf824cea8aad36e707.675c34a61f.20220321204512.a02caaccf3.a268ce5a@mail41.suw13.rsgsv.net>
59 X-Mailer: Mailchimp Mailer - **CIDA02caaccf3675c34a61f**
60 X-Campaign: mailchimp74bda5edf824cea8aad36e707.a02caaccf3
61 X-campaignid: mailchimp74bda5edf824cea8aad36e707.a02caaccf3
62 X-Report-Abuse: Please report abuse for this campaign here:
63 X-MC-User: 74bda5edf824cea8aad36e707
64 Feedback-ID: 171215441:171215441.8996217:us14:mc
65 List-ID: 74bda5edf824cea8aad36e707mc list <74bda5edf824cea8aad36e707.496857.list-id.mcsv.net>
66 X-Accounttype: pd
67 List-Unsubscribe: <#>, <mailto:#>
68 List-Unsubscribe-Post: List-Unsubscribe=One-Click
69 Content-Type: multipart/alternative; boundary="-----=_MCPart_853182961"
70 MIME-Version: 1.0
71
72 This is a multi-part message in MIME format
73
74 -----=_MCPart_853182961
75 Content-Type: text/plain; charset="us-ascii"
76
77 Here are the 3 best blog posts for blue team members
78
```

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

Email Header Analysis

we need to be 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

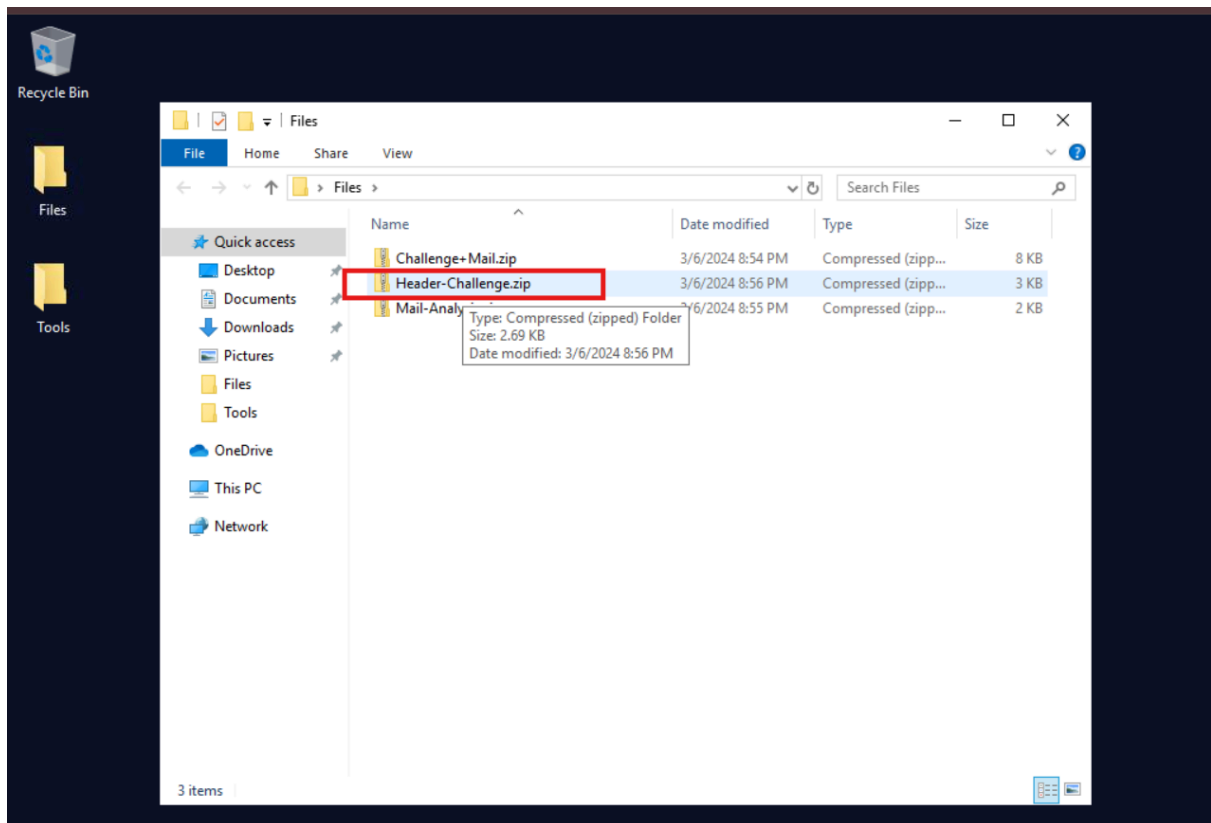
if they don't match might be phishing but not always

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

```
C:\Users\LetsDefend\Desktop\Files\May God Bless You...eml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
May God Bless You...eml
17      :from:reply-to;
18      bh=v8o7mdBNXkAnCaHgg3u86sUZRWiVJKE7b+tyurVJrIk=;
19      b=ybrqOF3nSyVly/KSc1976dQJLn2vPpIRb1A8fTnGKqvOj8hYbWxNCUNePAETu50K51
20      Tuu7b02Q/hK75NoOMMtQhkDYWdSHiaGaXzbXiSjhBedrRFuLkLLm0TpWeUtzi4gD2T0S
21      n/FC09kkNONKsLNQF4935MfgFkFI/1lRVEMze35E86vCQ/JIbdcl4VtGBKjZ7g7KzGHM
22      n9zusDNN+x7lbB+/GLjXb+/3nGeFy9tXaoRKNA4k2+bjQdeLGcaF21kBFaCYXxIMz56F
23      JVWZNzypgoNR+NhKyXeRo0EcOlPdb/qeqcBp6cnbUXWrQ7YR2Sd+WjTMNOiQ1CADknah
24      wrlw==
25  ARC-Authentication-Results: i=1; mx.google.com;
26      spf=pass (google.com: domain of mrs.dara@jcom.home.ne.jp designates 222.227.81.181 as permitted sender) smtp.
27  Return-Path: <mrs.dara@jcom.home.ne.jp>
28  Received: from mgwl.mx.zaq.ne.jp (snd01105-jc.im.kddi.ne.jp [222.227.81.181])
29      by mx.google.com with ESMTPS id y4sil0368943pfi.188.2022.02.21.18.17.45
30      (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
31      Mon, 21 Feb 2022 18:18:08 -0800 (PST)
32  Received-SPF: pass (google.com: domain of mrs.dara@jcom.home.ne.jp designates 222.227.81.181 as permitted sender) cl
33  Authentication-Results: mx.google.com;
34      spf=pass (google.com: domain of mrs.dara@jcom.home.ne.jp designates 222.227.81.181 as permitted sender) smtp.
35  Received: from mgwl.mx.zaq.ne.jp by omtal005-jc.im.kddi.ne.jp with ESMTP
36      id <20220222021744492.HQXF.56035.mgwl.mx.zaq.ne.jp@omtal005.jcom.zaq.ne.jp>;
37      Tue, 22 Feb 2022 11:17:44 +0900
38  Received: from User by omtal005-jc.im.kddi.ne.jp with SMTP
39      id <20220222021744186.RMIX.45921.User@omtal005.jcom.zaq.ne.jp>;
40      Tue, 22 Feb 2022 11:17:44 +0900
41  Reply-To: <mrs.dara@daum.net>
42  From: "Mrs. Dara Patton" <mrs.dara@jcom.home.ne.jp>
43  To: me
44  Subject: Re: May God Bless You..
45  Date: Mon, 21 Feb 2022 18:17:36 -0800
46  MIME-Version: 1.0
47  Content-Type: text/plain;
48      charset="Windows-1251"
49  Content-Transfer-Encoding: 7bit
50  X-Priority: 3
Normal text file      length: 5,000 lines: 75      Ln: 34 Col: 90 Sel: 14 | 1      Windows (CR LF)      UTF-8      INS
```

- 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

- in order 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
