Phishing-
Email Analysis

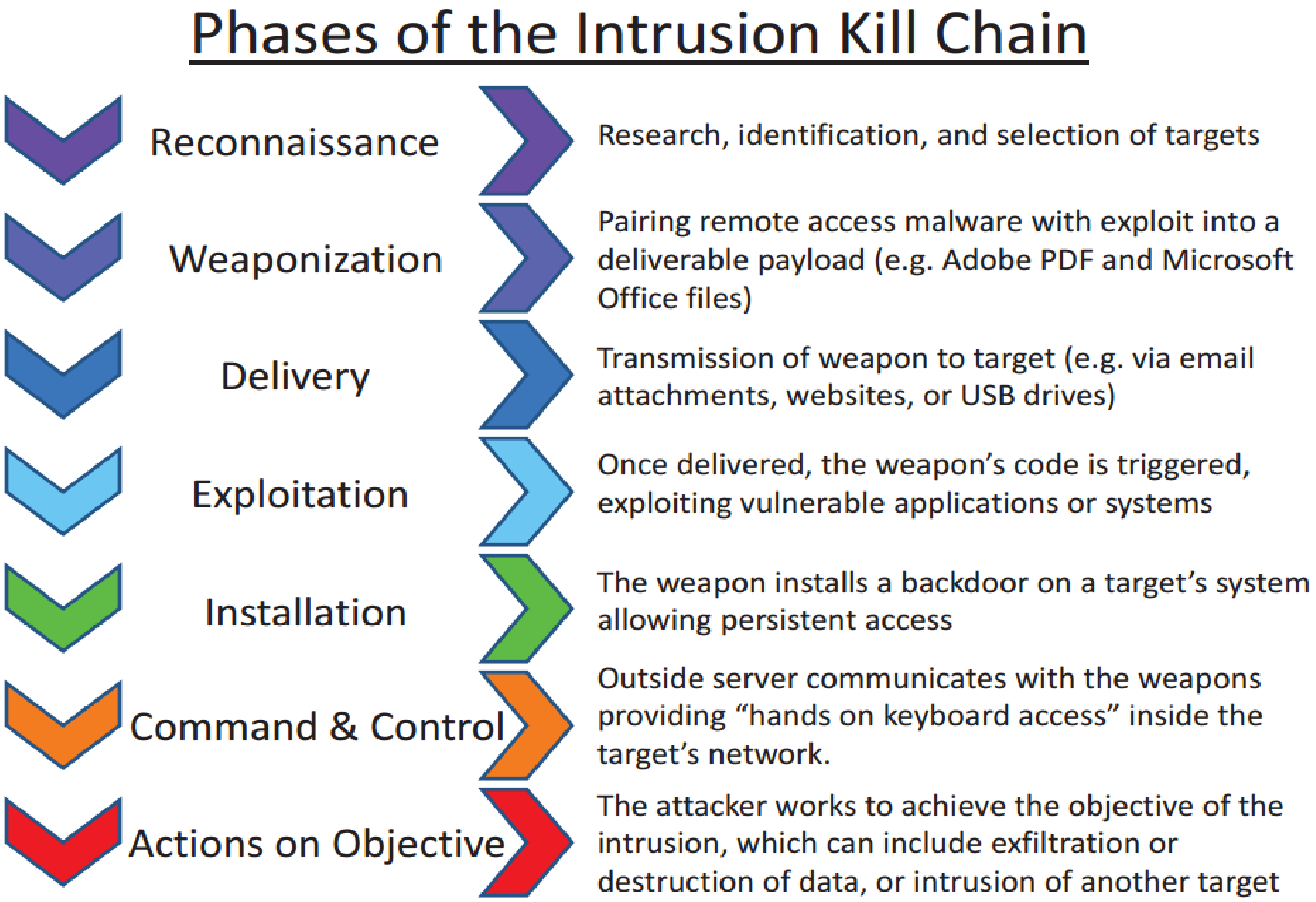
NELSON OJOVBO

https://www.linkedin.com/in/nelson-ojovbo/

Introduction to Phishing

- **Phishing attack** is a type of attack aimed at stealing personal data of the user in general by clicking on malicious links to the users via email or running malicious files on their computer.

- **Phishing attacks** correspond to the "**Delivery**" phase in the **Cyber Kill Chain** model created to analyze cyber-attacks. The delivery stage is the step where the attacker transmits the previously prepared harmful content to the victim systems / people.



Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

The Phishing attack is the most common attack vector for initial access**.** Of course, the only purpose of the attack is not to steal the user's password information.

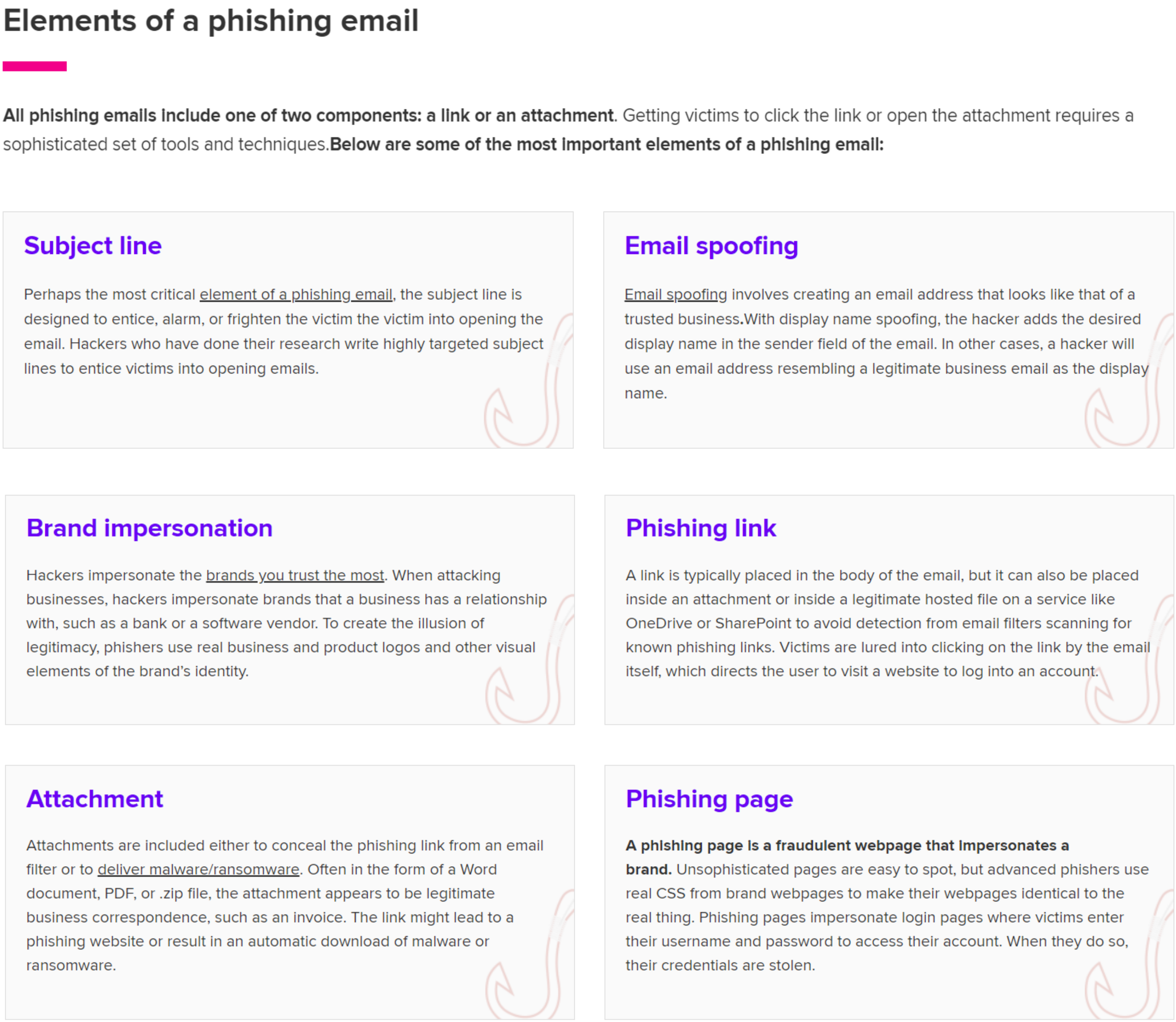
The purpose of such attacks is to exploit the human factor, the weakest link in the chain. Attackers use phishing attacks as the first step to infiltrate systems.

What is phishing email analysis?

Phishing email analysis involves studying the content of phishing emails to ascertain the techniques the attacker used.

What is a common indicator of a phishing email?

Common indicators of a phishing email include suspicious addresses, links, or domain names, threatening language or a sense of urgency, errors in the email, the inclusion of suspicious attachments, and emails requesting sensitive information.



Elements of a phishing email

All phishing emails include one of two components: a link or an attachment. Getting victims to click the link or open the attachment requires a sophisticated set of tools and techniques.**Below are some of the most important elements of a phishing email:**

Subject line

Perhaps the most critical element of a phishing email, the subject line is designed to entice, alarm, or frighten the victim the victim into opening the email. Hackers who have done their research write highly targeted subject lines to entice victims into opening emails.

Email spoofing

Email spoofing involves creating an email address that looks like that of a trusted business**.**With display name spoofing, the hacker adds the desired display name in the sender field of the email. In other cases, a hacker will use an email address resembling a legitimate business email as the display name.

Brand impersonation

Hackers impersonate the brands you trust the most. When attacking businesses, hackers impersonate brands that a business has a relationship with, such as a bank or a software vendor. To create the illusion of legitimacy, phishers use real business and product logos and other visual elements of the brand's identity.

Phishing link

A link is typically placed in the body of the email, but it can also be placed inside an attachment or inside a legitimate hosted file on a service like OneDrive or SharePoint to avoid detection from email filters scanning for known phishing links. Victims are lured into clicking on the link by the email itself, which directs the user to visit a website to log into an account.

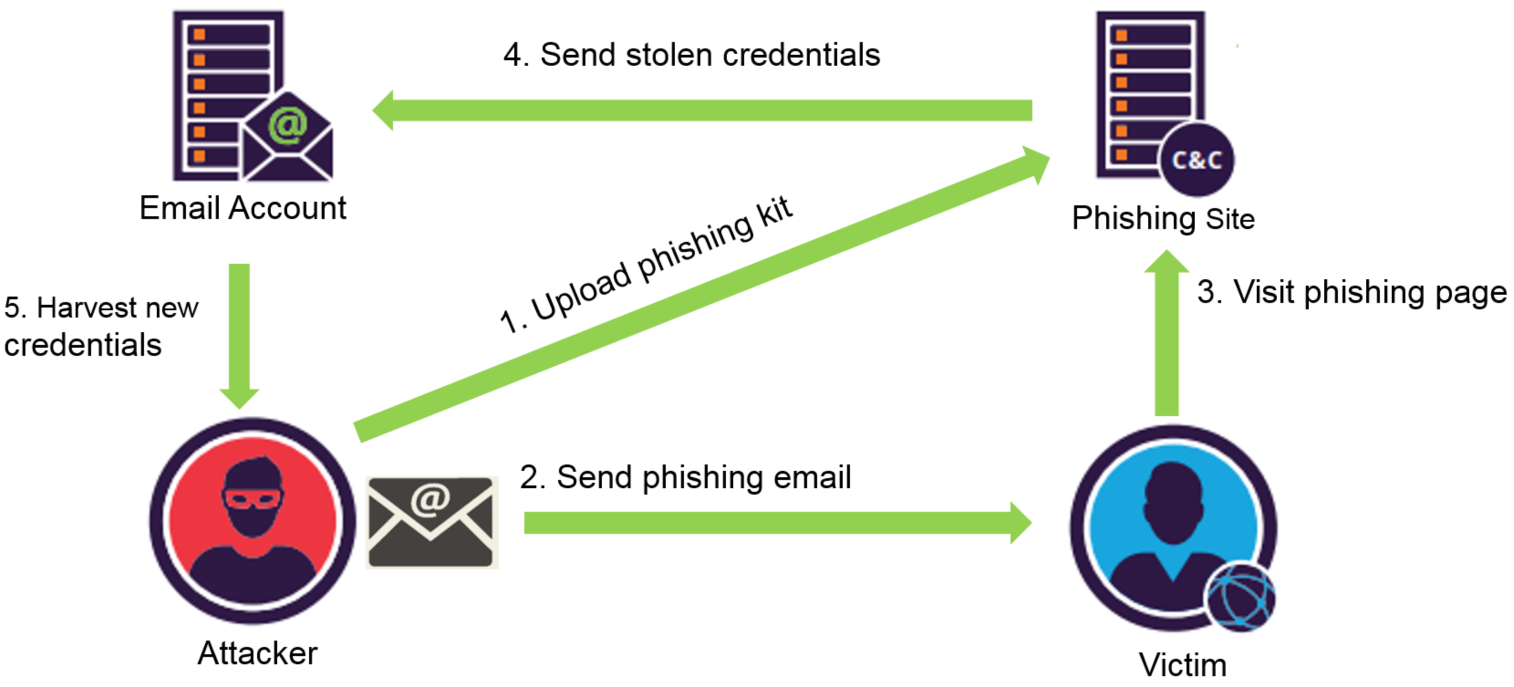
Attachment

Attachments are included either to conceal the phishing link from an email filter or to deliver malware/ransomware. Often in the form of a Word document, PDF, or .zip file, the attachment appears to be legitimate business correspondence, such as an invoice. The link might lead to a phishing website or result in an automatic download of malware or ransomware.

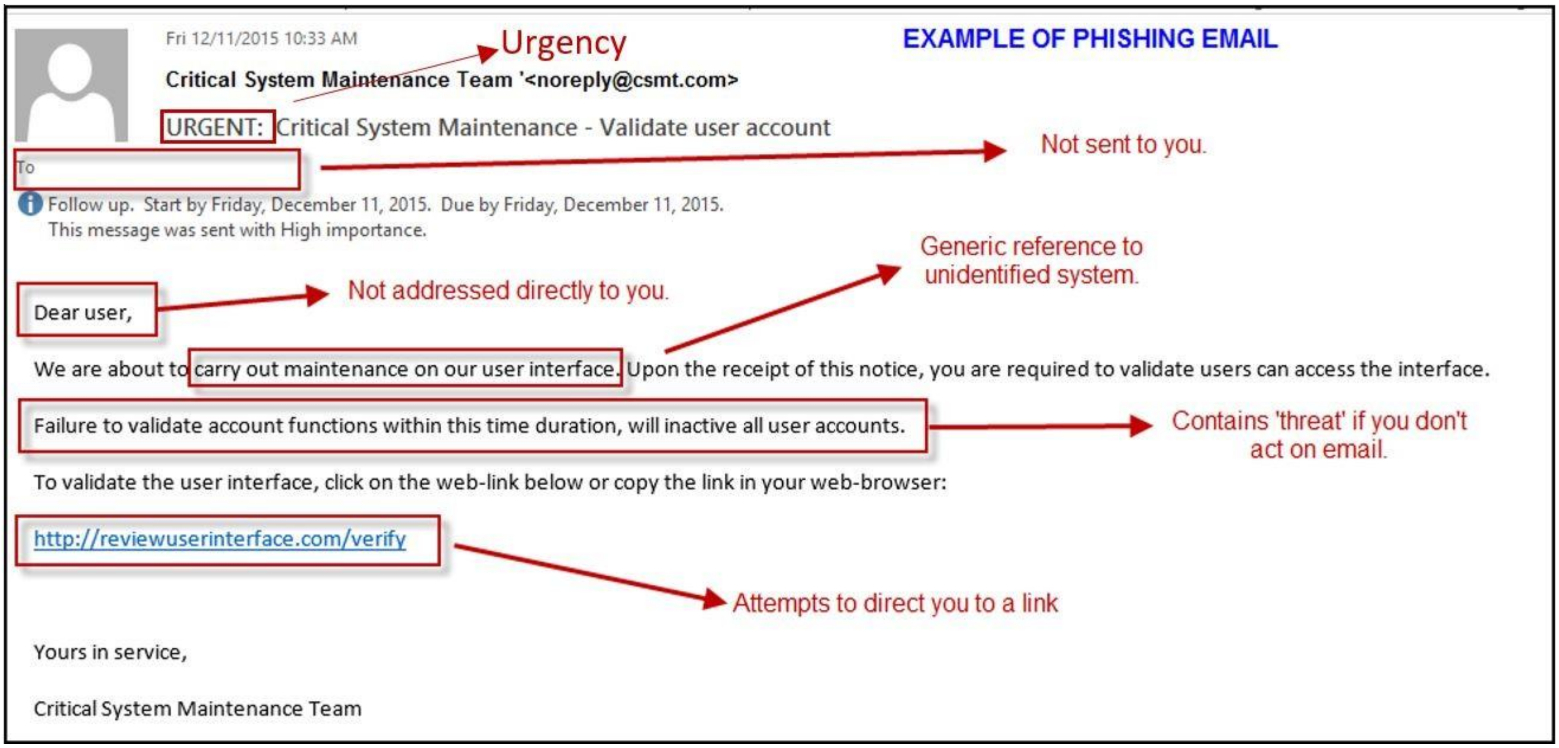
Phishing page

A phishing page is a fraudulent webpage that impersonates a brand. Unsophisticated pages are easy to spot, but advanced phishers use real CSS from brand webpages to make their webpages identical to the real thing. Phishing pages impersonate login pages where victims enter their username and password to access their account. When they do so, their credentials are stolen.

Phishing attack flow



EXAMPLE OF PHISHING EMAIL



EXAMPLE OF PHISHING EMAIL

Fri 12/11/2015 10:33 AM

Critical System Maintenance Team '<noreply@csmt.com>

URGENT: Critical System Maintenance - Validate user account

To

Follow up. Start by Friday, December 11, 2015. Due by Friday, December 11, 2015.
This message was sent with High importance.

Dear user,

We are about to carry out maintenance on our user interface. Upon the receipt of this notice, you are required to validate users can access the interface.

Failure to validate account functions within this time duration, will inactive all user accounts.

To validate the user interface, click on the web-link below or copy the link in your web-browser:

http://reviewuserinterface.com/verify

Yours in service,

Critical System Maintenance Team

Urgency

Not sent to you.

Generic reference to unidentified system.

Not addressed directly to you.

Contains 'threat' if you don't act on email.

Attempts to direct you to a link

Information Gathering

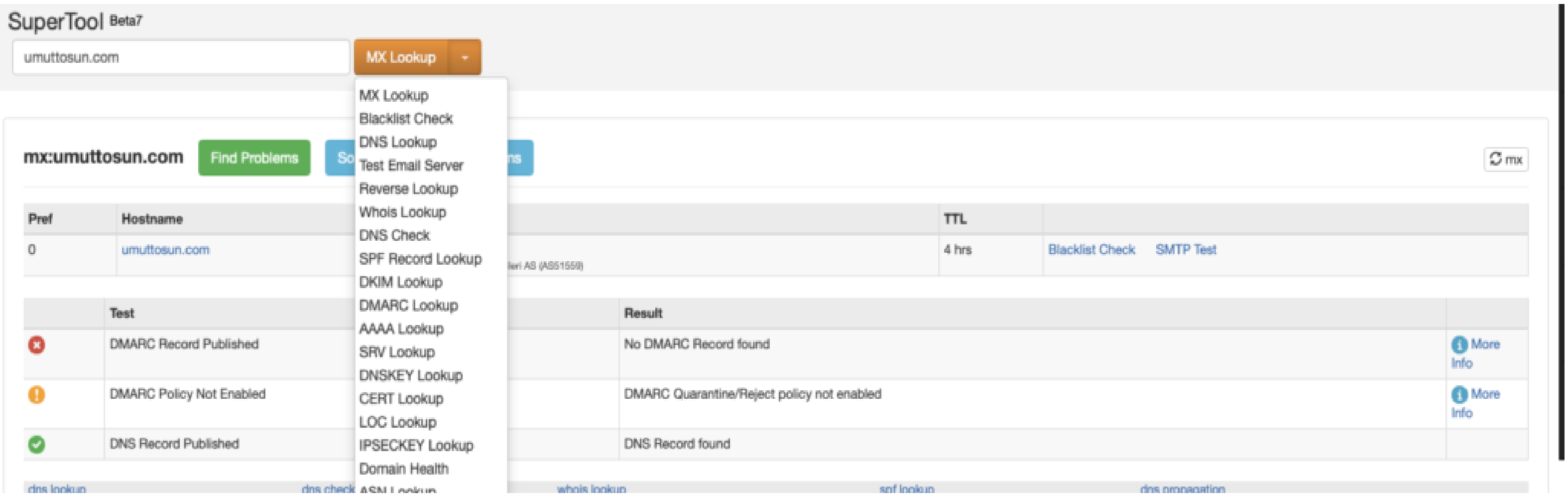
Spoofing

Attackers can send emails on behalf of someone else, as the emails do not necessarily have an authentication mechanism. Attackers can send mail on behalf of someone else using the technique called spoofing to make the user believe that the incoming email is reliable.

Several protocols have been created to prevent the Email Spoofing technique. With the help of **SPF, DKIM and DMARC** protocols, it can be understood whether the sender's address is fake or real. Some mail applications do these checks automatically. However, the use of these protocols is not mandatory and in some cases can cause problems.

- **Sender Policy Framework (SPF)**
- **DomainKeys Identified Mail (DKIM)**

To find out manually whether the mail is spoof or not, SMTP address of the mail should be learned first. **SPF, DKIM, DMARC and MX records** of the domain can be learned using tools such as Mxtoolbox. By comparing the information here, it can be learned whether the mail is spoof or not.



mx:umuttosun.com

Pref	Hostname		TTL	
0	umuttosun.com	eri AS (AS51559)	4 hrs	Blacklist Check SMTP Test

	Test	Result	
✗	DMARC Record Published	No DMARC Record found	More Info
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DNS Record Published	DNS Record found	

Since the IP addresses of the big institutions using their own mail servers will belong to them, it can be examined whether the SMTP address belongs to that institution by looking at the **whois** records of the SMTP IP address.

An important point here is that if the sender address is not spoof, we cannot say mail is safe. Harmful mails can be sent on behalf of trusted persons by hacking corporate / personal email addresses. This type of cyber attacks has already happened, so this possibility should always be considered.

E-mail Traffic Analysis

Many parameters are needed when analyzing a phishing attack. We can learn the size of the attack and the target audience in the search results to be made on the mail gateway according to the following parameters.

- **Sender Address**
- **SMTP IP Address**
- **Email Address Domain**
- **Subject (sender address and SMTP address may be constantly changing).**

In the search results, it is necessary to learn the recipient addresses and time information besides the mail numbers.

If harmful e-mails are constantly forwarded to the same users, their e-mail addresses may have leaked in some way and shared on sites such as **PasteBin**.

Attackers can find email addresses with **theHarvester** tool on Kali Linux. It is recommended that such information should not be shared explicitly, as keeping personal mail addresses on websites would be a potential attack vector for attackers.

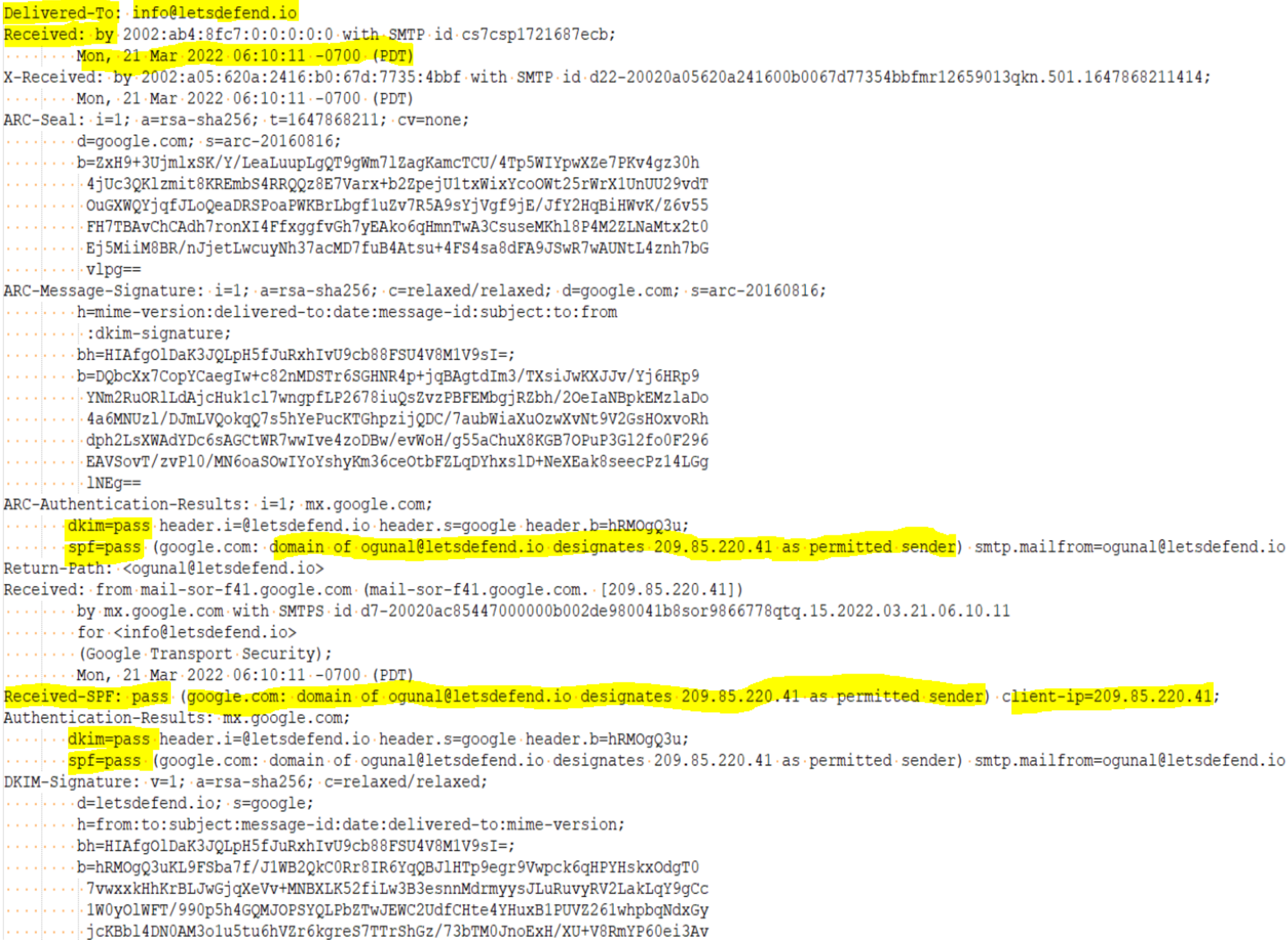
If mails are sent out of working hours, the attacker may be living on a different time-zone line. By gathering such information, we can begin to make sense of the attack.

What is an Email Header and How to Read Them?

In this section, we will explain what the header information in an email is, what can be done with this information and how to access this information. It is important to follow this section carefully as we will explain how to perform the header analysis in the next section.

What is an Email Header?

"**Header**" is basically a section of the mail that contains information such as sender, recipient and date. In addition, there are fields such as **"Return-Path", "Reply-To", and "Received".** Below you can see the header details of a sample email.

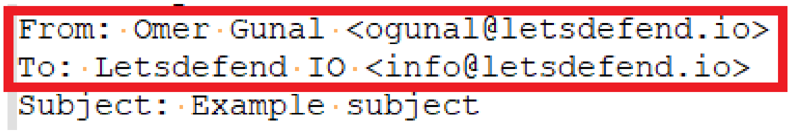


```
Delivered-To: info@letsdefend.io
Received: by 2002:ab4:8fc7:0:0:0:0:0 with SMTP id cs7csp1721687ecb;
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
X-Received: by 2002:a05:620a:2416:b0:67d:7735:4bbf with SMTP id d22-20020a05620a241600b0067d77354bbfmr12659013qkn.501.1647868211414;
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1647868211; cv=none;
        d=google.com; s=arc-20160816;
        b=ZxH9+3UjmlxSK/Y/LeaLuupLgQT9gWm7lZagKamcTCU/4Tp5WIYpwXZe7PKv4gz30h
         4jUc3QKlzmit8KREmbS4RRQQz8E7Varx+b2ZpejU1txWixYcoOWt25rWrX1UnUU29vdT
         OuGXWQYjqfJLoQeaDRSPoaPWKBrLbgf1uZv7R5A9sYjVgf9jE/JfY2HqBiHWvK/Z6v55
         FH7TBAvChCAdh7ronXI4FfxggfvGh7yEAko6qHmnTwA3CsuseMKhl8P4M2ZLNaMtx2t0
         Ej5MiiM8BR/nJjetLwcuyNh37acMD7fuB4Atsu+4FS4sa8dFA9JSwR7wAUNtL4znh7bG
         vlpg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:delivered-to:date:message-id:subject:to:from
         :dkim-signature;
        bh=HIAfgOlDaK3JQLpH5fJuRxhIvU9cb88FSU4V8M1V9sI=;
        b=DQbcXx7CopYCaegIw+c82nMDSTr6SGHNR4p+jqBAgtdIm3/TXsiJwKXJJv/Yj6HRp9
         YNm2RuORlLdAjcHuk1cl7wngpfLP2678iuQsZvzPBFEMbgjRZbh/2OeIaNBpkEMzlaDo
         4a6MNUzl/DJmLVQokqQ7s5hYePucKTGhpzijQDC/7aubWiaXuOzwXvNt9V2GsHOxvoRh
         dph2LsXWAdYDc6sAGCtWR7wwIve4zoDBw/evWoH/g55aChuX8KGB7OPuP3Gl2fo0F296
         EAVSovT/zvPl0/MN6oaSOwIYoYshyKm36ceOtbFZLqDYhxslD+NeXEak8seecPz14LGg
         lNEg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMOgQ3u;
       spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
Return-Path: <ogunal@letsdefend.io>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id d7-20020ac85447000000b002de980041b8sor9866778qtq.15.2022.03.21.06.10.11
        for <info@letsdefend.io>
        (Google Transport Security);
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
Received-SPF: pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMOgQ3u;
       spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=letsdefend.io; s=google;
        h=from:to:subject:message-id:date:delivered-to:mime-version;
        bh=HIAfgOlDaK3JQLpH5fJuRxhIvU9cb88FSU4V8M1V9sI=;
        b=hRMOgQ3uKL9FSba7f/J1WB2QkC0Rr8IR6YqQBJlHTp9egr9Vwpck6qHPYHskxOdgT0
         7vwxxkHhKrBLJwGjqXeVv+MNBXLK52fiLw3B3esnnMdrmyysJLuRuvyRV2LakLqY9gCc
         1W0yOlWFT/990p5h4GQMJOPSYQLPbZTwJEWC2UdfCHte4YHuxB1PUVZ261whpbqNdxGy
         jcKBbl4DN0AM3o1u5tu6hVZr6kgreS7TTrShGz/73bTM0JnoExH/XU+V8RmYP60ei3Av
```

What does the Email Header do?

A. Enables Shipper and Recipient Identification

- Thanks to the "From" and "To" fields in the header, it is determined from whom an email will go to whom. If we look at the email above that you downloaded in "eml" format, we see that it was sent from the address **ogunal@letsdefend.io** to **info@letsdefend.io**



```
From: Omer Gunal <ogunal@letsdefend.io>
To: Letsdefend IO <info@letsdefend.io>
Subject: Example subject
```

B. Spam Blocker

- It is possible to detect spam emails using **Header analysis** and other various methods. This protects people from receiving SPAM emails.

C. Allows Tracking an Email's Route

- **It is important to check the route it follows to see if an email came from the right address**. If we look at the sample email above, we see that it came from the **ogunal@letsdefend.io** address, but did it actually come from the **letsdefend.io** domain or from a different fake server that mimics the same name? We can use the header information to answer this question.

Important Email Header Fields

From

- The "From" field in the internet header indicates the name and email address of the sender.

To

- This field in the mail header contains the email's receiver's details.
- It includes their name and their email address. Fields like CC (carbon copy) and BCC (blind carbon copy) also fall under this category as they all include details of your recipients.
- If you want to find out more about carbon copy and blind carbon copy, check out how to use CC and BCC.

Date

- This is the timestamp that shows when the email was sent.
- In Gmail, it usually follows the format of "day dd month yyyy hh:mmss
- So if an email had been sent on the 16th of November, 2021, at 4:57:23 PM, it would show as Wed, 16 Nov 2021 16:57:23.

Subject

- The subject mentions the topic of the email. It summarizes the content of the entire message body.

Return-Path

- This mail header field is also known as Reply-To. If you reply to an email, it will go to the address mentioned in the Return-Path field.

Domain Key and DKIM Signatures

- The Domain Key and Domain Key Identified Mail (DKIM) are email signatures that help email service providers identify and authenticate your emails, similar to SPF signatures.

Message-ID

- The Message ID header field is a unique combination of letters and numbers that identifies each mail. No two emails will have the same Message ID.

MIME-Version

- Multipurpose Internet Mail Extensions (MIME) is an internet standard of encoding. It converts non-text content like images, videos, and other attachments into text so they can be attached to an email and sent through SMTP (Simple Mail Transfer Protocol).

Received

- The received field lists each mail server that went through an email before arriving in the recipient's inbox. It's listed in reverse chronological order — where the mail server on the top is the last server the email message went through, and the bottom is where the email originated.

X-Spam Status

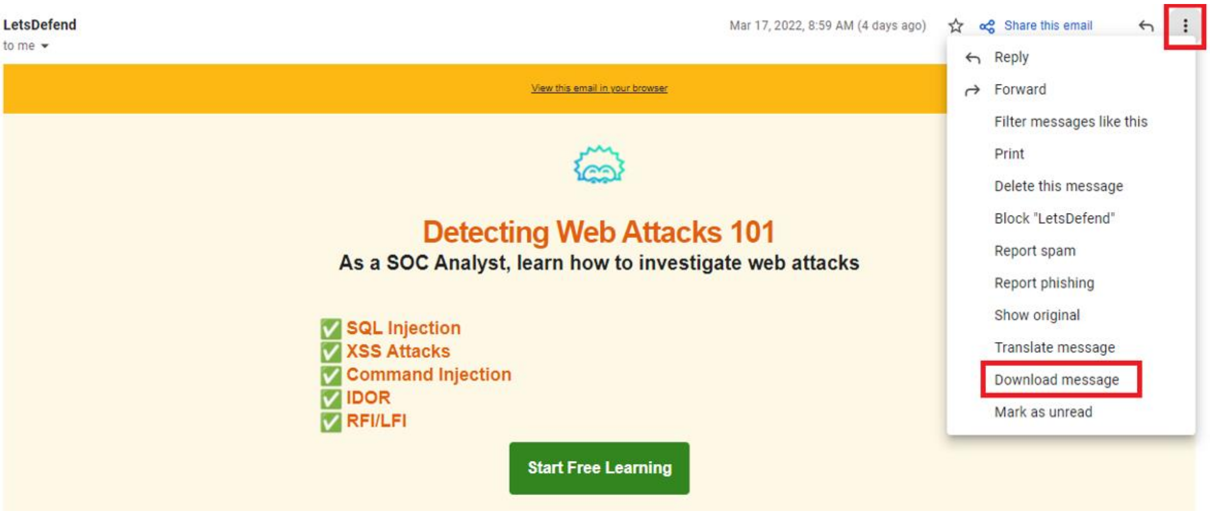
- The X-Spam Status shows you the spam score of an email message.
- First, it'll highlight if a message is classified as spam.
- Then, the spam score of the email is shown, as well as the threshold for the spam for the email.
- An email can meet either the spam threshold of an inbox or exceed it. If it's too spammy and exceeds the threshold, it will automatically be classified as spam and sent to the spam folder.

Reference of Field Definitions: gmass.co

How to Access Your Email Header?

Gmail

1- **Open the relevant e-mail**
2- **Click on the 3 points at the top right "..."**
3- **Click on the "Download message" button.**



LetsDefend
to me

Mar 17, 2022, 8:59 AM (4 days ago)

View this email in your browser

Detecting Web Attacks 101

As a SOC Analyst, learn how to investigate web attacks

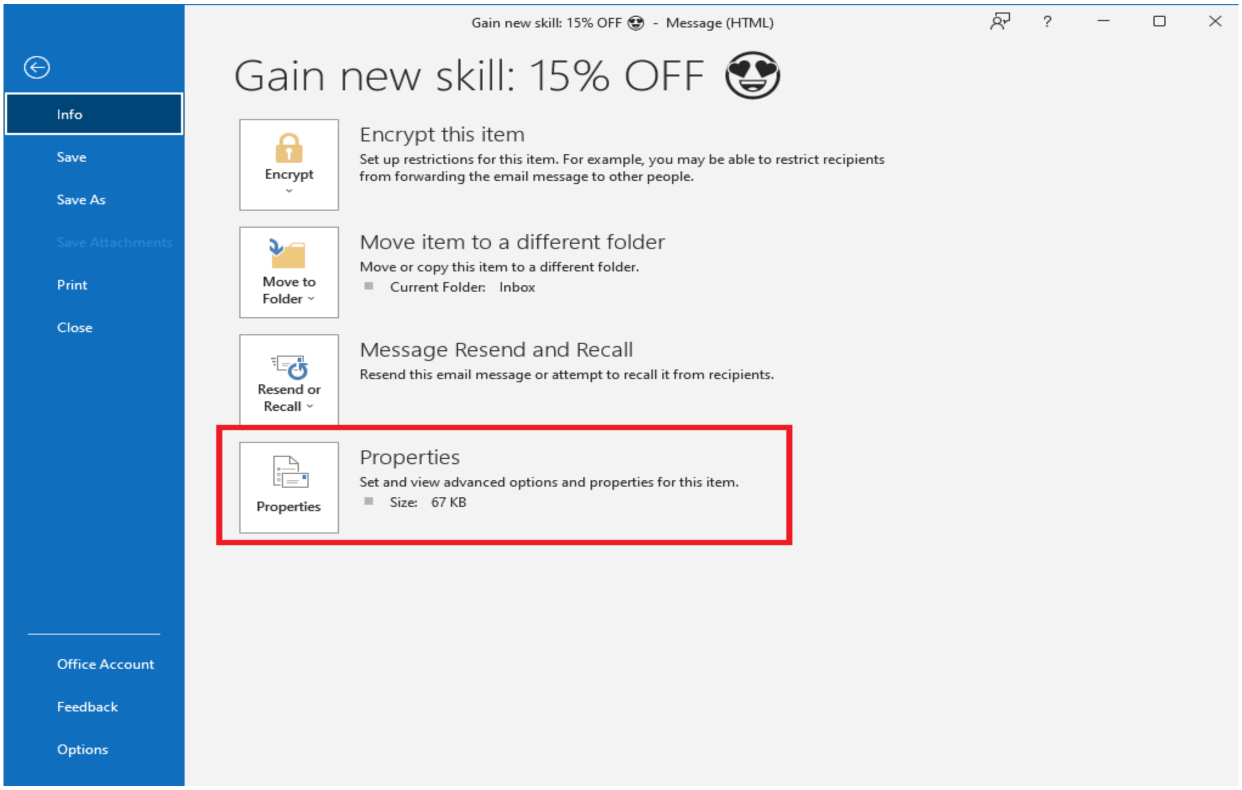
✅ SQL Injection
✅ XSS Attacks
✅ Command Injection
✅ IDOR
✅ RFI/LFI

4- Downloaded ".Open the file with the extension "eml" with any notebook application

Outlook

1- Open the relevant e-mail

2- File - > Info -> Properties - > Internet headers



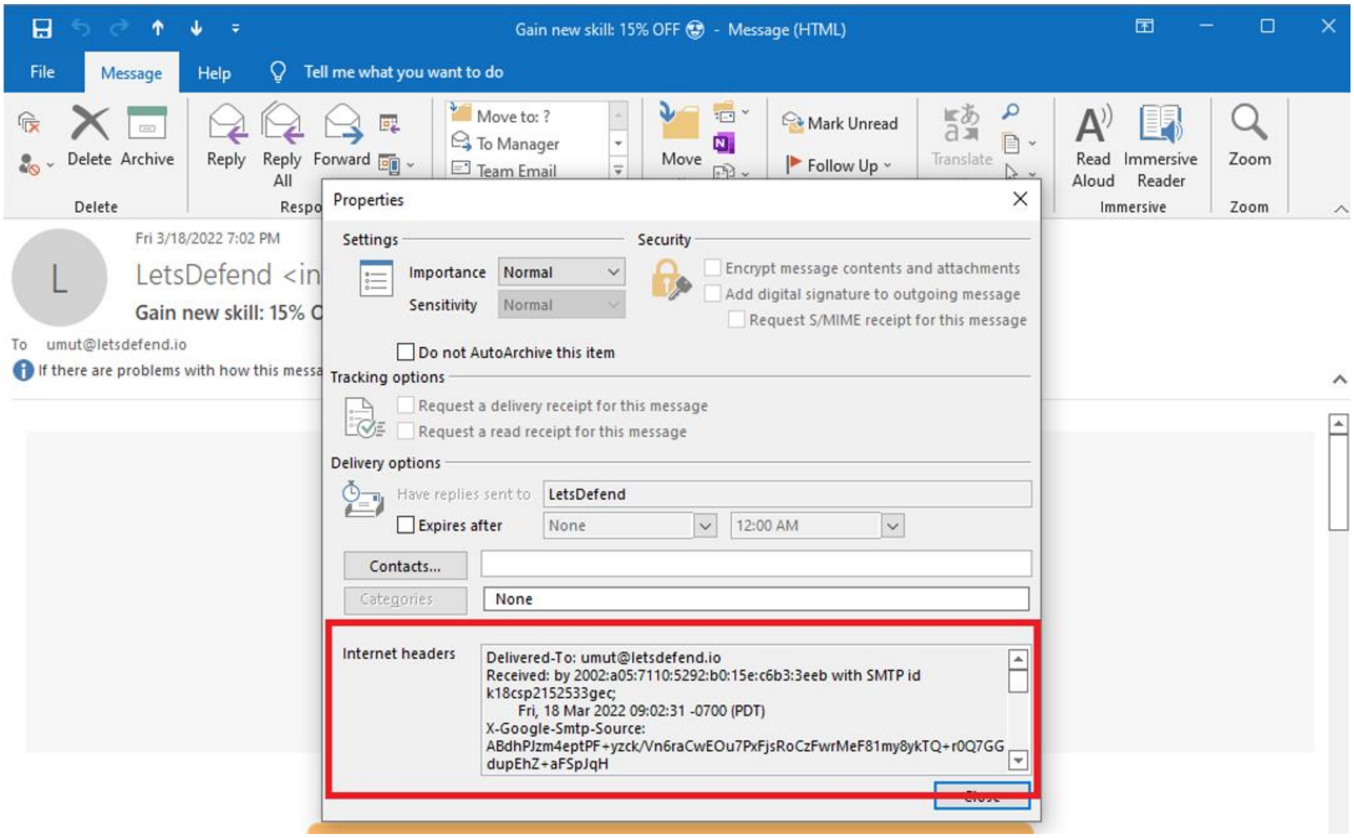
Gain new skill: 15% OFF 😍

Encrypt this item
Set up restrictions for this item. For example, you may be able to restrict recipients from forwarding the email message to other people.

Move item to a different folder
Move or copy this item to a different folder.
Current Folder: Inbox

Message Resend and Recall
Resend this email message or attempt to recall it from recipients.

Properties
Set and view advanced options and properties for this item.
Size: 67 KB



Fri 3/18/2022 7:02 PM

LetsDefend <in

Gain new skill: 15% O

To umut@letsdefend.io

If there are problems with how this messa

Importance: Normal
Sensitivity: Normal

□ Encrypt message contents and attachments
□ Add digital signature to outgoing message
□ Request S/MIME receipt for this message

□ Do not AutoArchive this item

□ Request a delivery receipt for this message
□ Request a read receipt for this message

Have replies sent to: LetsDefend
□ Expires after: None 12:00 AM

Categories: None

Internet headers

```
Delivered-To: umut@letsdefend.io
Received: by 2002:a05:7110:5292:b0:15e:c6b3:3eeb with SMTP id
k18csp2152533gec;
        Fri, 18 Mar 2022 09:02:31 -0700 (PDT)
X-Google-Smtp-Source:
ABdhPJzm4eptPF+yzck/Vn6raCwEOu7PxFjsRoCzFwrMeF81my8ykTQ+r0Q7GG
dupEhZ+aFSpJqH
```

EMAIL HEADER ANALYSIS LAB

Course Files

- **Filename:** Challenge Mail
- **Size:** 7,45 KB
- **Password:** infected
- **Download link:** https://app.letsdefend.io/download/downloadfile/Challenge%20Mail.zip

Practice Questions

- Download the email above, if we want to answer this email, what would the recipient's address be?
- What year was the email sent?
- What is the Message-ID value? (without > <)

SAMPLE EMAIL HEADER

```
Delivered-To: ogunal@letsdefend.io
Received: by 2002:a05:6400:159:0:0:0:0 with SMTP id hw25csp1949486ecb; Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzA6syR+DNCl4k2HAsTVGRMTuZ8qBPoI7WZhdA2aQRebfOMIA6xySOrt/bkng1NaGtoG3CB
X-Received: by 2002:a25:1344:0:b0:633:7592:9c0f with SMTP id 65-
20020a251344000000b0063375929c0fmr24595651ybt.211.1647895524591; Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
ARC-Authentication-Results: i=1; mx.google.com;
    dkim=pass header.i=@mailchimpapp.net header.s=k3 header.b=LDGOzGog;
    spf=pass (google.com: domain of bounce-mc.us14_171215441.8996217-675c34a61f@mail41.suw13.rsgsv.net designates
198.2.183.41 as permitted sender) smtp.mailfrom=bounce-mc.us14_171215441.8996217-675c34a61f@mail41.suw13.rsgsv.net
Return-Path: <bounce-mc.us14_171215441.8996217-675c34a61f@mail41.suw13.rsgsv.net>
Received: from mail41.suw13.rsgsv.net (mail41.suw13.rsgsv.net. [198.2.183.41])
     by mx.google.com with ESMTPS id o5-20020a0dcc05000000b002e5bb9dca69si6996501ywd.242.2022.03.21.13.45.23
     for <ogunal@letsdefend.io>
     (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);    Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce-mc.us14_171215441.8996217-675c34a61f@mail41.suw13.rsgsv.net
designates 198.2.183.41 as permitted sender) client-ip=198.2.183.41; Authentication-Results: mx.google.com;
    dkim=pass header.i=@mailchimpapp.net header.s=k3 header.b=LDGOzGog;
    spf=pass (google.com: domain of bounce-mc.us14_171215441.8996217-675c34a61f@mail41.suw13.rsgsv.net designates
198.2.183.41 as permitted sender) smtp.mailfrom=bounce-mc.us14_171215441.8996217-675c34a61f@mail41.suw13.rsgsv.net
Received: from localhost (localhost [127.0.0.1]) by mail41.suw13.rsgsv.net (Mailchimp) with ESMTP id 4KMmpW3vnnz9K82VW
        for <ogunal@letsdefend.io>; Mon, 21 Mar 2022 20:45:23 +0000 (GMT)
Subject: =?utf-8?Q?Top=203=20Blog=20posts=20for=20SOC=20teams=C2=A0=F0=9F=91=80?=
From: =?utf-8?Q?LetsDefend?= <info@letsdefend.io>

Reply-To: =?utf-8?Q?LetsDefend?= <info@letsdefend.io>

To: <ogunal@letsdefend.io>

Date: Mon, 21 Mar 2022 20:45:17 +0000

Message-ID: <74bda5edf824cea8aad36e707.675c34a61f.20220321204512.a02caaccf3.a268ce5a@mail41.suw13.rsgsv.net>

MIME-Version: 1.0
```

Email Header Analysis

In previous sections we talked about what a phishing email is, what header information is and what it does. Now, when we suspect that an email is phishing, we will know what we should do and what the analysis process should be like.

Here are the key questions we need to answer when checking headings during a Phishing analysis:

- **Was the email sent from the correct SMTP server?**

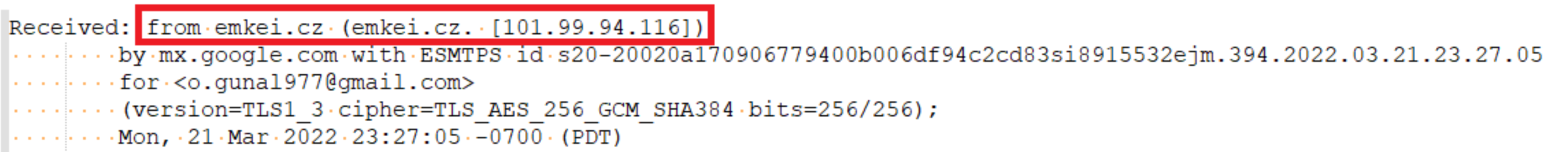
- **Are the data "From" and "Return-Path / Reply-To" the same?**

The e-mail examined in the rest of the article:

- password: infected
- Download Link: https://drive.google.com/file/d/1x4BQF9zdR2l913eISQtixb-kmi9Jan_6/view

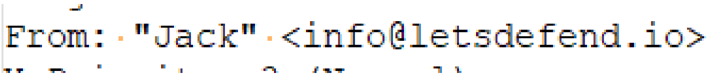
A. Was the email sent from the correct SMTP server?

We can check the "Received" field to see the path followed by the mail. As the image below shows, the mail is **"101[.]99.94.116"** from the IP address server.



```
Received: from emkei.cz (emkei.cz. [101.99.94.116])
        by mx.google.com with ESMTPS id s20-20020a170906779400b006df94c2cd83si8915532ejm.394.2022.03.21.23.27.05
        for <o.gunal977@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Mon, 21 Mar 2022 23:27:05 -0700 (PDT)
```

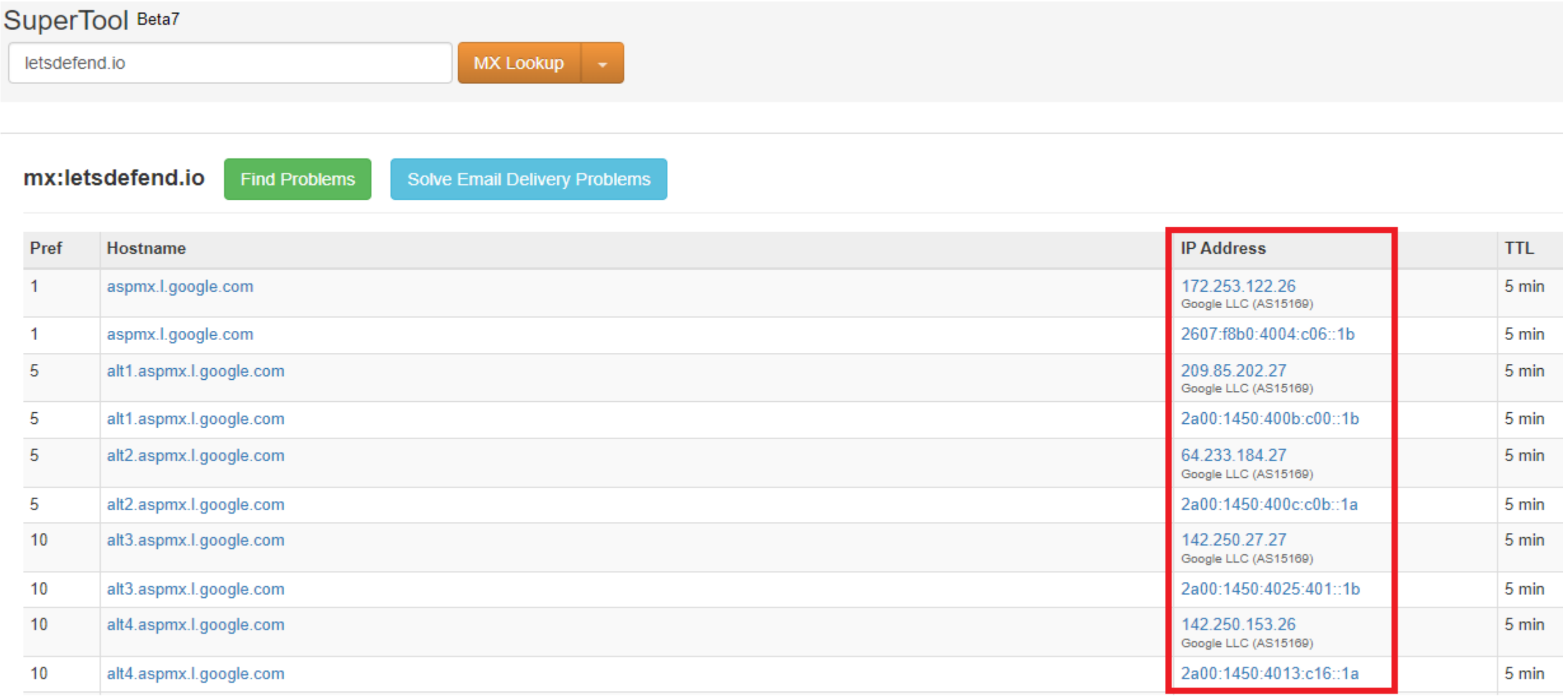
If we look at who is sending the mail ("sender"), we see that it came from the domain Letsdefend.io



```
From: "Jack" <info@letsdefend.io>
```

So under normal circumstances, "letsdefend.io" should use, "101[.]99.94.116" to send mail. To confirm this situation, We can query the MX servers actively used by "letsdefend.io"

"mxtoolbox.com" helps by showing you the MX servers used by the domain you searched.



Pref	Hostname	IP Address	TTL
1	aspmx.l.google.com	172.253.122.26 Google LLC (AS15169)	5 min
1	aspmx.l.google.com	2607:f8b0:4004:c06::1b	5 min
5	alt1.aspmx.l.google.com	209.85.202.27 Google LLC (AS15169)	5 min
5	alt1.aspmx.l.google.com	2a00:1450:400b:c00::1b	5 min
5	alt2.aspmx.l.google.com	64.233.184.27 Google LLC (AS15169)	5 min
5	alt2.aspmx.l.google.com	2a00:1450:400c:c0b::1a	5 min
10	alt3.aspmx.l.google.com	142.250.27.27 Google LLC (AS15169)	5 min
10	alt3.aspmx.l.google.com	2a00:1450:4025:401::1b	5 min
10	alt4.aspmx.l.google.com	142.250.153.26 Google LLC (AS15169)	5 min
10	alt4.aspmx.l.google.com	2a00:1450:4013:c16::1a	5 min

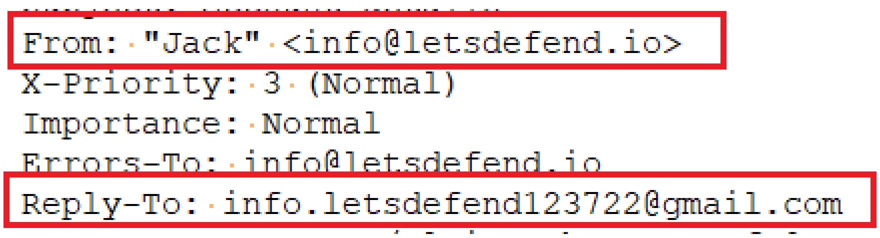
If we look at the image above, the "letsdefend.io" domain uses Google addresses as an email server. So there is no relationship with the emkei[.]cz or "101[.]99.94.116" addresses.

In this check, it was determined that the email did not come from the original address, but was spoofed.

B. Are the data "From" and "Return-Path / Reply-To" the same?

Except in exceptional cases, we expect the sender of the e-mail and the person receiving the responses to be the same. An example of why these areas are used differently in Phishing attacks:

Returning to the e-mail we downloaded above, all we have to do is compare the email addresses in the "From" and "Reply-to" fields.



```
From: "Jack" <info@letsdefend.io>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: info@letsdefend.io
Reply-To: info.letsdefend123722@gmail.com
```

As you can see, the data is different. In other words, when we want to reply to this e-mail, we will send a reply to the gmail address below. Just because this data is different doesn't always mean it's definitely a phishing email, we need to consider the event as a whole. In other words, in addition to this suspicious situation, if there is a harmful attachment, URL or misleading content in the e-mail content, we can understand that the e-mail is phishing.

Course Files

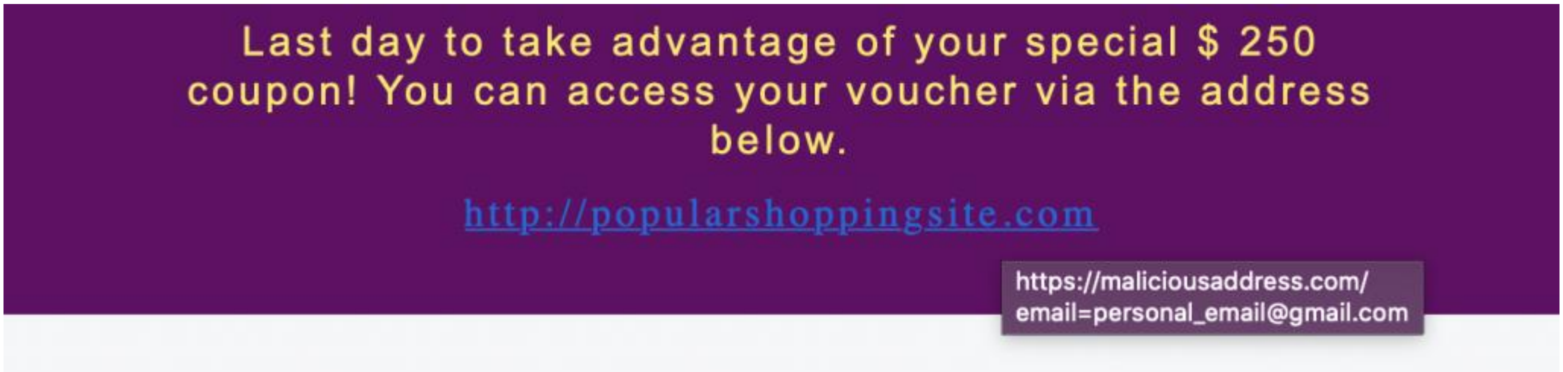
- **Filename:** Header Challenge
- **Size:** 2,69 KB
- **Password:** infected
- **Download**: https://drive.google.com/file/d/1x4BQF9zdR2l913eISQtixb-kmi9Jan_6/view

LAB Questions

1. If I want to reply to this email, which address will it be sent to?
   - open the email with text editor and check the reply-to field
2. From which IP address was the email sent?
   - check the email fields
3. Download the email above ("Header Challenge"), are the sender's address and the address in the "Reply-To" area
   - check from and reply-to fields

Static Analysis

It is a fact that mails composed of plain text are boring. For this reason, mail applications provide HTML support, allowing the creation of mails that can attract more attention of users. Of course, this feature has a disadvantage. Attackers can create e-mails with HTML, hiding URL addresses that are harmful behind buttons / texts that seem harmless.



Last day to take advantage of your special $ 250 coupon! You can access your voucher via the address below.

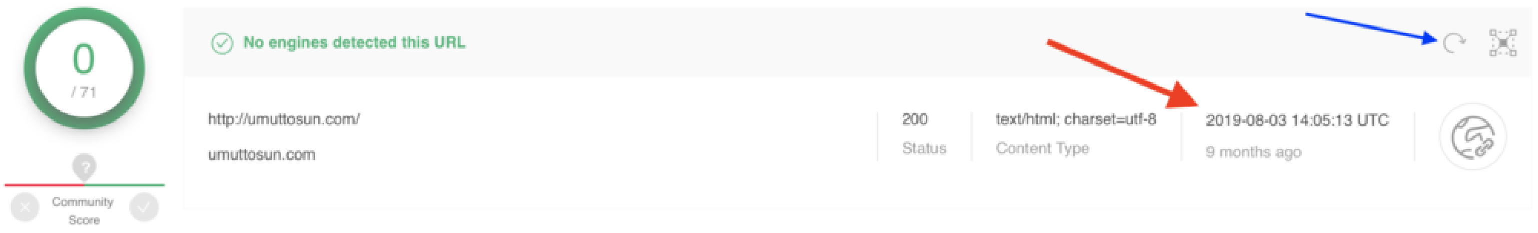
http://popularshoppingsite.com

https://maliciousaddress.com/
email=personal_email@gmail.com

As seen in the image above, the address that the user sees can be different when the link is clicked (the real address is seen when the link is hovered).

Attackers take a new domain address in most phishing attacks and do a phishing attack within a few days and finish their work. For this reason, if the domain name in the mail is new, it is more likely to be a phishing attack.

It is possible to find out whether the antivirus engines detect the web address as harmful by searching the web addresses in the mail on VirusTotal. If someone else has already analyzed the same address / file in **VirusTotal**, **VirusTotal does not analyze from scratch, it shows you the old analysis result. We can use this feature both as an advantage and a disadvantage.**



0
/ 71

Community Score

No engines detected this URL

http://umuttosun.com/
umuttosun.com

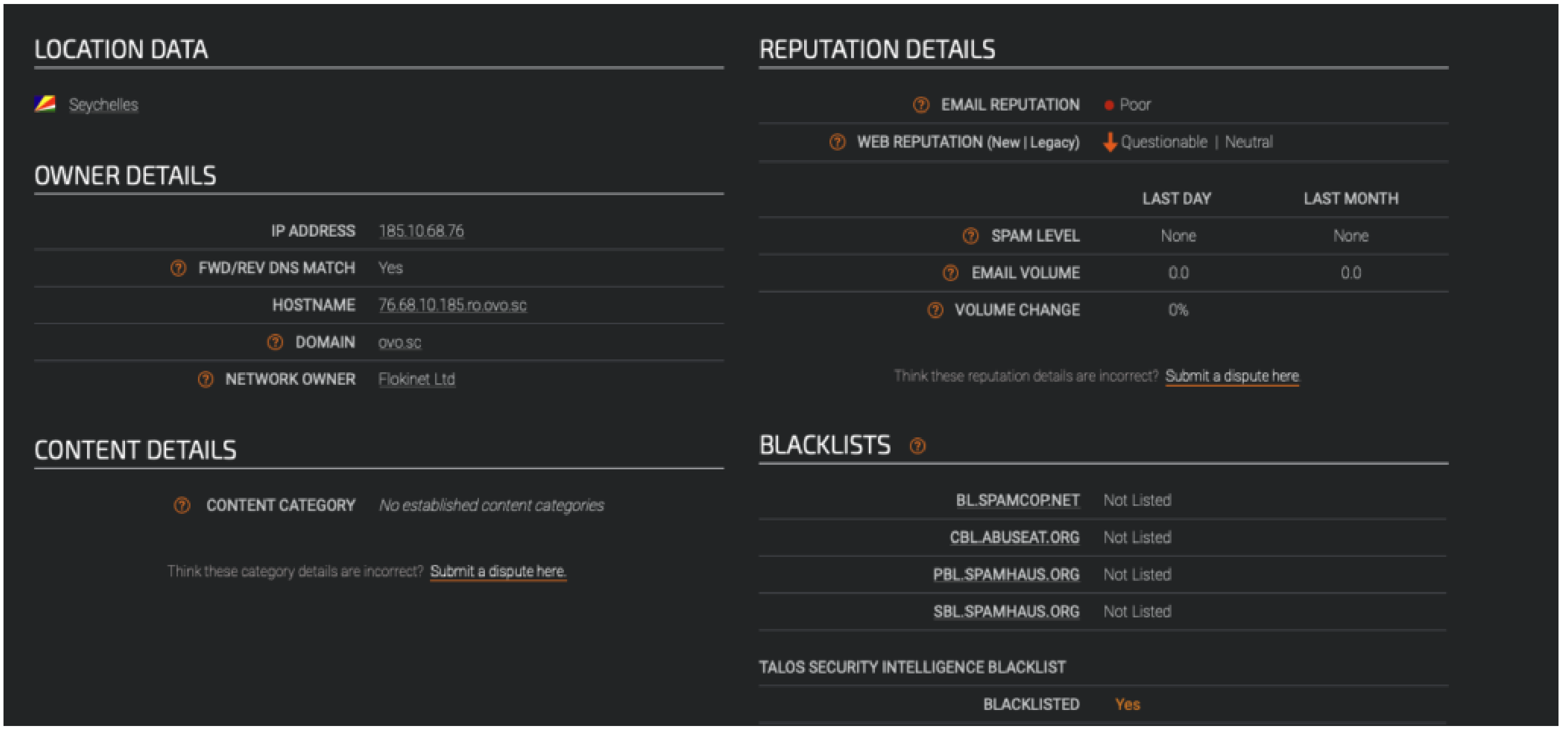
200	text/html; charset=utf-8	2019-08-03 14:05:13 UTC
Status	Content Type	9 months ago

If the attacker searches the domain address on **VirusTotal** without containing harmful content on it, that address will appear harmless on VirusTotal, and if it goes unnoticed, you may be mistaken for this address to be harmless.

In the image above, you can see that umuttosun.com address appears harmless, but if you look at the section marked with the **red** arrow, you will see that this address was searched 9 months ago, and this result is 9 months ago. **To have it analyzed again, the button marked with the blue arrow must be pressed.**

Performing static analysis of the files in the mail can enable the learning of the capacity / capabilities of that file. However, since static analysis takes a long time, you can get the information you need more quickly with dynamic analysis.

Cisco Talos Intelligence has search sections where we can learn reputations of IP addresses. By searching the SMTP address of the mail we detected on Talos, we can see the reputation of the IP address and find out whether it is included in the blacklist. If the SMTP address is in the blacklist, it can be understood that an attack was made on a compromised server.



LOCATION DATA

Seychelles

OWNER DETAILS

IP ADDRESS	185.10.68.76
FWD/REV DNS MATCH	Yes
HOSTNAME	76.68.10.185.ro.ovo.sc
DOMAIN	ovo.sc
NETWORK OWNER	Flokinet Ltd

CONTENT DETAILS

CONTENT CATEGORY	*No established content categories*

Think these category details are incorrect? Submit a dispute here.

REPUTATION DETAILS

EMAIL REPUTATION	● Poor
WEB REPUTATION (New | Legacy)	Questionable | Neutral

	LAST DAY	LAST MONTH
SPAM LEVEL	None	None
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	

Think these reputation details are incorrect? Submit a dispute here

BLACKLISTS

BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed

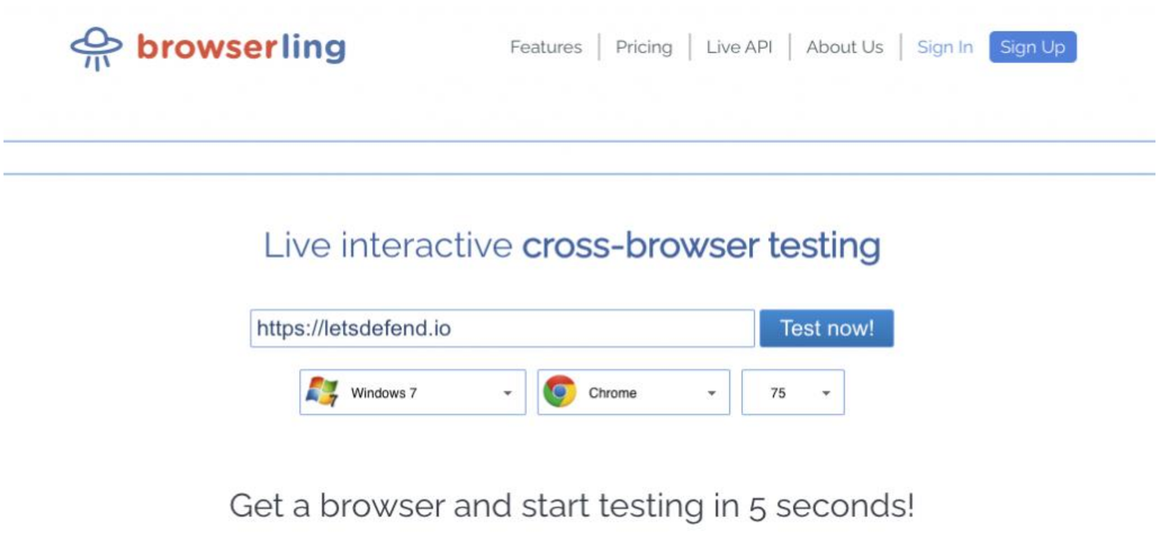
TALOS SECURITY INTELLIGENCE BLACKLIST

BLACKLISTED	Yes

Likewise, the SMTP address can be searched on VirusTotal and AbuseIPDB to determine if the IP address has previously been involved in malicious activities.

Dynamic Analysis

URLs and files can be found in the mail. These files and URL addresses need to be examined. You don't want your data to be stolen by hackers by running these files on your personal computer. For this reason, the websites and files in the mail should be run in sandbox environments and the changes made on the system should be examined, and it should be checked whether they are harmful or not.



Live interactive cross-browser testing

https://letsdefend.io

Get a browser and start testing in 5 seconds!

If you want to quickly check the web addresses in the mail, you can see the content of the website using online web browsers such as Browserling. The good thing about such services is that you will not be affected by a possible zero-day vulnerability that affects browsers, since you do not go to the web page on your own computer.

The disadvantage of using web browsers such as Browserling is that if the malicious file is downloaded on the site, you cannot run this file. For this reason, your analysis will be interrupted.

Sandbox Environment for Email Header Analysis

You can examine suspicious files and websites in sandbox environments. When you examine the files in these environments, you remove the risk of infecting your computer with malware. Many sandbox services / products are available. These products / services are available for paid and free use. You can choose one / more of these services according to your needs.

A few commonly used sandboxes:

- VMRay
- Cuckoo Sandbox
- JoeSandbox
- AnyRun
- Hybrid Analysis(Falcon Sandbox)

NOTE

- ❖ Malware can wait for a certain period of time without any action to make detection difficult. You must wait for the malware to work before you decide that the examined file is not harmful.

- ❖ The fact that there are no urls and files in the mail does not mean that this is not harmful. The attacker can also send it as a picture so as not to get caught up in the analysis products

Additional Techniques

Another technique that attackers use is to perform phishing attacks using normally legal sites. Some of them are as follows.

A. Using services that offer Cloud Storage services such as Google and Microsoft

Attackers try to click on Google / Microsoft drive addresses that seem harmless to the user by uploading harmful files onto the drive.

B. Using services that allow creating free subdomains such as Microsoft, Wordpress, Blogspot, Wix

Attackers try to deceive security products and analysts by creating a free subdomain from these services. Since whois information cannot be searched as a subdomain, it can be seen that these addresses were taken in the past and belongs to institutions such as Microsoft, WordPress.

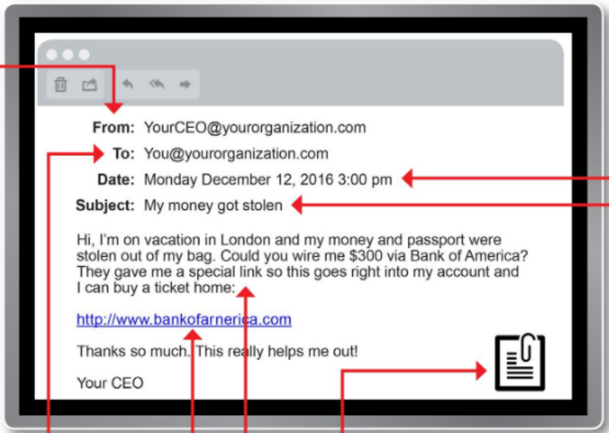
C. Form applications

Services are available that allow free form creation. Attackers use these services instead of creating a fishing site themselves. Since the domain is harmless under normal conditions, it can pass on to the user without getting stuck on antivirus software. Google Form is an example of these services. When looking at whois information, the domain can be seen to be Google, so the attacker can mislead analysts.

Hand-on Practice Lab with SOC Alerts on LetsDefend Platform

- 93 - SOC146 - Phishing Mail Detected - Excel 4.0 Macros
- 82 - SOC140 - Phishing Mail Detected - Suspicious Task Scheduler
- 45 - SOC114 - Malicious Attachment Detected - Phishing Alert
- 52 - SOC120 - Phishing Mail Detected - Internal to Internal
- 86 - SOC141 - Phishing URL Detected

Social Engineering Red Flags



From: YourCEO@yourorganization.com

To: You@yourorganization.com

Date: Monday December 12, 2016 3:00 pm

Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

DEFENSIVE PROTECTIVE MEASURES

Some defensive layers to take into consideration to assist in preventing email phishing attacks and credential stealing from phishing attacks would be:

- **Email scanning and filtering**
- **Email security gateways**
- **DNS authentication (DMARC, DKIM, and SPF)**
- **Anti-malware and anti-spam**
- **Multi-factor authentication (MFA)**
- **Phishing security awareness**

No matter how robust the email defensive layers are, phishing emails will find their way into a user’s mailbox. In the end, the user is the last measure in these defensive protection layers, and they are only as strong as the effectiveness of the phishing security awareness training provided by the organization.

REFERENCE

- https://app.letsdefend.io/training/lessons/phishing-email-analysis
- https://www.linkedin.com/pulse/phishing-email-simple-analysis-asif-ali/
- https://www.imperva.com/blog/our-analysis-of-1019-phishing-kits/