

Task 2: Analyze a Phishing Email Sample.

Author

Sakshi Dhananjay Kamble

M.Sc. Cybersecurity, University of Mumbai

ElevateLabs

Objective

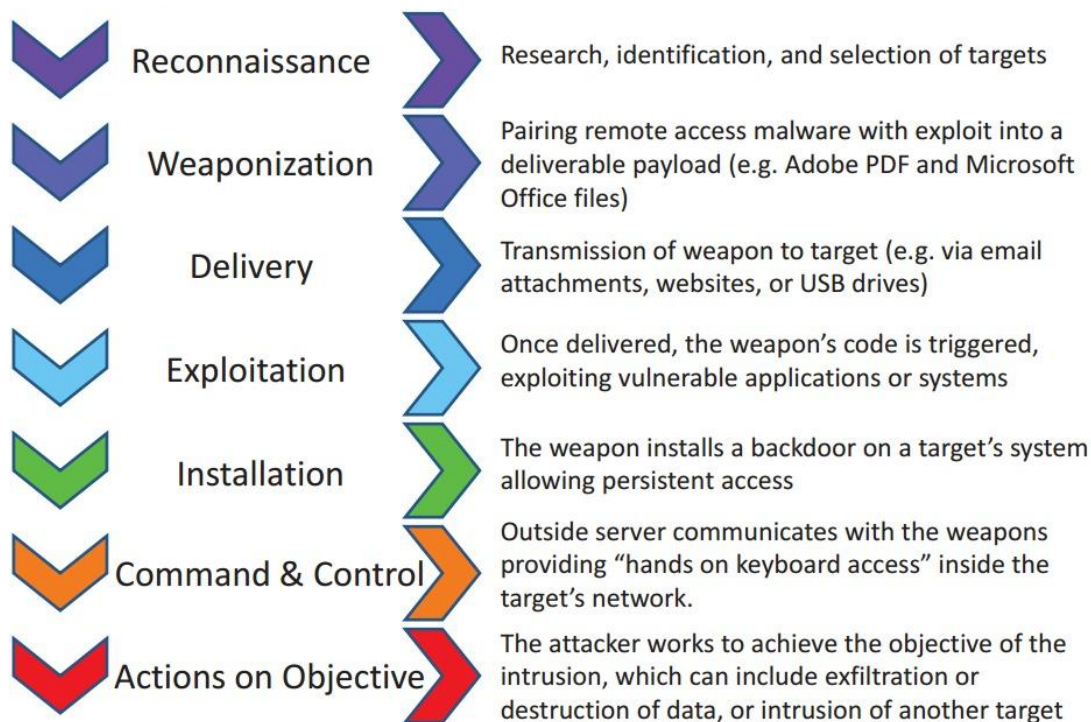
To identify phishing characteristics in a suspicious email sample by analyzing the sender, content, and headers.

Introduction to Phishing

A phishing attack is a type of attack that usually aims to steal the user's personal information by tricking them into clicking on malicious links in emails or running malicious files on their computer.

Phishing attacks fall into the "Delivery" phase of the Cyber Kill Chain model created to analyze cyber-attacks. The 'delivery' phase is where the attacker transfers the pre-arranged malicious content to the victim systems/people.

Phases of the Intrusion Kill Chain



The attackers usually aim to get victims to click on the malicious link in the email by using tricky phrases such as "you have won a gift", "don't miss out on the big discount", "if you don't click on the link in the email your account will be suspended".

Last Day for Your Special \$ 200 Coupon! | [View Online](#)


DON'T GET
HOOKED

With the link prepared by the attackers, the harmful address may actually seem harmless.

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

<http://popularshoppingsite.com>

Phishing is the most common initial attack vector.

Of course, the purpose of the attack is not to steal the user's password information, but to exploit the human factor, the weakest link in the chain. Attackers use phishing attacks as a first step to infiltrate systems.

Information Gathering

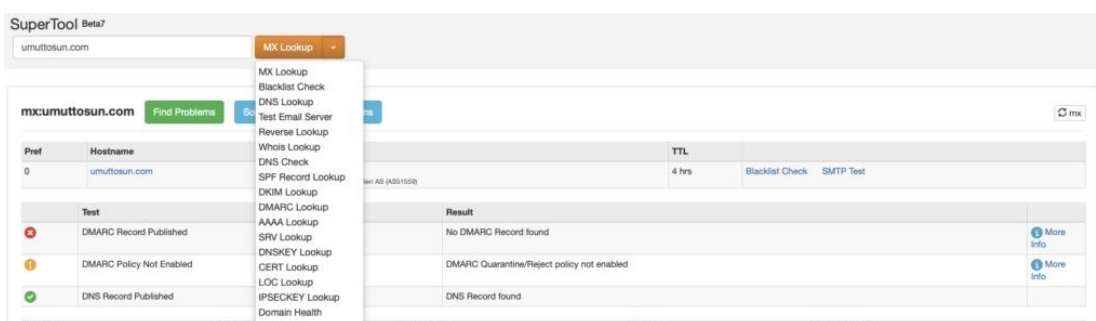
Spoofing

Because emails do not necessarily have an authentication mechanism, attackers can send emails in the name of someone else. Attackers can do this by using a 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. The SPF, DKIM, and DMARC protocols can be used to determine whether the sender's address is fake or real. Some email programs check emails automatically. However, the use of these protocols is not mandatory and can cause problems in some cases.

Sender Policy Framework (SPF)

DomainKeys Identified Mail (DKIM)

To manually determine if a mail is spoofed or not, the SMTP address of the mail should first be identified. The domain's SPF, DKIM, DMARC, and MX records can be obtained using tools such as Mxtoolbox. Comparing this information will tell you if the email is spoofed or not.



SuperTool Beta7

umuttosun.com

MX Lookup

mxmuttosun.com Find Problems

Test	Result
DMARC Record Published	No DMARC Record found
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
DNS Record Published	DNS Record found

As large institutions using their own mail servers will have their own IP addresses, you can check whether the SMTP address belongs to that institution or not by looking at the Whois records of the SMTP IP address.

It is also worth noting that even if the sender's address is not spoofed, we cannot say that the email is safe. Harmful emails can be sent in the name of trusted individuals by hacking corporate/personal email addresses. Such cyber-attacks have happened in the past, so it is always worth considering the possibility.

E-mail Traffic Analysis

Many parameters are needed to analyze a phishing attack. 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)

In addition to the email numbers, 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 PasteBin.

Attackers can find email addresses using the Harvester tool on Kali Linux. Posting personal email addresses on websites could provide a potential attack vector for attackers, so it is recommended that such information is not explicitly shared.

If the emails are sent out of office hours, the attacker may be in a different time zone. By gathering this sort of information, you can begin to figure out the nature of the attack.

What is an Email Header and How to Read Them?

In this lesson, we will explain the header information in an email, how to access it, and what you can do with it. 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?

The header is a section of the email containing information such as sender, recipient, and date. There are also components such as 'Return-Path', 'Reply-To', and 'Received'. Below you can see the header details of an example 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=2xH9+3UjmlxSK/Y/LeaLuupLgQT9gWm71ZagKamcTCU/4Tp5WIYpWxZe7PKv4gz30h
4jUC3QK1Zmit8KREmbs4RRQz8E7Varx+b22pejUitxWixYcoOWt25rWx1Uuu29vdt
OUGWQYjgJfJLQeAdRSPOaPwKBrLbgfluZv7R5A9sYjVgf9jE/JfY2HqBiHWVK/26v55
FHT7BAvChCadh7ronXI4FfxggfVgh7yEAKo6qHmtWA3CuseMKh18P4M2ZLNAMtx2t0
Ej5Mi1M8BR/njjetLwcuyNh37acMD7fuB4Atsu+4FS4sa8dFA9J3Swr7WAUNL4znh7bg
vlpq==
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=pass header.i=@letsdefend.io header.s=google header.b=hRM0gQ3u;
b=DqbcXk7COpYCaegIw+c82nMDStr6SGHNR4p+jgBagtDim3/TXsiJwXKJjV/Yj6Hrp9
YNm2RuORLLdAjChuk1cl7wngpFLP2678iuqSvzPBFEbmgjRzh/20eIaNBpkEMlaDo
4a6MNUz1/DJmLVqckq7s5HyPuckTGhpriJQDC/7aubWiaXuoZwXvnt9V2GsHoxvORh
dph2LsXWAdYDc6sAgctWR7wIve4zoDBw/evWoH/g55aChuX8KGB7OPuF3G12fo0F296
EAVSovT/zvPl0/MN6oaSOWIYoYshYfm36ceOtbFLqYhxs1D+NeXEak8seecPz14Lg
INEg==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@letsdefend.io header.s=google header.b=hRM0gQ3u;
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 d7-20020ac85447000000b002de980041b8sor9866778gtq.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=hRM0gQ3u;
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=HIAfG0lDaK3JqLpH5fJuRxiVU9cb88FSU4V8M1V9sI=;
b=hRM0gQ3uKLF8Sba7f/J1WB2QkC0Rr8IR6YqBJLHTp9e9r9Vwpc6gHPYHsxcxOdgt0
7vwxkKhRrBLJwGjQXeVv+MNBXKLS2fiLW3B3esnnMdrmyysJLuRuvyRv2LaLqY9gCc
1W0y01WFT/990pSh4GQMJPYSYQLPb2TwEWC2UdFCHTE4YHuxB1PUV2261whpbqNdxGy
jCkBB14DN0AM3ou5tu6hVzr6kgreS7TrShGz/73btM0JnoExH/XU+V8RmYp60e13Av
```

What does the Email Header do?

Allows you to identify the sender and recipient

Thanks to the "From" and "To" fields in the header, you can find out who is sending an email and who is receiving it. If we look at the email above, which you have downloaded in "eml" format, we can see that it was sent from "ogunal@letsdefend.io" to "info@letsdefend.io".

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

Spam Blocker

It is possible to detect spam emails using header analysis and various other methods. This prevents people from receiving SPAM emails.

Allows You to Track an Email's Route

It is important to check the route an email takes to see if it came from the correct address. If we look at the example email above, we can see that it came from the address "ogunal@letsdefend.io", but it is still not certain whether it came from the domain "letsdefend.io" or from another fake server that imitates the same name. We can use the header information to answer this question.

Important Fields

From

The 'From' field in an Internet header shows the name and email address of the sender.

To

This field in the mail header contains the details of the recipient of the email, including their name and email address. Such as CC (carbon copy) and BCC (blind carbon copy) also fall under this category, as they all contain details of your recipients.

To find out more about carbon copy and blind carbon copy, see [How to use CC and BCC](#).

Date

This is the timestamp showing when the email was sent.

In Gmail, it usually follows the format day dd month yyyy hh:mm:ss

So if an email was sent on 16 November 2021 at 4:57:23 pm, it would show up as Wed, 16 Nov 2021 16:57:23.

Subject

The subject is the topic of the email. It summarises the content of the entire message body.

Return-Path

This email header field is also known as Reply-To. When you reply to an email, the reply is sent to the address specified in the Return-Path field.

Domain Key and DKIM Signatures

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 is a unique combination of letters and numbers that identifies each email. No two emails will have the same Message ID.

MIME-Version

Multipurpose Internet Mail Extensions (MIME) is an Internet coding standard. It converts non-text content, such as images, videos, and other attachments, into text so that non-text content can be attached to an email and sent via SMTP (Simple Mail

Transfer Protocol).

Received

The Received section lists each mail server that an email has passed through before arriving in the recipient's inbox. It's listed in reverse chronological order - the mail server at the top is the last server the email message passed through, and the mail server at 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.

It then shows the spam score of the email and the spam threshold for the email.

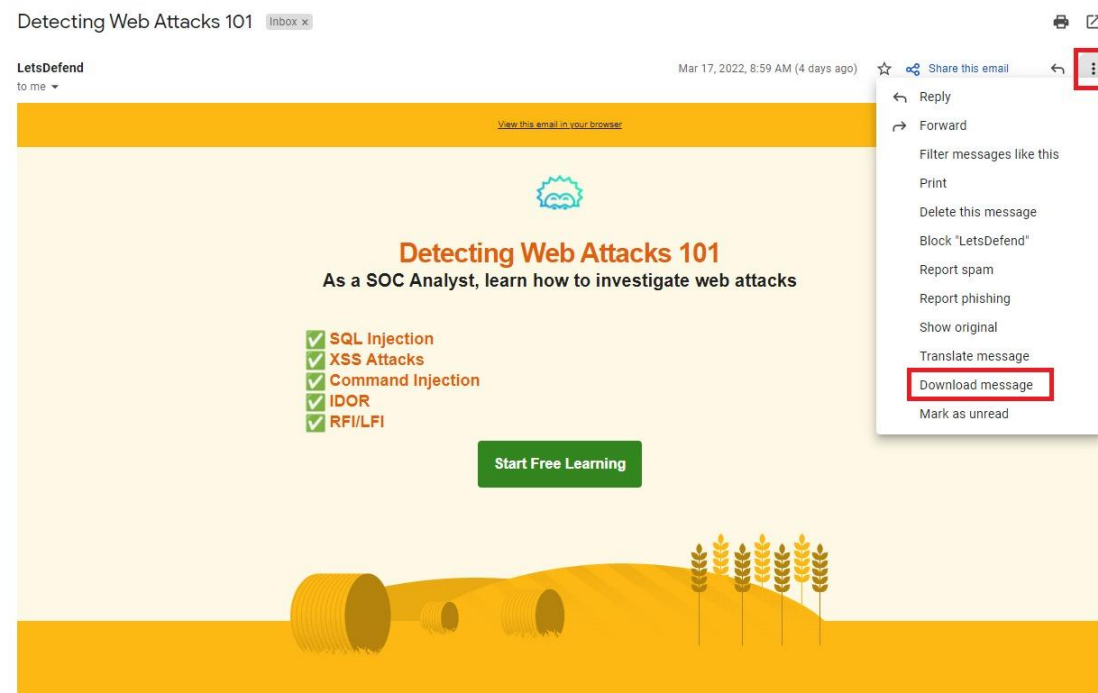
An email can either meet or exceed an inbox's spam threshold. If it's too spammy and exceeds the threshold, it's automatically classified as spam and sent to the Spam folder.

Field Definitions: gmass.co

How to Access Your Email Header?

Gmail

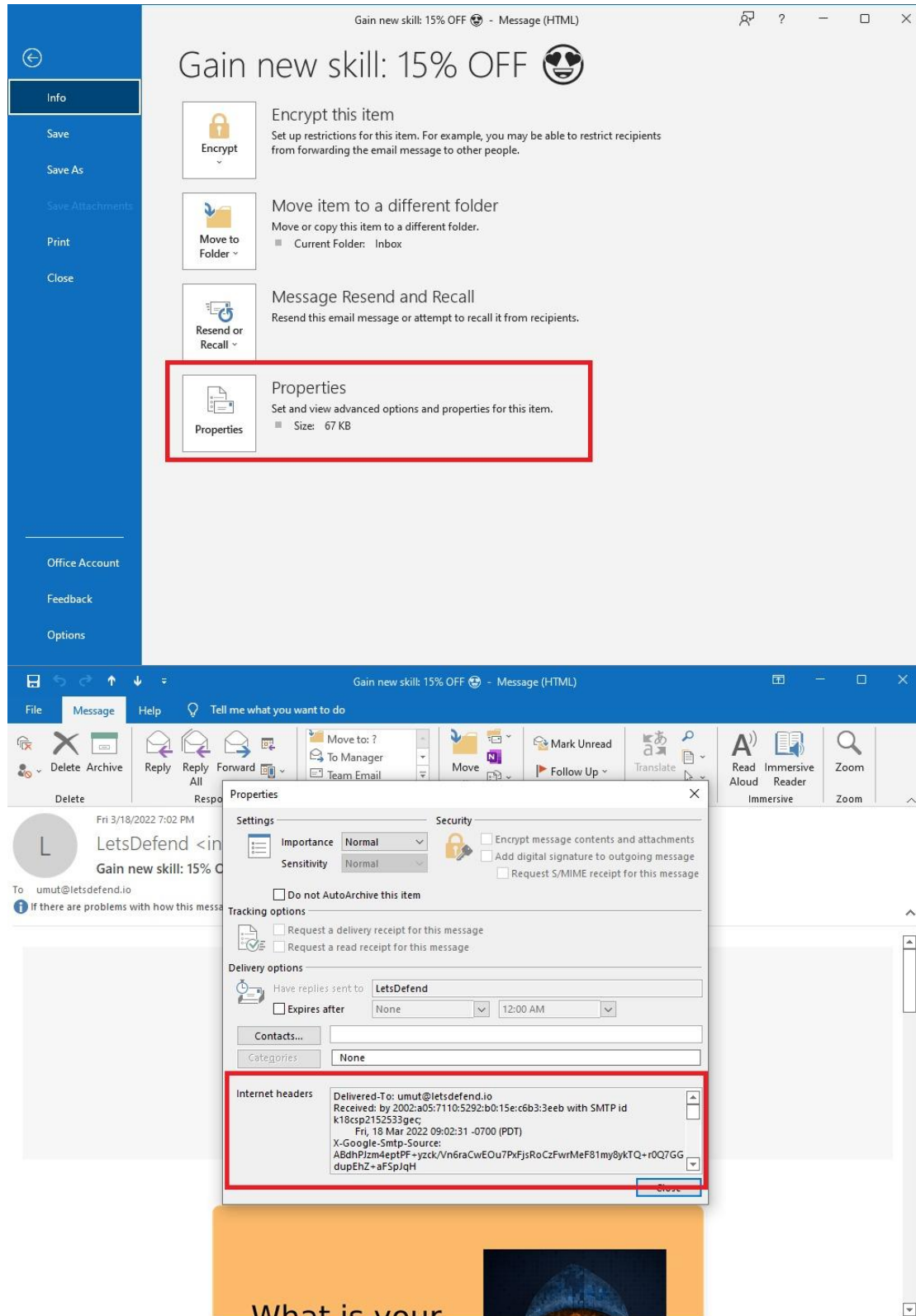
- 1- Open the email in question
- 2- Click on the 3 dots at the top right "..."
- 3- Click on the "Download message" button.



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

Outlook

- 1- Open the email in question
- 2- File -> Info -> Properties -> Internet headers



Email Header Analysis

In the previous lesson, we looked at what a phishing email is, what the 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:

Note: Connect to the lab machine with the connect button below. Use the "C:\Users\LetsDefend\Desktop\Files\Mail-Analysis.zip" file to analyze the email. (File Password: infected)

Was the email sent from the correct SMTP server?

We can check the "Received" field to see the path the email took. As you can see in the image below, the email came from the server with the IP address "101[.]99.94.116".

```
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 can see that it is coming from the domain "letsdefend.io".

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

So, under normal circumstances, "letsdefend.io" should be using "101[.]99.94.116" to send mail. To confirm this, we can query the MX servers that "letsdefend.io" is actively using."

"mxtoolbox.com" will help you by showing you the MX servers used by the domain you are asking for.

SuperTool Beta7

letsdefend.io

mx:letsdefend.io

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 domain "letsdefend.io" uses Google addresses as its email server. So there is no relation with the addresses emkei[.]cz or "101[.]99.94.116".

This examination showed that the email did not come from the original address, but was spoofed.

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

Except in exceptional cases, we expect the sender of the email and the recipient of the replies to be the same. Here is an example of how these parts are used differently in phishing attacks:

Someone sends an email (Gmail, Hotmail, etc.) to LetsDefend with the same last name as someone who works for Google, LetsDefend tells the employee that they have issued the invoice and they need to pay to their XXX account. It inserts the real Google employee's email address in the "Reply-To" field so that the fake email address will not stand out when the email is replied to.

Going back to the email we downloaded above, all we need to do is compare the email addresses in the 'From' and 'Reply-to' sections.

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, if we want to reply to this email, we will send a reply to the gmail address below. Please note that just because this data is different doesn't always mean that it's definitely a phishing email, we need to look at the event as a whole. In other words, in addition to this suspicious situation, if there's a malicious attachment, URL, or misleading content in the content of the email, we can understand that it's a phishing email. In the next lesson, we will analyze the data in the body of the email.

Static Analysis

Many people find plain text boring, which is why email programs offer HTML support, allowing you to create emails that are more likely to grab the user's attention. Of course, there is a downside to this feature. Attackers can use HTML to create emails that hide malicious URLs behind buttons or text that appear to be 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](https://maliciousaddress.com/email=personal_email@gmail.com)

By querying VirusTotal for web addresses in emails, you can find out if the antivirus engines detect the web address as harmful. If someone else has already analyzed the same address/file in VirusTotal, VirusTotal will not analyze it from scratch, it will show you the old analysis result. This feature can be considered both an advantage and a disadvantage.



If the attacker searches the domain address in VirusTotal when it does not contain malicious content, this address will appear to VirusTotal to be harmless. However, if you miss this tiny detail, you could be fooled into thinking that this address is harmless. In the image above you can see that the address umuttosun.com appears to be harmless, but if you look at the section marked with a red arrow you can see that this address was scanned 9 months ago and this result is 9 months old. To scan it again, click the blue arrow button.

If the site was previously scanned by VirusTotal, it could mean that the attacker wanted to see the detection rate of the site during the preparation phase. If we analyze it again, the antivirus engine will detect it as phishing, which means that the attacker tried to trick the analysts.

Performing a static analysis of the files in the email can provide insight into the capacity/capability of the file. However, since static analysis takes a long time, dynamic analysis can provide the information you need more quickly.

Cisco Talos Intelligence has search sections where we can learn the reputation of IP addresses. By looking up the SMTP address of the email we detected in Talos, we can see the reputation of the IP address and find out if it is on the blacklist. If the SMTP address is blacklisted, it can be assumed that the attack was carried out 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.ov0.sg
DOMAIN	ov0.sg
NETWORK OWNER	Floknet 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
SPAM LEVEL	None
EMAIL VOLUME	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

Similarly, the SMTP address can be searched on VirusTotal and AbuseIPDB to find out if the IP address has been involved in malicious activity in the past.


Dynamic Analysis


URLs and files in an email need to be checked to make sure they are safe. 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 to the system should be examined to see if they are harmful or not.


[Features](#) | [Pricing](#) | [Live API](#) | [About Us](#) | [Sign In](#) | [Sign Up](#)

Live interactive cross-browser testing

[Test now!](#)


Windows 7


Chrome

75

Get a browser and start testing in 5 seconds!

You can use online web browsers such as Browserling to quickly check the web addresses in the email. The advantage of such services is that you are not burdened by a possible zero-day vulnerability that would impact browsers, as you are not visiting the website on your own computer. On the other hand, the disadvantage of using web browsers such as Browserling is that if the malicious file is downloaded from the website, you will not be able to run it. This could interrupt your analysis.

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](https://maliciousaddress.com/email=personal_email@gmail.com)

Before going to the links in the email, you should check if there is any important information in the URL. If we examine the example in the image above, and the user's email address in the email parameter. So even if the user does not enter their password on the phishing page, when they click on popularshoppingsite[.]com and visit the website, the attacker will know that this user is valid. The attacker can increase the success rate of the attack by social engineering the valid users in later attacks. Therefore, it is important to change information such as email addresses before accessing websites.



Sandbox environments allow you to examine suspicious files and websites without the risk of infecting your computer with malware. Many sandbox services/products are available for both paid and free use. You can choose one or more of these services according to your needs.

Some commonly used sandboxes:

VMRay

JoeSandbox

AnyRun

Hybrid Analysis(Falcon Sandbox)

Malware can wait a certain amount of time without taking any action to make detection more difficult. You have to wait for the malware to take action before you decide that the file being scanned is not malicious.

Also, the fact that there are no URLs and files in the email does not mean that it is not malicious. The attacker may also send the malware as an image to avoid detection by the analysis tools.

Additional Techniques

In addition to the phishing attack techniques mentioned in the previous lesson, attackers can also use normally legitimate websites. Some of these include:

Using services that offer cloud storage services such as Google and Microsoft

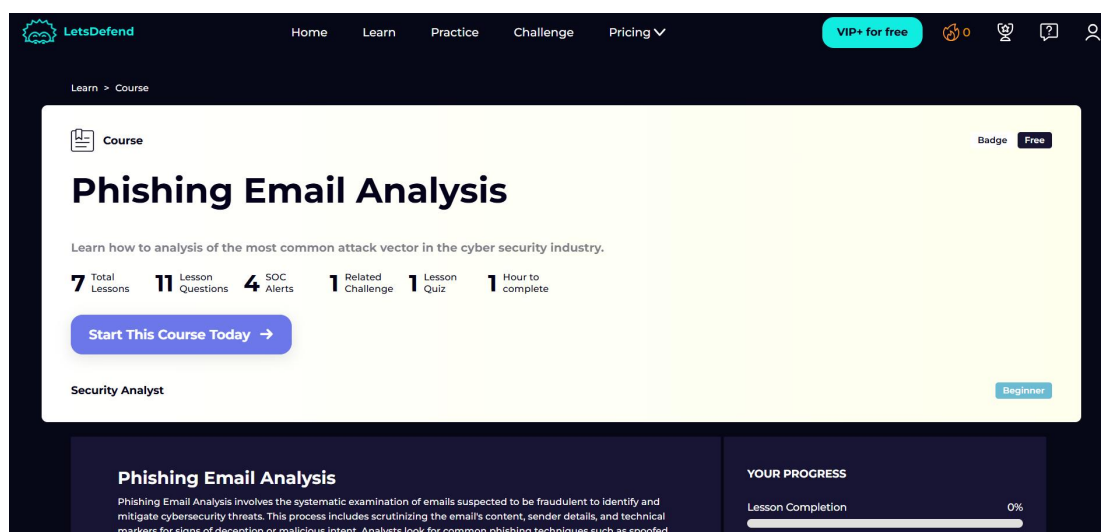
Attackers attempt to trick users into clicking on Google / Microsoft Drive links that appear to be harmless to trick the user into downloading malicious files.

Using services that allow the creation of 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, analysts can be tricked into believing that these addresses have been taken in the past and belong to institutions such as Microsoft, WordPress, and others.

Form applications

Various services allow free-form creation, and attackers benefit from this rather than creating a phishing site themselves. As the domain is usually harmless, it can be forwarded to the user without triggering anti-virus software. Google Form is an example of such a service. As the Whois information shows that the domain is Google, the attacker can mislead analysts.



Key Concepts

- Phishing

00..

- Email spoofing
 - Header analysis
 - Threat detection
 - Social engineering
-

Disclaimer

This analysis was conducted in a controlled, educational setting. Do not attempt to open real phishing emails without appropriate precautions.
