



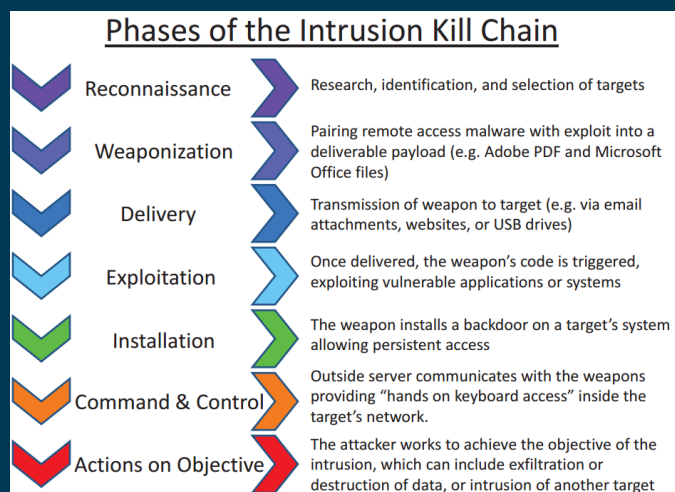
PHISHING CAMPAIGN ANALYSIS



LETSDEFEND

PHISHING ATTACK

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.

The attackers generally aim to click on the harmful link in the mail, such as "you have won a gift", "do not miss the big discount", "if you do not click on the link in the mail your account will be suspended" to direct users to click on the links in the mail.


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.



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.

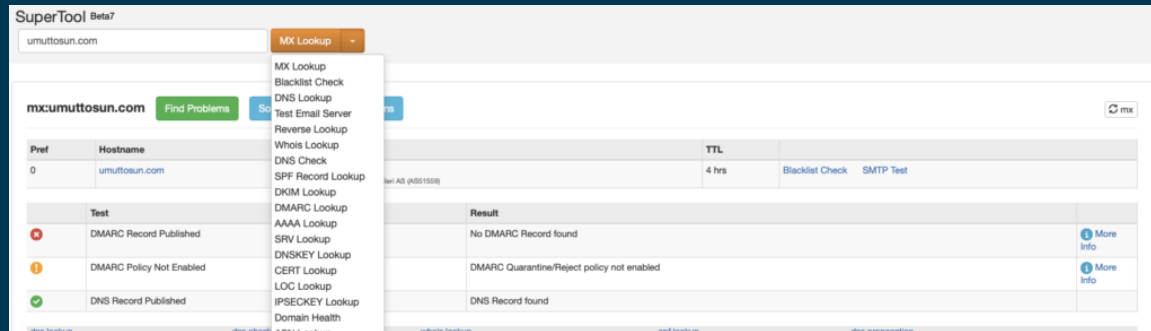
- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)

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.



INFORMATION GATHERING





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(info@letsdefend.io)
 - SMTP IP Address(127.0.0.1)
 - @letsdefend.io (domain base)
 - letsdefend (Besides the gmail account, attacker may have sent from the hotmail account)
 - Subject (sender address and SMTP address may be constantly changing)

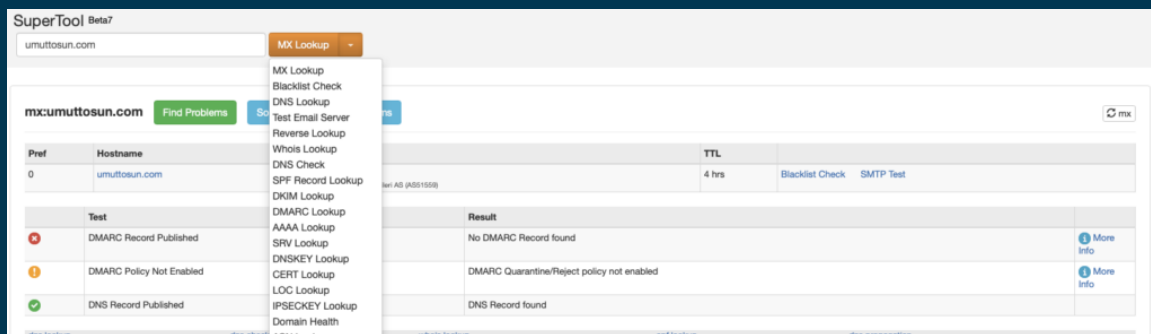
In the search results, it is necessary to learn the recipient addresses and time information besides the mail numbers. If harmful e-mails are constantly forwarded to the same users, their e-mail addresses may have leaked in some way and shared on sites such as PasteBin.

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.

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.



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.



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.



If the page was previously searched on VirusTotal, it may mean that the attacker wanted to see the rate of detection of the site during the preparation phase. If we analyze it again, antivirus engine detects it as phishing, which means that the attacker has a move to trick analysts.

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

Flocknet 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

CB.LABUSEAT.ORG

Not Listed

PBL.SPAMHAUS.ORG

Not Listed

SBL.SPAMHAUS.ORG

Not Listed

TALOS SECURITY INTELLIGENCE BLACKLIST

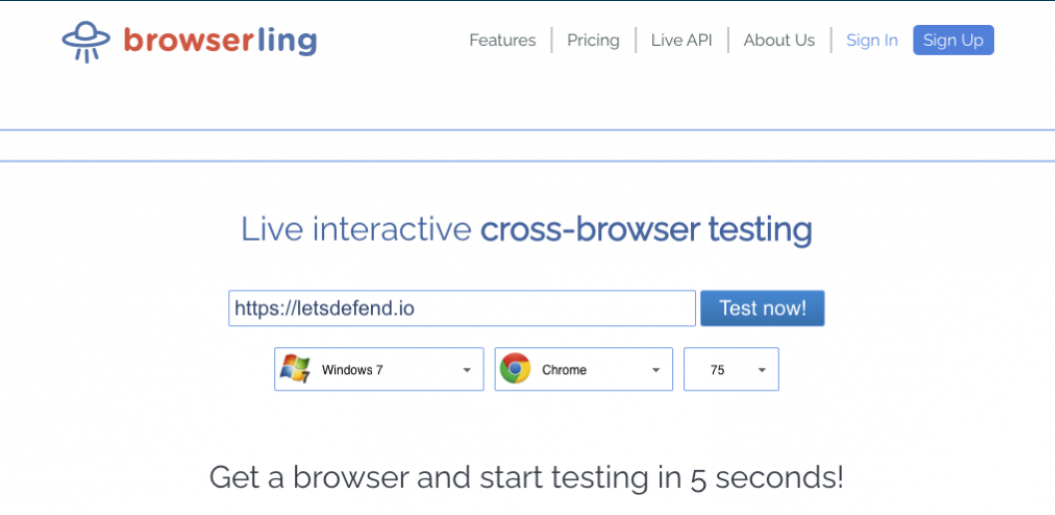
BLACKLISTED

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.

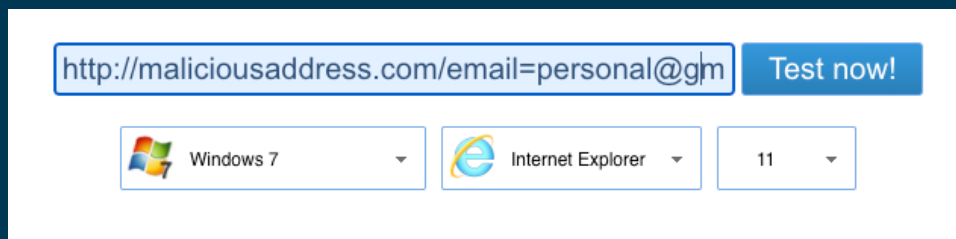



The screenshot shows the Browserling website interface. At the top, there is a navigation bar with the Browserling logo (a blue alien head) and the text "browserling". To the right of the logo are links for "Features", "Pricing", "Live API", "About Us", "Sign In", and a blue "Sign Up" button. Below the navigation bar, the main heading reads "Live interactive cross-browser testing". Under this heading is a text input field containing the URL "https://letsdefend.io" and a blue "Test now!" button. Below the input field are three dropdown menus: the first shows the Windows 7 logo and "Windows 7", the second shows the Chrome logo and "Chrome", and the third shows the number "75". At the bottom of the interface, a message states "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.



Before going to the addresses in the mail, it should be checked whether there is important information in the address. When we examine the example in the image above, when the user clicks on popularalisverissitesi.com, it is seen that the address of the user is actually visited, and the email address of the user in the email parameter. Even if the user does not enter his / her password on the phishing page, it means that the link in the mail is accessed when this address is reached and the attacker understands that this user is valid. It can increase the success rate of the attack it will carry out by doing social engineering attacks over the users that are valid in the attacks it will carry out later. For this reason, it is necessary to change the information such as e-mail address before accessing the addresses.



The image shows a screenshot of a phishing page. At the top, there is a text input field containing the URL `http://maliciousaddress.com/email=personal@gm`. To the right of this field is a blue button labeled "Test now!". Below the URL field, there are three dropdown menus. The first dropdown menu shows the Windows logo and the text "Windows 7". The second dropdown menu shows the Internet Explorer logo and the text "Internet Explorer". The third dropdown menu shows the number "11".



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)

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.

- 
- 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.
 - 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.
 - 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.

