Study of Phishing Attack

[1]Dishant Vakte, [2]Aniket Thakker

[1]Student, [2]Student,
[1]Information Technology,
[1]Shah and Anchor Kutchhi Engineering College, Mumbai, India.

Abstract : The extensive use of internet has positive as well as negative sides to it. Cyber-attacks have become very popular these days as everything has gone online. Cyber-attack is an attack made by cyber-criminals on internet users. Cyber-attacks consist of a number of attacks like denial-of-service attacks, ransomware, MITM, phishing, etc. Phishing consists of the hacker pretending to be someone who he is not and trying to gather personal information and credentials from potential victims. Phishing is venerable, but increasingly sophisticated form of cyber-attacks. With general precautionary measures these attacks can also be prevented.

***IndexTerms* –Phishing, Fraudulent emails, phishing-kits, clone websites.**

I. Introduction

Phishing can be classified as a kind of social-engineering attack which is used to gain personal information or credentials of victims by acting as a trusted entity. This stolen information such as credit card numbers, passwords and other sensitive data is used for the attacker’s personal benefit. Phishing utilizes feigned email as a tool. The aim is to delude the email recipient into assuming that the message is something they want or need like an inquiry from their bank, an email from their office, etc. and to click a link or download an attachment.

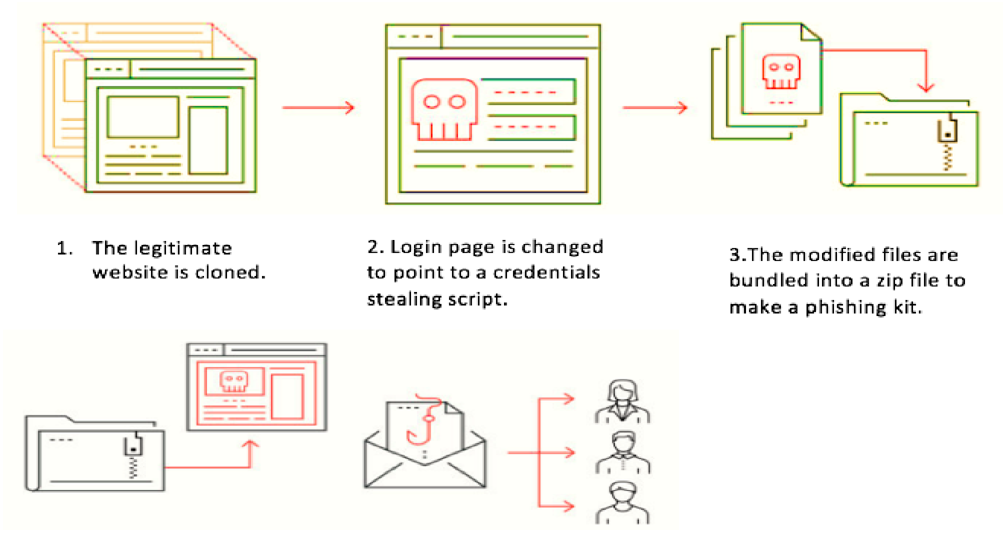
What really characterizes phishing is the form the message takes. The attacker impersonation as a credible entity of some sort, many a times a real or believably real individual, or an enterprise the victim might do business with.

II. Theory and Study

1. Phishing kits

Phishing kits make it easy for an attacker to start a phishing attack even without the need of too much technical knowledge. A phishing tool consists of phishing website resources and tools. After successful installation of these tools on the server, the attacker only has to send emails to a number of people. Websites like OpenPhish and Phishtank contain lists of known phishing kits. The dark web is used to obtain the phishing kits and the mailing list as well. Some kits allow the user to use well known enterprise names to spoof as it increases the chance that a person might fall prey to it.

The phishing kits can be analyzed and the users of the kits can be tracked. Where the credentials are being sent can also be found by examining the phishing kits. We can also see where credentials claim to be sent from.



1. The legitimate website is cloned.

2. Login page is changed to point to a credentials stealing script.

3.The modified files are bundled into a zip file to make a phishing kit.

4. The phishing kit is uploaded to the hacker’s website, files are unzipped.

5. Emails are sent with links pointing to the new spoofed website.

2. Phishing Kits

2.1 Handover Sensitive Information

In this the aim of the attacker is to trick the user/or person using the site to reveal/share sensitive/personal information most often username and password which can then be used by the attacker to gain access to the owners account or to breach system account.
For eg. A bank phishing mail, Here the attacker sends millions of people mails containing bank's link hoping that even few users might be banks customers and may click the link, which will redirect them towards a fake website that looks like original banking site when user enters account information the attacker gains this access and misuses it for own benefits.
This type of attack is known as HOSI or Hand Over Sensitive Information attack.

2.2 Download Malware

In this type of attack the attacker tries to attack the user's computer by making the victim download or infect their own device with harmful malware. Most of such codes are "soft-targeted" i.e they might be sent with an attachment usually in a .zip file or a Microsoft document .docx file.
Such files contain embedded code that once open infects the victim's device. The most common malicious code is ransomware, in 2017 during ransomware attacks it was believed that 93% of all the phishing email contained ransomware code.
In Ransomware the attacker locks the victim out of his/her own data and demands money to give access to the information. In 2017 most of the world's companies fell for this and were attacked using ransomware.

2.3 Spear Phishing

When the attacker craft a message personally for the targeted individual rather than bait and hook method, it is known as spear phishing, in this phishing the attacker makes victim believe that the mail is from his co-workers, friend, family by fraudulent mails.

2.4 Whaling

When spear phishing is used on a very high order target such as CEOs of bank/MNC's, board members who are particularly vulnerable, such spear phishing of high value targets is known as Whaling. Whaling chances of success are low but the outcome is generally higher.

3. Avoiding Phishing Attacks

Phishing attacks can be avoided by taking certain precautions on user as well as enterprise levels. Users must be cautious to look for small mistakes in the spoofed messages like small changes in the domain name in the URLs.

Enterprises can take the following steps:

1. Two factor authentication is one of the efficient ways to avoid phishing attacks due to the verification process it contains when logging in to applications. It is mostly based on passwords and usernames. Even when credentials are compromised, these credentials alone are insufficient to gain access.

2. Severe password management policies must be implemented and users must be enforced to change their passwords after certain time intervals and reusing of passwords must not be allowed for various applications.

3. Enlightening the users about these malpractices and creating awareness can also be helpful in preventing phishing attacks. Secure practices must be enforced like avoiding opening external email links.

Few simple ways to avoid falling prey to phishing are:

1. Be well informed about the various phishing techniques as new techniques are developed all the time. By knowing about them in advance you may lower your risk of falling prey to one.

2. Avoid clicking on links from unknown entities as they may lead you to a clone website of a legitimate website, created by a hacker which may be used to steal your login credentials. Go directly to the source rather than clicking the potentially dangerous link sent to you via email. Avoid downloading files from untrusted sources.

3. Installing an Anti-Phishing toolbar might help as it compares the site you are visiting to the lists of known phishing websites, if the site is found to be dangerous, the toolbar sends an alert to the user.

4. Anti-spyware and firewalls can to helpful in preventing phishing attacks. These must be updated time to time as new ways to scam are developed all the time. Firewall prevents the access to malicious files as it blocks the attacks and act as a buffer between the user and the attacker. Antivirus scans all the files that you receive via the internet.

5. All the secure websites start with 'https'. Checking the address of the website before entering details must be an habit. Never give out personal or financial information on the emailed links or anywhere on the internet. Companies will never email you asking for your personal or financial information.

6. Pop-ups usually masquerade as components of a legitimate website, most of the times they are just phishing attempts. Avoid clicking on these pop-ups as most often they lead you to phishing sites. Most of the popular browsers have a feature that allows the user to block pop-ups.

7. Keep a habit of personally checking your bank statements on regular basis no ensure no fraudulent transactions is made without your knowledge.

4. Detection of phishing attacks

Detection of phishing is tough as the sites are visually similar to that of original website but the detection can be still done.

1. No company/organization will contact you through open email domain like “@gmail.com”

2. All companies use their own personal email domain that provides extra layer of security.

3. Check for spelling errors, spelling errors are the most common way pf spotting phishing attacks

4. Attachments or links are attached without any reasons particularly “.zip” files and/or “.docx” files

5. No SSL on the webpage must be a strong indicator as the site you’re visiting is a phishing site, SSL encrypts all data transfer which makes your account information encrypted but phishing websites do not use SSL.

6. Terms and conditions are missing, unavailable or unfavorable, T&C are present on every authentic site and missing T&C’s should be a strong indicator of a phishing website.

III. CONCLUSION AND SUMMARY

5. Summary

Phishing might be a negative aspect of internet, but with just proper care, knowledge and attention we can prevent phishing. The reach of internet is increasing day by day and with internet the risk of phishing increases too. A simple way to avoid phishing scams is to make people aware about it. Simple methods like not downloading untrusted content, not sharing private information on the internet and not replying to emails from unknown entities. Many machine learning algorithms and artificial intelligence methods have been developed to take down clone and fraudulent websites. Social networking websites are taking major steps to eliminate fake accounts and bots. Even emails are passed through spam detection softwares. Ad block extensions for browsers could also be of great help. We should take necessary precaution while browsing the internet as not to fall prey to one of these scams.

REFERENCES

[1] A. S. Alazri, “The awareness of social engineering in information revolution: Techniques and challenges,” 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015.
[2] P. Mcfedries, “Technically Speaking: Gone Phishin',” IEEE Spectrum, vol. 43, no. 4, pp. 80–80, 2006.
[3] A. Papanikolaou, V. Vlachos, A. Papathanasiou, K. Chaikalis, M. Dimou and M. Karadimou, "Cyber crime in Greece: How bad is it?," 2013 21st Telecommunications Forum Telfor (TELFOR), Belgrade, 2013, pp. 1-4.
[4] B. Sahu, N. Sahu, S. K. Sahu and P. Sahu, "Identify Uncertainty of Cyber Crime and Cyber Laws," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 450-452.