Phishing-Types and Methods for Detection

Mariadas Ronnie C.P
Asst. Professor, Dept. of MCA
SCMS School of Technology and Management,
SSTM, Muttom, Aluva.

Jincy Rachel Varghese
P G Scholar, Dept. of MCA
SCMS School of Technology and Management,
SSTM, Muttom, Aluva.

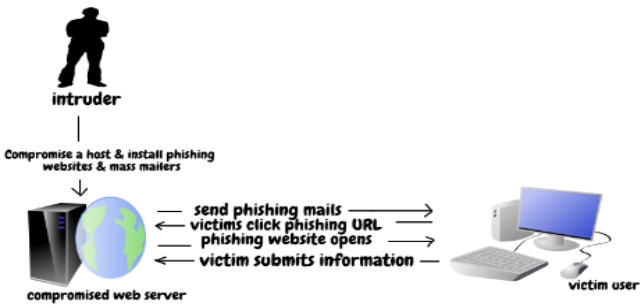
***Abstract*—Today, the most common method used by many intruders to get the personal information about various users is by sending emails. This method is known as phishing. In this, the intruders try to gain vital information about the users. It may include passwords, username, bank account details and so on. Today, there are different kinds of phishing techniques that have been developed which are difficult to trace even for an educated person. One of the main challenging issues in this area is to detect phishing with high accuracy. This is because the phishing website and the corresponding website look so similar in appearance. Some of the features set like text format, text content, CSS, HTML tags, image and so forth are utilized by various phishing techniques based on visual similarity.**

Keywords-anti-phishing, history, types of phishing, link count checker.

I. INTRODUCTION

In today's cyber-world, phishing is one of the main problems and it causes financial and other personal losses to both individuals and industries. Phishing can be briefly explained as sending fake e-mails by intruders, which may appear to be e-mails coming from corresponding organization and ask the users to enter their personal information by specifying some security reasons. This information includes username, password, bank account details and other confidential details. This fake email looks exactly similar to the legitimate one, which is enough to fool even an educated person. Phishing can not only propagate through emails, but also through SMS, social networking sites, instant messengers, VoIP and so forth. But the most common way of propagating phishing is through e-mails. It is said that about 65% of phishing is achieved by fooling the users to click on the hyperlink attached to the e-mails. There are different kinds of phishing techniques currently available. Among them, spear phishing is very popular nowadays.

In 2015, Business e-mail compromise (BEC) was considered as a major threat. In BEC, the intruders used spear phishing methods to fool individuals, organizations or both. A particular individual within the organization are also targeted by more sophisticated spear phishing techniques. It is similar to fishing in the water, but here, instead of catching the fish, the intruders try to obtain personal information of the users. In this, when a user click on the link attached to the e-mail and provide their necessary details, those credentials are obtained by the intruders on the other side. The intruders then use these credentials to do their malicious purposes.



II. BACKGROUND AND HISTORY

One of the key issues in the computer technology since early 90's is security. During this period, the computer had different methods to make sure that a particular application is not able to use memory which are not allotted to it. In order to protect passwords several encryption and access control techniques were developed in 1960's. In 1970's, the computers were studied as a new complete domain. The concept of "phone phreaking" was a common term from 1950's till 1960's.

In 1960, the paper published by Bell included the actual frequencies used for routing the codes. In 1964, AT&T started to monitor telephone calls to find phone "phreakers". In 1978, the first international commercial spam was sent by the marketing manager of DEC, G Thuerk. In that, a single mass e-mail was created and sent to approximately 393 West Coast ARPANET users. The mail was about advertising the availability of new model of DEC computers. In 1983, a security threat called "Trojan horse" was first described by K. Thompson. In 1985, a magazine called "Phrack" begun publishing which was written by hackers and for hackers.

In December 1995, it has been reported that the hackers tried to hack DOD (US Department of Defence) computers

for about 250k times and approximately 65% of them were successful in the same year. The term "phishing" was first used by the hackers who stole America On-line (which is the largest Internet Service Provider in US) by accessing the passwords of the user in 1996. The "alt.2600" hacker group in January 1996 mentioned the term phishing on the Internet for the first time.

Also in 1997, several publications warned its users about the new security threat called phishing. It was in the year 1998, the phishers started to make use of messages to attack its victims. The phishers started to make use of mass mailers to spread phishing mails and URLs to fool its targeted users from 2000 onwards.

In 2001, the first victim among the financial institutions of phishing was e-gold. To spread their network, the phishers started sending spam messages. In 2005, Buffalo spammer was arrested for sending millions of spam mails and fraudulently using stolen identities. Because of the phishing attack, the Bank of America lost about 1.2 million usernames and SSNs of their customers in 2005.

It was in the year 2006; the phishers targeted VoIP for the first time. According to Gartner study, in 2007, about 1.5million identities of US citizen got stolen due to phishing. It was in the year 2008; S. Wallace received $711M judgement for posting spam messages on the walls of Facebook's members.

The most costly cyber hack ever was reported in the year 2011. Due to the attack of phishing, the Credit card and Debit card details of more than 10M Sony Entertainments and PlayStation Network users were stolen and caused a great loss to the respective companies. Over the pass decades, there was a dramatic increase in the numbers of phishing attacks. At first, it was concentrated mainly using spam e-mails, but now phishing attacks have evolved into much more advanced threats such as using SMS, online gaming and so forth.

According to the reports of eCrime Trends Reports in the year 2012, the phishing attacks are increasing up to 12% every year. For major financial companies and clients phishing emails are becoming a major threat day by day.

III. TYPES OF PHISHING

There are different types of phishing are available. Some of them are discussed below:

A. Spear Phishing

It is one of the most commonly used phishing attack. The attacks which target mostly a particular individual or an organization is termed as spear phishing. In this, for increasing the probability of success, the attackers may try to obtain the confidential information about their target. This is one of the most successful attacks on the internet today.

A threat group called Group-4127 who targeted email accounts attached to Hillary Clinton's 2016 presidential campaign was based on spear phishing attack. Spear phishing became a great threat to users by attacking more than 1,800 Google accounts and implementing accounts-google.com domain.

B. Clone phishing

This type of phishing attack uses previously delivered and legitimate emails containing a link or an attachment. The content and recipient address (es) is taken and this information is used to create spam mail or cloned email. The attachment or link in the email is then replaced with a malicious version and it appears to be sent from the original sender.

C. Whaling

There are several phishing attacks which exist in which the attacks have been specifically targeted at senior executives and others within the businesses and such type of phishing attacks are referred as whaling.

In this, the content of the masquerading web page/email is crafted in such a way that it can fool the target very easily. The content of the whaling emails are often appeared to be customer complaint, legal subpoena or executive issue. They are often designed to masquerade the critical business details.

D. Deceptive phishing

In this phishing attack, the fraudsters target a legitimate company and try to obtain all the confidential information about the company. This may be people's personal information or login credentials and so forth.

The success of deceptive phishing lies on how closely the spam emails resembles to the legitimate company's official correspondence. To avoid being a victim of deceptive phishing, the users should check all the URLs carefully to prevent redirecting to an unknown website.

E. Web Spoofing

Web Spoofing is one of the attacks that scrutinize and transform all the web pages that are sent to the user machine and obtain all the information entered by the users into the forms. The user may find difficult to protect themselves from such type of attacks because the user sees no suggestion or receive any messages that anything is erroneous. Once the information about the user is collected, the attacker can easily access the victim's credit card, their bank accounts and can establish false identities. Individuality theft and credit card deception are the two main risks that the user faces through this attack.

F. Tab nabbing

This type of phishing attach take the advantage of people who have manifold tabs open at any one point of time. It is

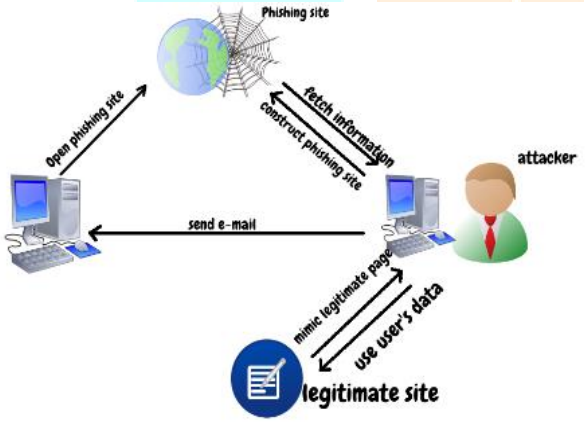
one of the recent and emerging types of phishing attack that the user should take care of. In this, the phishers misuse this propensity to obtain information of popular websites through cookies.

G. Session Hijacking

In this type of attack, all the user's activities are scrutinized until they log on to object account. This may be bank account and their credential information. After this, the malicious software takes the control and it can do unauthorized actions such as fund transfer, obtaining exclusive information about the user and so on.

IV. PHISHING MECHANISM

The mechanism of phishing is shown in the following figure. In any phishing website, the objective is to target a genuine website. The phishing website also contains some input fields. When the user inputs his/her personal and confidential information, it is then transferred to the attacker on the other side.



An attacker steals the information from innocent user by doing the following steps:

The first step is the construction of the phishing website. In this, the attacker finds or sets his target which may be a well-known organization. After conducting detailed study and collecting relevant information about the organisation, the attacker creates a fake website of the organisation which is exactly the same as that of the genuine website of the organisation. The fake website resembles exactly same which makes it difficult even for the educated people to identify the theft.

The second step is URL sending. In this step, the attacker composes a bogus e-mail and sends that to thousands of users. If the attacker uses spear phishing method, he will sends the e-mail only to a selected individual or particular target. With the help of blogs, forms and so forth, the attacker can also spread the link of the phishing website.

The third step is the stealing of the credentials. When the targeted user clicks on the link of the phishing website, he/she may find some input fields to enter some information. This field may be for login, entering back accounts, address and other personal details. Once the credentials are entered by the user, the attacker can easily access it.

The fourth step in the process of phishing is identity theft. In this, after gaining the user credentials through phishing website, the attacker can use it for their own personal interest, for example, buying products by using the credit card details of the user.

V. NEW TRENDS IN PHISHING

The concept of phishing was based on fooling the users and obtaining user details. But now phishing attacks are no longer just about fooling the innocent users. The attackers use many other techniques to obtain the user information. This may include more realistic-fake login page, malicious files, and better tricks to fool the innocent users. The targets of the phishers are changing day by day and no one would have any idea about whom they are targeting of. An example of such type of phishing is that an attack to hide a malware behind SharePoint link, which was considered to be one of the most trustworthy applications in Microsoft.

The new current trend in phishing is very simple. The attacks are slow and patient. One point to be noted is that, greater attacks always come from patient attackers. Such type of attacks may last months or even years and it can never be discovered so easily. Some patient attackers are ready to wait even for months to obtain the credentials of the users.

If the target is an organisation, the attackers may study in depth about organisation; learn about its workers and their relationship with the organisation. Once the hacker gets a clear picture about the details of the organisation, he can easily spread the phishing e-mails.

It seems to be impossible to prevent the phishing attacks nowadays because new phishing techniques are emerging day by day. But some of the anti-phishing methods can be used to prevent phishing to some extent.

VI. COMMON METHODS TO AVOID PHISHING

A. Attribute based anti-phishing techniques

This technique implements each reactive and proactive anti-phishing defences. A tool called Phish Bouncer has enforced this method. In case of false information feeder check, if the input is false data and if that false data is accepted by the corresponding website, then that website can be phished site.

Advantages: It is able to detect more phished sites when compared to other techniques. Another advantage of this technique is that it can be used for detecting both known and unknown attacks.

Disadvantages: It takes more time when compared to other techniques. This is because it performs multiple checks to authenticate sites.

B. Genetic Algorithm Based Anti-Phishing techniques

It is an associate approach of detecting phishing websites. Genetic algorithm usually contains easy rules that can be used against preventing phishing attacks. These rules differentiate a traditional website from a fake website. These fake website visits events with likelihood of phishing attacks. This rule can be explained as follows: if the e-mail have associated with information processing the address of the URL and if it matches with the set of rules for the white list, then we can conclude that the received mail is an authenticated one.

Advantages: One of the exiting features of this technique is that it notifies the user about the malicious link before user reads the mail. This method can also be used to detect malicious web link.

Disadvantages: A single rule is far from enough for phishing detection. As more and more phishing techniques are emerging day by day, we need multiple set of rules.

C. An Identity Based Anti-Phishing Techniques

Identity Based Anti-Phishing Technique is based on mutual authentication methodology where every other's identity is validated by each user and on-line entities throughout the handclasp. To stop phishers from masquerading as legitimate on-line entities, it also associate Nursing anti phishing technique.

Advantages: For both sever as well as client it provides mutual authentication. And using this technique, the user need to provide the password for the first time when the session is initialised.

Disadvantages: In this, the phishing technique can be compromised if the hacker gain access to the client computer and disable the plug-ins of the browser.

D. Content Based Anti-phishing Approach

A tool called GoldPhish implements this method and it provides security to internet sites that are well-established. It is based on the fact that, the phishing web contents are active only for short amount of time and it can acquire low rank throughout net search.

Advantages: It does not result in false positive and it provides zero day phishing.

Disadvantages: It delays the performance of the website.

E. Character Based Anti-Phishing Techniques

Most of the time attackers try to obtain details from the user by making them to click on the hyperlink attached with the e-mail. This technique uses the characteristics of hyperlink in order to detect phishing links. A tool that implements this technique is called LinkGuard Tool.

The LinkGuard does the following steps for phishing detection: First, the DNS are extracted from the actual and visual links and both the DNS are compared. If both these DNS are not equal, then it is a phishing attack. If the DNS contains dotted decimal IP address, there are chances that it can be a phishing attack.

Advantages: Like Attribute Based Anti-Phishing Technique, it can detect both known and unknown attacks. Also, about 96% of the phishing attacks can be detected using LinkGuard in real time.

Disadvantages: Since dotted decimal IP addresses instead of domain names may be suitable in some special circumstances, the LinkGuard may also result in false positives.

VII. PROPOSED SYSTEM

Nowadays much software has been developed to check/count the number of external and internal links in a particular website. For example, LinkCount Checker can help you track the internal, external links and backlinks of your web pages optimization.

By adapting the concept of a LinkCount Checker, we can propose an algorithm for detecting phishing. Normally, a phishing site contains high number of cross-links.

A. Algorithm

- Check the number of links in the fake website with the actual website.
- If the number of links in the actual website is not equal to the links in the fake website, then it is a link of a phishing website.
- Raise an error message to inform the user that the specified link is not an authorised one.
- Then the user can report the phished link to APWG (Anti Phishing Working Group- To reduce the number of phishing attacks there is a group called APWG, which will have a list of phishing pages. If a user finds that, the page he visits is a phishing page then he can report it to the APWG. They will add that page in the list of phishing page.
- If the number of links in the actual website is equal to the links in the fake website, then it is not a phishing website.
- If yes, go and check the specified link with the set of predefined "whitelists" of URLs. White lists consist of set of authorised links. This process can help the user to double check whether the specified mail is from an authorised authority or not.
- If the URL is found to be in the set of whitelisted URLs, then we can conclude that it is from an authorised website.
- Redirect the user to the specified authorised website.

Based on the above suggested algorithm, we can develop a program to be fit in the firewall or others devices of the authorised website that are devised for protection, to protect against the threat of phishing.

VIII. CONCLUSION

Phishing is one of the major problems that the cyber world is facing today. In this attack, the attacker try to obtain the personal and financial information about the user by making them to provide their information to the fake website, which exactly looks similar to that of legitimate website. The fake website resembles so close to the legitimate website that can even fool educated people. Through this paper, we have proposed a new method for detecting phishing- phishing detection based on link counter. This paper also provides a better understanding about the concept of phishing, its history, and different types of phishing, various anti-phishing technique and so forth.

REFERENCES

[1] ManaliDeshmukh and Shraddha K. Popat (2017, April). Different Techniques for Detection of Phishing Attack. IJESC. Volume 7 (Issue No. 4)

[2] A.Sarannia and U.R.Padma (2014, March). Prevention Model for Phishing Attacks in Web Applications Using Linkguard Algorithm. IJIRCCE. Volume 2 (Special Issue 1)

[3] Suman Bhattacharyya, Chetan Kumar Pal and Praveen Kumar Pandey (2017, March). Detecting Phishing Websites, a Heuristic Approach. IJLERA. Volume 2 (Issue 03). PP – 120-129.

[4] NirmalaSuryavanshi and Anurag Jain. A Review of Various Techniques for Detection and Prevention for Phishing Attack. IJACT.

[5] U.Naresh, U.VidyaSagar and C.V. Madhusudan Reddy "Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm" IOSR Journal of Computer Engineering (IOSR-JCE).

[6] APWG, Phishing activity trends paper [online].

AUTHORS

Mariadas Ronnie C.P received M.Phil Information Technology (IT) in 2012, M.Tech Computer and Information Technology (CIT) in 2011 from M.S University, Tirunelveli, India, MCA Degree from Bharathiar University, Coimbatore, India in 2001. Currently he is working as Asst. Professor at SCMS School of Technology and Management (SSTM), Muttom. His research interest lies in the areas of Image Processing and Cyber Security.

Jincy Rachel Varghese is currently pursing Post Graduation in MCA at SCMS School of Technology and Management (SSTM), Muttom, Alwaye, Cochin. Her keen interest lies in the areas of Database Management System and Cyber Security.