Phishing Types and Techniques of Anti Phishing: A Review

Prof.Kaushalya J. Nakum
Dept of Computer
[1, 2]Vadodara Institute of Engineering,kotambi.

Abstract- *In today's era, phishing become very serious problem. Phishing is a technique to fetch and collect personal information using different way through e-mails and websites. Sensitive information like username, password theft by hackers through online. Phishing frequently occures in email spoofing or instant messaging. Phishing email contains some link or detail into which ask detail to the users to fill their personal information so that become easy for attacker to hack the information. This paper contain an overview about a variety of phishing attacks and techniques to protect the information.*

Keywords- Phishing, Email, Threat, Technique

I. INTRODUCTION

There is variety of different types of attack like active and passive attack, among them phishing attack is most critical attack[2]. Into this attack, an attacker will collect the information through various ways to find the vulnerability of the networks[7]. There is requirement of security to protect the data from various attacks[6]. Phishing is a frequent risk and is widely happens in social media. Into Phishing emails have detail and link which direct toward the infected website Phishing email attract to the user to provide and to enter the personal information, so that the hacker will hack the information whatever the user enters[4]. Phishing email has been send by phisher to huge number of people and the phisher will calculate that how many people who read that email and enteredthe information[2]. It is very hard that when we visit the website is an actual site or malicious site because its look like very similar as actual one[1].Phishing is one of the attack which is recognized as spoofing. That's why researchers are trying to decrease the risk and vulnerabilities[5].

As per the statistics of phishing activity trend report,3rd quarter 2017 which is realese on feb 2018 given by Anti Phishing Working Group (APWG), the unique phishing sites detected was 73,393 highest in august.

Based on the report prepared by the Anti-Phishing working group organization[6], there were about 163,333 phishing attacks reported in 2014. A study by McAfee Lab[3] showed that there were about 30,000,000 new suspected URLs in Quarter 3 for the year 2014.

Rest of the section of the paper is organized is as follows. Section II of this paper gives the different types of phishing attacks. Section III gives the liturature review of various types of the phishing attacks. Section IV describe the different possible anti phishing techniques and section V concludes the paper

II. TYPES OF PHISING ATTACKS

In this section, a brief description related to types of phishing attacks.

A. Deceptive Phishing

Deceptive phishing is one kind of message which create emergency about that are requisite to confirm information about the account, requesting users to re- enter their information, changes in account, new free services need rapid action, and many other malicious sites are mail by attacker to numerous recipient with the expection that the some of them will react by clicking on that link or by login onto a fake site where their sensitive information can be collected and later on misused by attacker.

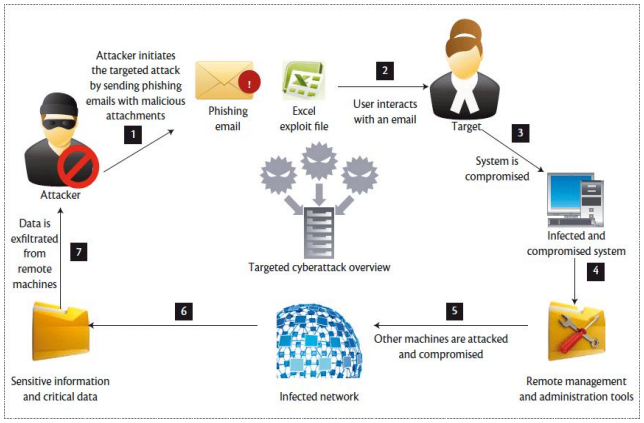

Fig. 1. Scenario of Phishing Attack

B. *Malware-Based Phishing*

This types of phishing based on scams like it occupy malicious software on users' PCs. Malware can be attachment file which is sent by email, as a file which is downloadable from a website which showing some problem solution for a particular issue. This attack will happen on that user who are using out dated software applications.

C. *Key loggers and Screen loggers*

In this type of phishing, information which is enter by user through keyboard will be capture by malware software and that information stored in some hidden file and send it to the attacker by internet from any location to any place. It will stay with user's browsers as a hidden program and execute it itself whenever browser will be started by user.

D. *Session Hijacking*

This works based on observing the actions of the users when users login in to the account and start their transaction and do their important task, at that same time unauthorized action will be performed. This type of action will cause major loss and it will happens without user's aware.

E. *Data Theft*

User store their sensitive information in PC's. Without knowledge to the user, that information will be theft from system. Commonly, this information is user information such as passwords, security numbers, credit card detail, other personal information, private corporate information. After stealing data from users, like confidential communications, design documents, legal opinions, employee related records, etc., hackers will misuse those detail by any ways to gain profits from them or to damage for any economic or by selling that information to competitors.

F. *DNS-Based Phishing ("Pharming")*

In DNS based phishing attack, it will change the hosts file. In this attack fake address will be return by hackers and transaction will happens for communication to the fake website. Users enter their sensitive details in fake website but they are unaware of this and it will be theft by the hackers from remote location.

G. *Content-InjectionPhishing*

In this type of attack hackers will change the actual content with the bogus content in the website which will mislead the user to provide their sensitive information.

H. *Man-in-the-Middle*

In this hacker will be in between the user and the website. Whenever user enters their information hackers will take the information without causing interruption to the users. Later on hackers will use this information when the user is not active on the system.

I. *Search Engine Phishing*

Phishers will create web pages for fake products, get the pages indexed by search engines, and wait for unsuspecting customers to enter their confidential information as part of an order, sign-up, or balance transfer. Such pages usually offer product or services at a price slightly too good to betrue

III. ANALYSIS OF VARIOUS ANTI PHISHING TECHNIQUES

Phishing main objective is to theft sensitive information through web such as passwords and credit card information from various users.

Abdulghanialiahmed,Nurulamirahabdullah[1],propos es a detection technique of phishing websites based on checking Uniform Resources Locators (URLs) of web pages. Generally legitimate webpage and fake web page both are different in url, based on features of url like ip address, url length, position, domain and suffix or prefix, it find that applied webpage is real webpage or fake webpage. user enter url it check all characteristic and make decision and alert to user that it is real or phishing url.

SeoungYeop Na, Hyun Kim and Dong HoonLee[2] uses authentication schemes of server using SSL/TLS to defend Internet banking customers from phishing attacks. Using SAPIM in banking system, user can recognized genuine server and protect themselves from phishing. Through advanced SAPIM, can give more security because SURL will be saved in certificate and the phishing URL is not identical with the SURL saved in the certificate. Conclusion is SAPIM is used to prevent the phishing attacks and advanced SAPIM is used to avoid the active phishing attacks.

According to EnginKirda and Christopher Kruegel[4], phising attacks become most critical day by day and using an AntiPhish technique which protect the inexperienced web user from the phishing attack which occurs when user accessing webpage. They apply technique in AntiPhish application which embedded into browser and when

user enter into phishing webpage it tracks information of the user and prevent from phishing webpage.

Aanchal Jain and Prof. VineetRichariya[5] proposed a prototype web browser which work as an agent and verify the data from phishing attacks. web browser is used by user to read the email and there is any suspicious threat is there, it identifies and notify to the user and asks to remove the email. so this way user notified about suspicious webpage and prevent from phishing.

MadhusudhananChandrasekaranRamkumarChinchaniShambhuUpadhyaya[6] proposes a unique technique known as PHONEY. Through this techniqhe it can detects and analys the phishing attacks.Thekey idea behind this technique is defense the users by providing the sensitive information to the website. To mitigate phishing attack through web,this tool will work as browser extension.

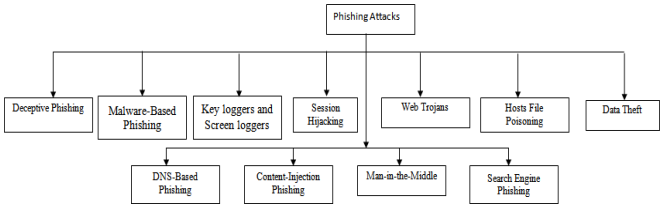

Fig. 2. Types of Phishing Attack

IV. CONCLUSION

Phishing is a serious problem that results in a frequent threat and the risk is high in social media.Phishing takes benefit of the trust that the user fall down to recognize difference between real webpage and fake webpage. Therefore, when this happens, the hacker has the opportunity to gain the personal and sensitive information of the targeted user, such as passwords, usernames, security codes, and credit card numbers, among other things. This paper discuss about the various types of phishing attacks and various anti phishing techniques used to detect and prevent phishing attack.

REFERENCES

[1] Abdulghani Ali Ahmed,NurulAmirahAbdullah,"Real Time Detection of Phishing Websites"IEEE 2016.
[2] SeoungYeop Na, Hyun Kim and Dong Hoon Lee 2014," Prevention Schemes Against Phishing Attacks on Internet Banking Systems" International Journal of Advance Soft Computing Application, Vol. 6, No.1, March 2014 ISSN 2074-8523
[3] Mcafee Labs Threats Report: February 2015. Retrived from http://www.macfee.com/us/resorces/repors/rp-quarterly-threat-q4-2014.pdf
[4] EnginKirda and Christopher Kruegel2005 ," Protecting Users Against Phishing Attacks with AntiPhish". Computer Software and Applications Conference, COMPSAC 2005. 29th Annual International (Volume:1).
[5] Aanchal Jain and Prof. VineetRichariya 2011," Implementing a Web Browser with Phishing Detection Techniques" World of Computer Science and Information Technology Journal, Vol. 1, No. 7,289-291.
[6] MadhusudhananChandrasekaranRamkumarChinchaniShambhuUpadhyaya," PHONEY: Mimicking User Response to Detect Phishing Attacks", WOWMOM '06 Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, Pages668-672, IEEE Computer Society Washington
[7] RachnaDhamija, J. D. Tygar, Marti Hearst," Why Phishing Works" CHI '06 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages581-590, ACM 2006.