International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 5, September- October 2017 ISSN 2278-6856

CYBER CRIME: PHISHING ATTACKS AND VARIOUS ANTI-PHISHING TECHNIQUES

PRATEEK CHOUDHURY

SIKKIM MANIPAL INSTITUTE OF TECHNOLOGY
(B.TECH- 3RD YEAR)

ABSTRACT: ***Phishing is a technique to steal or obtain private data like pass-codes, usernames, data or pin using fake links which pretends to be trustworthy and original. Users often goes through these links and when doing so, the fraud/hacker gathers the required informations and it becomes easy for him (hacker) to access his (victim) personal informations. This paper presents an overview idea and basic details about various phishing attacks and various techniques to protect the private information.***

Keywords: Phishing,Cyber-Crime,Risk,Attackers

1.INTRODUCTION: Phishing is the procedure or method to gather personal informations such as usernames, passwords, and bank card details of the customers often for fraudulent reasons, by disguising as a trustworthy entity(often via links or pings) through electronic mediums. The word is tossed as a homophone of fishing which is similar of using a bait in an attempt to catch a fish (victim). Now a days these malicious method have become the major centre of risk in the internet. In this era almost everyone can access his/her accounts via internet through the methods like internet banking ,net banking or online transactions and due to this constant link between the user and his bank account, internet serves as the main element. Phishing emails are send to thousand of users and the phisher keeps a record for the percentage of users who have read that email and went through the informations . So it becomes extremely difficult to find that we are actually visiting an actual site or a fraud site.

According to the statistics given by Anti Phishing Working Group (APWG) in December 2015, the unique phishing sites detected was 630,494 and the top two countries in phishing hosting site was Belize (81.3%) and USA (76.8%).In this paper we focus on various types of phishing attacks and different anti phishing techniques.

The remaining section of the paper is designed as follows. Section II of this paper gives the different types of phishing attacks. Section III give the analysis of various types of phishing attacks. Section IV gives us the conclusion on this topic and Section V is the reference part of this paper.

2. DIFFERENT TYPES OF PHISHING ATTACKS:

There are different methods of phishing attacks but few basic attacks are as follows:

2.1. SPEAR PHISHING:

Spear Phishing is a highly personalized method of phishing in which the phisher customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick and make believe the recipient or the target into believing that they have a connection with the sender. This technique has become famous specially in social media sites like twitter, facebook where attackers use multiple sources of information to target a person's private information.

2.2. MALWARE BASED PHISHING:

This phishing method refers to the scams which involves several types of malicious software running on users PC's or laptops. The person who does not generally updates their software on regular basis are likely to get affected from this type of phishing in which the phisher sends downloadable files in form of email attachments and waits for the user to download it so the phisher can get and easily access his/her(victims) personal datas.

2.3. DECEPTIVE PHISHING:

In this type of phishing the fraudster impersonate a legitimate company and attempts to steal person's private credentials and login details. In this case a user might get a mail from the copied company to register or change details due to some delicacy and security reasons but actually during this process when the user tries to login and give input in that website all the users data are transferred to the attacker and so the attacker can easily acess the users personal information.

2.4. TROJANS PRESENT IN WEB:

In this process the users essential credentials are being transmitted and they are send to the attackers. This happens when a user tries to login his/her account and this is the major time when his private credentials are being transferred to the attackers through the medium (web).

2.5. SESSION HIJACKING:

Session Hacking describes a pre-planned attack where the victims activities or performances are monitored until they sign in to a target account or make any transactions and establish their required credentials. At that point the fraudulent software takes over and comes into its role and undertake unauthorized actions such as transferring funds, without the user's knowledge.

2.6. SEARCH ENGINE PHISHING:

In this phishing activity the phisher creates an attractively designed website which includes several offers made especially for the victim so that victim can go inside the link and give his/her private details. Once the details are provided there, it becomes very easy for the phisher to log into the users account and make illegal transactions.

2.7. CONTENT INJECTION PHISHING:

In this type of phishing the content replacement takes place i.e. the hacker changes some of the original content of the website and replace it with some fake links and contents so that the user can get mislead and provide their private credentials to the hacker.

2.8. DATA THEFT:

This happens generally in unsecured PC’s where some piece of sensitive information are stored somewhere else in servers. Definitely PC’s are used for accessing the servers and underwent uncompromised. Data theft is a widely used approach for business spying purposes. By stealing confidential datas and logics, design documents, legal opinions, employee related records, etc., thieves or the rival ailments profit from selling to those who may want to cause economic damage or to the competitors.

2.9. MAN-IN-THE-MIDDLE:

In this the phisher is present between the user and the system. The hacker continuously gets the user credentials and information without giving prior knowledge to the user. The user doesn’t get any hints about how his/her information are stole and when the user becomes inactive his/her credentials are used to access the users account illegally.

2.10. PHARMING:

Pharming is the term given mainly to the Domain Name System (DNS)- based phishing. In this phishing technique the phishers or the hackers intrudes with a company's hosts files or domain name system so that requests for URL’s or name service returns to an invalid/fake address and subsequent communications are directed to a fake site. When this transfer of URL’s occurs the user doesn’t comes to know about anything and proceeds further by giving his personal credentials and information.

3. ANALYSIS OF VARIOUS ANTI PHISHING TECHNIQUES:

The basic aim of phishing is to steal a person’s essential and personal credentials like passwords and bank account details via online transactions or forms which users fill during online processes.

[1] Madhusudhanan Chandrasekaran Ramkumar Chinchani Shambhu Upadhyaya proposes a new technique called ‘PHONEY’ which has the capacity to detect phishing attacks automatically.The basic logic behind this technique is user can provide fake informations to the website so that the user can be safe and secure.

[2] Mohd Mahmood Ali introduces Association Rule mining technique for deceptive phishing. The proposed approach is named as APD (Anti-phishing Detector), detects Phishing in Messenger systems. Antiphishing system (APD) detects out any sort of suspicious phishing attacks when messages are exchanged between clients of a messaging system.Re-occuring words are also checked in this system and if any suspicious or abnormal activities occurs in between,then the user is immediately informed about this.

[3] Nilkesh Surana,Neha Sabe proposed a new algorithm ‘Linkguard algorithm’ to remove phishing attacks. The characteristics of hyperlink are used in this algorithm to minimize the attacks. .Linkguard algoritm analyzes the difference between the visual link and actual link.

[4] V. Suganya has gave brief details about phishing and has given a brief idea about all sort of attacks and protective measures regarding phishing attacks.

[5] Brad Wardman, Tommy Stallings introduced a matching file algorithm to review itself and change itself according to the website policies. The file matching and string alignment techniques tested include Main Index matching, Deep MD5 Matching and majorly a novel algorithm named Syntactical Fingerprinting.In this techniques matching of documents occurs between the original and the fake website document.This technique has been proved to be 80-90% accurate in identifying the phishing contents.

[6] Venkata Prasad Reddy, V. Radha, Manik has also proposed two new techniques for detecting phishing techniques.The first one is spoof alert and the other is browser extension.In the first technique the participation of white lists are involved which contains data as per the users comfort and in the second method trusted windows are there which are dedicated for password entry which displays a photographic image.The URL’s which are selected by the user and the URL’s present in the white list are being compared and same happens with the IP(Internet Protocol) also.If in both cases they are same then the website which user is visiting is an original one and if they are different then the website is a duplicate one.

4. CONCLUSION:

Phishing is one of the most dangerous and illegal way of obtaining a users personal informations especially via social media.The main aim of this problem is that it gets the trust of the user and use it for a wrong purpose.A person who visits that site can also not determine whether the site is an original or a fake one.When this phishing attack occurs the hacker or the phisher has the full chance to obtain bank related passwords,account details and personal informations so that the hacker can access the monetory related details of the customer without the prior knowledge of the customer.This paper deals and discusses about phishing,its various types and few techniques to prevent this attack.

REFERENCES:

[1] Madhusudhanan Chandrasekaran Ramkumar Chinchani Shambhu Upadhyaya," 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

[2] Eric Medvet, Engin Kirda, Christopher Kruegel 2008," Visual-Similarity-Based Phishing Detection" Proceedings of the 4th international conference on Security and privacy in communication networks

[3] Venkata Prasad Reddy, V. Radha, Manik Jindal 2011," Client Side protection from Phishing attack" International Journal Of Advanced Engineering Sciences And Technologies Vol No. 3, Issue No. 1, 039 – 045.

[4]V.Suganya,"A review on phishing attacks and various phishing techniques",International Journal of Computer Applications (0975 – 8887) Volume 139 – No.1, April 2016

[5] Aanchal Jain and Prof. Vineet Richariya 2011," Implementing a Web Browser with Phishing Detection Techniques" World of Computer Science and Information Technology Journal, Vol. 1, No. 7, 289-291.

[6] Mohd Mahmood Ali and Lakshmi Rajamani 2012," APD: ARM Deceptive Phishing Detector System Phishing Detection in Instant Messengers Using Data Mining Approach" Springer Berlin Heidelberg

[7] Nilkesh Surana, Prabhjot Singh, Umesh Warade, Neha Sabe 2015," Detection and Prevention of Phishing Attacks in Web" International Journal of Scientific Engineering and Technology Research, ISSN 2319-8885 Vol.04,Issue.08, April-2015, Pages:1595-1598