Volume 5, No. 6, June 2014
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

ANALYSIS OF ISSUES IN PHISHING ATTACKS AND DEVELOPMENT OF PREVENTION MECHANISM

Dr Vijay Singh Rathore, Neelam Gupta
Professor & Director, Shree Karni Collge, deep.neel@gmail.com
Research Scholar, Mewar University, Chittorgarh(Raj.) deep.neel@gmail.com

Abstract- As size and complexity of today's most modern computer chips increases, new techniques has been developed. With increasing of new development off course but it also brings some disadvantage and loss for people. Information security s greatly increased in visibility over the past two decades. Over the last 15 years governance around the policies and procedures that make up information security has grown and new more specific areas such as data governance has begun to emerge.Nowdays popular word scam or we say phishing is spreading in whole world. This word begins with a letter or email which is sent to a selected recipient making an offer allegedly result in a large payoff for the victim. In order to solve this problem we emphasize to give the information of on all these phishing attack and what solution can be used to stop these attack and how can we save from these scams.
This paper presents on antiphishing that aims to protect user again spoofed web site based phishing attack. The issues which has been developed to be analysis. To this end what we can change in the existing mechanism which are using for prevention.

INTRODUCTION

The word phishing means the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individual to reveal personal information such as credit card, password online. Phishing scams are typically fraudulent email message appearing to come from legitimate enterprises. Phishing is a new word produced from 'fishing' it refers to the act that the attacker allure users to visit a faked website by sending them faked emails and stealthily gt victim's personal information. This information then can be used for future target advantage or even identity theft attacks.

The act of stealing personal information via the Internet for the purpose of committing financial fraud has become a significant criminal activity on the Internet. However there has also been as increase in attack diversity and technical sophistication by the people conducting phishing and online financial fraud.

Email and the Internet is a wonderful resource that has revolutionized the way humans communicate and access information. Unfortunately, it has also proven to be a fertile medium for the unscrupulous and the morally challenged. Scammers regularly use email in attempts to steal money or personal information from unsuspecting victims. Those inexperienced in the ways of the Internet are especially vulnerable to these scammers. It has a negative impact on the economy through financial losses experienced by business and consumes along with diverse effect of decreasing consumer confidence in online commerce. Phishing scams have flourished in recent years due to favorable economic and technological condition. The technical resources needed to execute phishing attacks can be readily acquired through public and private sources. Some technical resources been streamlines and automated allowing use by nontechnical criminals. This makes phishing both economically and technically viable for a large population of less sophisticated criminals.

OBJECTIVE

The objective of our research is to study and analyze various issues in phishing attack. To provide benefit to the user so that a systematic and more reliable approach can be used to maintain the prevent users from email scams. This research aims towards a comprehensive literature review for the analysis of various prevention mechanisms. We will review the trends in these capabilities over the past two years and discuss currently deployed countermeasures. This project focus to identify and consolidate the prevention mechanism and to formulate a methodology to evaluate these models.

WORKING

The majority of phishing attacks appear to originate in china. Last year, a significant rise in phishing attacks on shared virtual scams. In these attacks, a phisher breaks into a web server that hosts large number of domains then places then places the phishing content on every domain which infected thousands of web Sites simultaneously. While the financial industry continues to be primary target for phishers, it's certainly not the only sector vulnerable to attack. Auction sites, payment services, retail and social networking sites are also frequent targets, as are cell phones providers and manufacturers. No business or brand is inherently safe. It if poses on company's official website it diminish its online brand and deter customers from using actual website out of fear of becoming fraud victims.

Criminals began to target specific companies and their customers in order to improve their returns. These attacks used advanced technical capabilities such as exploitation of weak website coding or security flaws within desktop operating system. The phishes combined multiple technical elements along with social engineering to target an attack on specific brands. Any organization that does web based e-commerce is a potential target. This time, as expected,

targets included social networks, search engines and email services, telecom companies, e-payment services, banks, and other credit and financial institutions. However, there were a few surprises as well, such as tax and customs agencies, the governments of various countries, car companies, insurance companies, medical institutions, oil companies, and transportation companies (including some airlines).

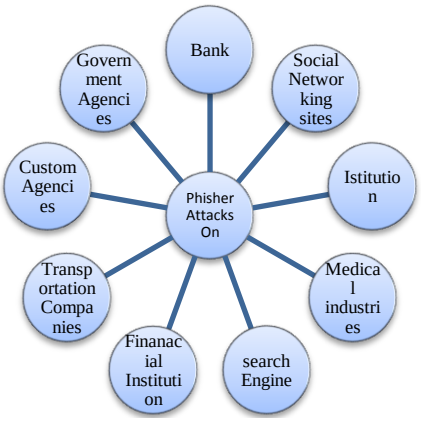

Figure:1 Targeted Users

Phishing attack are growing in number and in technical sphistication.The most common form of phishing is by email. Prentending to be from your financial iinstitution or a legitimate retailer or governemtn agency, the sender asks you to confim your personal information for some made of reason. The act of sending an email to a user flasely claiming to be an established legitimate enterprise in an attempt. The flat flaw that enabled the sensitive information to be stolen is possible when an end user is not properly educted on an easy to do and wel known SSL exploit—SSL MIMM. The hackers take benefit of that to get access your sensitive data.The victim a/c like hotmail, gmail, yahoo, social networking site, like myspace, orkut, facebook, banking account etc. Web hosts are free webspace where any one can upload created phishers. Phishers is fake login page that we create and send this phisher link to the victim. When the user use his account his username sheme and password will save in phisher link. So we need some space on Internet for phishers.

In phishing scam phishers first decide which business to target and determining how to get email address for the customer of that business .Once they know which business to spoof and who their victims are phishers create methods for delivering the message and collecting the data.Then he attack the phishers and sends a phony message that appears to be from a reputable source.He then record the information victim enters into web pages.

Just a few years ago, phishing attacks were primarily seen by researchers as just one of several threats found in email spam. For some time, phishing remained relatively primitive from a technical point of view. It was relatively rare and it typically posed a threat only to the most naïve and inexperienced users. But today, the scale of these attacks and the technologies used are such that phishing has been elevated to a category of its own, meriting a separate study.

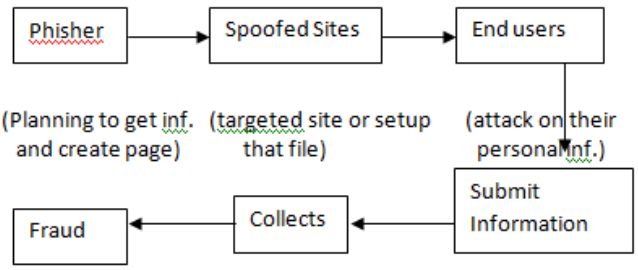

Figure: 2

DIFFERENT TYPES OF SCAMS

Scam is a fraudulent or dishonest business scheme designed to make a quick profit. There are different types of scams like home working schemes, special offers, scam emails, domain name renewal scams, and others. Junk or spam email is a scheme designed with the purpose of personal gain. They offer cheap products and services and free goods. Fraudsters send emails with offers for product trials, free holidays, downloads, and products. And ask users to supply their personal and credit card details in order to get access to their accounts. Scam includes computer virus scams, competition and lottery scams, and shopping and auction scams. Get-rich-quick scams offer a system for investing and making a lot of money. Fraudsters may approach face-to-face, over the telephone, by mail, or email. There are other types of scam such as money laundering and chain letter scams. Money laundering refers to concealing money that has been earned from illegal or unlawful activities. It can be money from scams, drug trafficking, and organized crime..

In Soft scams fraudster misrepresents a service or product to make it more attractive. Some types of mail order scams fall in this category. Hard to detect and often go unnoticed until it's too late Hard scam involves nonexistent products, services, and businesses. In addition to these scams, other are affinity scams that prey upon members of identifiable groups such as ethnic groups, religious groups or professional groups, sports investment scams, and others.facebook prize scams, hitman scams, and service scams. Lottery emails are one variety whereby fraudsters send emails to consumers and inform them that they have won the jackpot. Then they will ask you to cover the fees, and you will end up losing money. There are some warning signs that you are being scammed. If you hit the jackpot, you won't be notified by email. You. Bad investment scams involve actual products and companies with extremely high risk. Identity theft is also growing in which one can steal someone else's ID, stolen ID can be used purchase things online, commit crime in someone else's name, commit tax fraud, and so on. These are Internet scams with the growth of internet there is a rapid growth of these scams. Broadcast is a popular method for sending email messages to many person. By sending messages about fictitious account charges verify account information, new free services are broadcast to many recipients for the collection of confidential information.

Malware-Based Phishing refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file

from a web site, or by exploiting known security vulnerabilities--a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date. Malware-based phishing involves running Malicious software are also running on the user's machine. So the malwar introduced as an email attachment or as a downloadable file exploiting security vulnerabilities. This is a particular threat for small and medium businesses (SMBs) who fails to update their software applications.

Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. DNS-Based Phishing "Pharming" is the term given to hosts file modification or Domain Name System (DNS)-based phishing. With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. The result: users are unaware that the website where they are entering confidential information is controlled by hackers and is probably not even in the same country as the legitimate website. Pharming is a type of attack intended to redirect traffic to a fake Internet host. There are different methods for pharming attacks, among which DNS cache poisoning is the most common Phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even multiplayer games. Below are some major categories of phishing.

In clone phishing phisher does get information such as content and recipient addresses from a legitimate email which was delivered previously, then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy

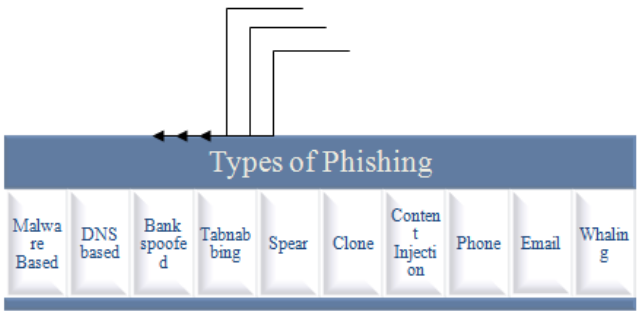

Figure: 3

Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly,spear phishers target selected groups of people with something in common, for example people from the same organization In phone phishing, the phisher makes phone calls to the user and asks the user to dial a number. The purpose is to get personal information of the bank account through the phone. Phone phishing is mostly done with a fake caller ID.Phone Phishing This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source Banking scams are designed to extract sensitive banking information from recipients.

This information can then be used to craft more convincing scam messages again targets, gain access to a victim's bank account, commit identity theft, etc. Bank customers are popular targets of those who engage in phishing attacks. If you have a bank account, you more than likely access it online from time to time. As a result, you probably have a username and a password that are associated with your online account. Most people understand the importance of keeping that kind of information confidential; if it falls into the wrong hands, a great deal of sensitive financial information would be compromised. Unfortunately, many people fall victim to bank phishing scams each year and inadvertently give out sensitive information to people who have criminal activities on their minds.

The most common way that a phisher gets the ball rolling on a bank phishing attack is by sending out thousands of spoof emails. The goals of fake job offers and work from home scams range from attempting to extract sensitive information to recruiting users to commit illegal acts unknowingly under the disguise of a job. If a job offer sounds too good to be true, it likely is. Verify the legitimacy of a company through sources such as the Better Business Bureau, physical addresses, Internet searches and more. Tabnabbing is a computer exploit and phishing attack , which persuades users to submit their login details and passwords to popular websites by impersonating those sites and convincing the user that the site is genuine.

RELATED CASES

One "woman" scamming had money sent to a generic name like Joseph Hancock alleging she could not collect the money due to losing her international passport. After sending the money the victim is given bad news the woman was robbed on the way to the bus stop and the victim feels compelled to send more money. The fraudster never visits the victim and is willing to chat with the victim through a chat client as long as the victim is still willing to send more money

Recently, a few ICICI Bank customers in Mumbai, to their utter dismay, discovered that e-mails can be extremely hazardous A few customers of ICICI Bank received an e-mail asking for their Internet login name and password to their account. The e-mail seemed so genuine that some users even clicked on the URL given in the mail to a Web page that very closely resembled the official site. The scam was finally discovered when an assistant manager of ICICI Bank's information security cell received e-mails forwarded by the bank's customers seeking to crosscheck the validity of the e-mails with the bank. Such a scam is known as 'phishing.' The Nigerian scam is another very popular e-mail related scam that has found a few victims in India. The scam

itself is simple. An e-mail, which claims to be written by a prominent official from an African country asks the recipient to help them release millions in the bank and offers them a share of the bounty.
Once the recipient responds he is asked to visit the (African) country and meet with officials to collect the money. But once there, instead of getting money, he is forced to cough up a considerable sum.This scam is known as the 'Advance Fee Fraud' or '419 Fraud,' after the section of the Nigerian Penal Code that specifically prohibits this con.

Fraudulent cheques and money orders are key elements in many advance-fee scams, such as auction/classified listing overpayment, lottery scams, inheritance scams, etc., and can be used in almost any scam when a "payment" to the victim is required to gain, regain or further solidify the victim's trust and confidence in the validity of the scheme.

CONCLUSION

This research is primarily set out to identify and consolidate the prevention mechanism associated with phishing scams and to formulate a framework to evaluate, categorize and handle these issues. The insights that will be gained from the research are expected to form a set of guidelines for designing this system in the form of a structured framework for evaluation for prevention mechanism. No single model or mechanism can adequately protect a system. The research investigations need to be undertaken to examine various technical issues.

In this research, we will try to eliminate the drawbacks of all the available prevention mechanism aspects and include new and improvised method for obtaining a generalized framework.

As a conclusion, it is our hope that this research will provide some insight on how and why these detection and prevention mechanism are important and how currently available mechanism can be improved to plan better prevention mechanism. We will explore in terms of reliability, performance and feasibility to obtain a generalized framework.

REFERNCES

[1]. Engin Kinda and cristopher kruegel , technical university of vienna, Austre

[2]. Fraud slat New phishing tactis- and how they impact on your business.

[3]. Contributing Research Analyst Ron Collette, CISSP and Mike Gentile CISSP Feb 2006.

[4]. Phishing to hack email A/C password by Aelksandar.

[5]. How phishing works by Tracy V. Wilson.

[6]. What is spear phishing? MS security at home

[7]. Fake subpoenas harpoon 2, 100 corporate falcats

[8]. By Jake Stroup,Identity Theft Issues in 2011,2011,http://www.about.com / / Identity Theft Issues for2011.htm.

[9]. Jason Milletary US-CERT,Technical Trends in Phishing Attacks.

