ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Phishing: Threats & Challenges

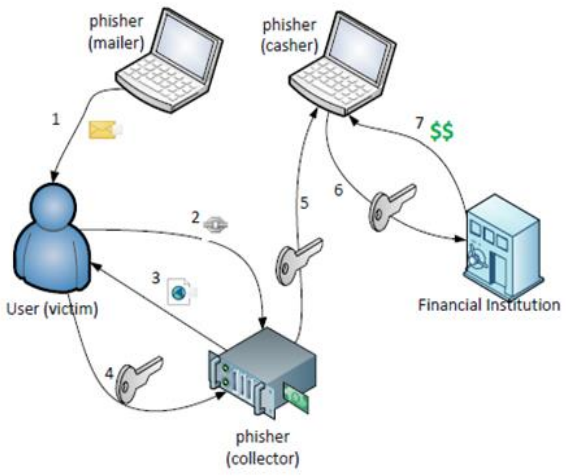
[1] Shashank singh, [2] Sovan kar, [3] Siddhant khemka, [4] Mahaveer sahu, [5] Reji Thomas
[1,2,3,4] UG Scholars, Dept. of Computer science & Engineering, SSCE, Bengaluru.
[5] Asst. Prof., Dept of Computer Science & Engineering , SSCE, Bengaluru.

Abstract:- **Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Cyber-crime is emerging as a serious concern. To the world of computer technology which is evolving ever so fast the government, police and intelligence units are taking this issue very seriously. The world of cybersecurity is not a small term it deals with the threats such as Phishing, Eavesdropping, spoofing, tampering, Clickjacking, Hacking. In this paper, we are going to deal with the challenges regarding phishing. Phishing is derived from two words "Password harvesting" which means fishing for passwords. It is an attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trust, phishing can be classified as a form of social engineering. Phishing is a general term which deals with several subtypes which are discussed further in the paper. Phishing is further classified into Spear phishing, Whale phishing, and Clone phishing. The threats of phishing have confronted us with several challenges concerning with security of data, vulnerability inside an organization, holes insecurities in a computer system.**

***Keywords*: Spear phishing, Whale phishing, Clone phishing**

I. INTRODUCTION

Now a day's attacks had become major issues in networks. Attacks will intrude into the network infrastructure and collect the information needed to cause vulnerability to the networks. Security is needed to prevent the data from various attacks. Attacks may either be active attack or passive attack. One type of passive attack is phishing.



Phishing is an attempt of obtaining sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. The word phishing comes from the word "neologism" created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim.

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to another web address where users are made to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that are infected with malware. Phishing is also known as brand spoofing or carding. 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.

Following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

formatter will need to create these components, incorporating the applicable criteria that follow

II. TYPES OF PHISHING

In this section, we give a brief description about the different types of phishing attacks:

A. Deceptive phishing:

It is the messages that are required to confirm information about the account, requesting users to reenter their information, fictitious account charges, unwanted account changes, new free services requiring quick action, and many other malicious sites are send to many recipients with the hope that the unsuspecting will react by clicking a link.

B. Malware-Based Phishing:

This refers to scams that involve running malicious software on users' PCs. Malware can be as an email attachment, as a downloadable file from a web site for a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

C. Key loggers and Screen loggers:

This type of malware tracks the input from the keyboard and the relevant information will be send to the hackers through internet. They go into the users' browsers as a small program and run automatically when the browser is started as well as into system files as device drivers or screen monitors. Session Hijacking: This deals with monitoring the activities of the users until they sign in to the account or transaction and create their important information. At that point the infected software will perform unauthorized actions, such as transferring funds, without the user's knowledge.

D. Spear phishing:

Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the internet today, accounting for 91% of attacks.

E. Clone phishing:

Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient addresses taken and used to create an almost identical orcloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

G. Whale phishing:

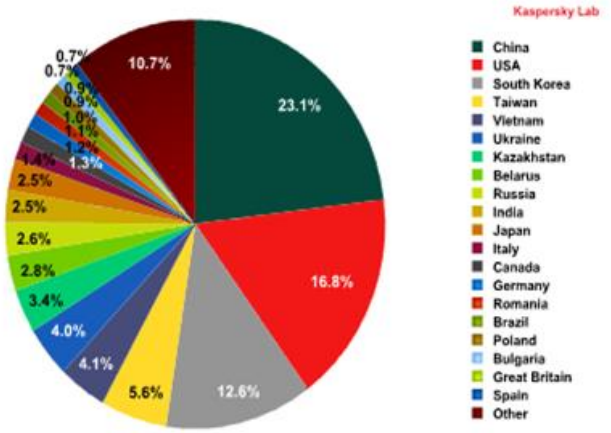
Several phishing attacks have been directed specifically at senior executives and other high-profile targets within businesses, and the term whaling has been coined for these kinds of attacks. In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue. Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority. The content is meant to be tailored for upper management, and usually involves some kind of falsified company-wide concern. Whaling phishers have also forged official-looking FBI subpoena emails, and claimed that the manager needs to click a link and install special software to view the subpoena.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

III. PHISHING ATTACKS

2001: The first known direct attempt against a payment system affected E-gold in June 2001, which was followed up by a "post-9/11 id check" shortly after the September 11 attacks on the World Trade Center.
2003: The first known phishing attack against a retail bank was reported by The Banker in September 2003.
2004: It is estimated that between May 2004 and May 2005, Approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately US$929 million. United States businesses lose an estimated US$2 billion per year as their clients become victims.



Phishing is recognized as a fully organized part of the black market. Specializations emerged on a global scale that provided phishing software for payment (thereby outsourcing risk), which were assembled and implemented into phishing campaigns by organized gangs. 2006: Almost half of phishing thefts in 2006 were committed by groups operating through the Russian Business Network based in St. Petersburg. Banks dispute with customers over phishing losses. The stance adopted by the UK banking body APACS is that "customers must also take sensible precautions ... so that they are not vulnerable to the criminal. Similarly, when the first spate of phishing attacks hit the Irish Republic's banking sector in September 2006, the Bank of Ireland initially refused to cover losses suffered by its customers, although losses to the tune of €113,000 were made good. Phishers are targeting the customers of banks and online payment services. Emails, supposedly from the Internal Revenue Service, have been used to glean sensitive data from U.S. taxpayers. While the first such examples were sent indiscriminately in the expectation that some would be received by customers of a given bank or service, recent research has shown that phishers may in principle be able to determine which banks potential victims use, and target bogus emails accordingly. Social networking sites are a prime target of phishing, since the personal details in such sites can be used in identity theft. In January 2009, a phishing attack resulted in unauthorized wire transfers of US$1.9 million through Experi-Metal's online banking accounts.

IV. METHODS OF PREVENTION

There are anti-phishing websites which publish exact messages that have been recently circulating the internet, such as FraudWatch International and Miller smiles. Such sites often provide specific details about the particular messages. To avoid directly dealing with the source code of web pages, hackers are increasingly using a phishing tool called Super Phisher that makes the work easy when compared to manual methods of creating phishing websites.
As recently as 2007, the adoption of anti-phishing strategies by businesses needing to protect personal and financial 2005: In the United Kingdom losses from web banking fraud—mostly from phishing—almost doubled to GB£23.2m in 2005, from GB£12.2m in 2004, while 1 in 20 computer users claimed to have lost out to phishing in 2005.
information was low. Now there are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing. These techniques include steps that can be taken by individuals, as well as by organizations. Phone, web site, and email phishing can now be reported to authorities, as described below.

A. Browsers alerting users to fraudulent websites:
Another popular approach to fighting phishing is to maintain a list of known phishing sites and to check websites against

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

the list. Microsoft's IE7 browser, Mozilla Firefox 2.0, Safari 3.2, and Opera all contain this type of anti-phishing measure. Firefox 2 used Google anti-phishing software. Opera 9.1 uses live blacklists from Phish tank, cyscon and GeoTrust, as well as live whitelists from GeoTrust. Some implementations of this approach send the visited URLs to a central service to be checked, which has raised concerns about privacy. According to a report by Mozilla in late 2006, Firefox 2 was found to be more effective than Internet Explorer 7 at detecting fraudulent sites in a study by an independent software testing company.

An approach introduced in mid-2006 involves switching to a special DNS service that filters out known phishing domains: this will work with any browser, and is similar in principle to using a host's file to block web adverts.

To mitigate the problem of phishing sites impersonating a victim site by embedding its images (such as logos), several site owners have altered the images to send a message to the visitor that a site may be fraudulent. The image may be moved to a new filename and the original permanently replaced, or a server can detect that the image was not requested as part of normal browsing, and instead send a warning image.

B. Augmenting password logins:

The Bank of America's website is one of several that ask users to select a personal image (marketed as Site Key), and display this user-selected image with any forms that request a password. Users of the bank's online services are instructed to enter a password only when they see the image they selected. However, several studies suggest that few users refrain from entering their passwords when images are absent. In addition, this feature (like other forms of two-factor authentication) is susceptible to other attacks, such as those suffered by Scandinavian bank Nordea in late 2005, and Citibank in 2006.

A similar system, in which an automatically generated "Identity Cue" consisting of a colored word within a colored box is displayed to each website user, is in use at other financial institutions.

Security skins are a related technique that involves overlaying a user-selected image onto the login form as a visual cue that the form is legitimate. Unlike the website-based image schemes, however, the image itself is shared only between the user and the browser, and not between the user and the website. The scheme also relies on a mutual authentication protocol, which makes it less vulnerable to attacks that affect user-only authentication schemes.

Still another technique relies on a dynamic grid of images that is different for each login attempt. The user must identify the pictures that fit their pre-chosen categories (such as dogs, cars and flowers). Only after they have correctly identified the pictures that fit their categories are they allowed to enter their alphanumeric password to complete the login. Unlike the static images used on the Bank of America website, a dynamic image-based authentication method creates a one-time passcode for the login, requires active participation from the user, and is very difficult for a phishing website to correctly replicate because it would need to display a different grid of randomly generated images that includes the user's secret categories.

C. Eliminating phishing mail:

Specialized spam filters can reduce the number of phishing emails that reach their addressees' inboxes, or provide post-delivery remediation, analyzing and removing spear phishing attacks upon delivery through email provider-level integration. These approaches rely on machine learning and natural language processing approaches to classify phishing emails. Email address authentication is another new approach.

V. CONCLUSION

Phishing is a critical problem that results in a continual threat and the risk is high in social media. Phishing takes advantage of the trust that the user may not be able to tell that the site being visited, or program being used, is not real; therefore, when this occurs, the hacker has the chance to gain the personal 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 prevent phishing attack.

This paper based study revealed that users are vulnerable to phishing-based social engineering attacks indicating that there is still a significant lack of awareness in line with previous findings. An understanding of how to identify a phishing attack cannot be underestimated as current anti-phishing mechanisms may not guarantee the user complete protection. As a result increased user awareness is paramount as a countermeasure against phishing.

REFERENCES

[1] Engin Kirda and Christopher Kruegel 2005 ," Protecting Users Against Phishing Attacks with AntiPhish". Computer Software and Applications Conference, COMPSAC 2005. 29th Annual International (Volume: 1).

[2] Craig M. McRae Rayford B. Vaughn 2007 ," Phighting the Phisher:Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks ",Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07).

[3] Alireza Saberi, Mojtaba Vahidi, Behrouz Minaei Bidgoli 2007, "Learn To Detect Phishing Scams Using Learning and Ensemble Methods", Proceedings of the 2007 IEEE/WIC/ACM.

[4] M. Young, The Technical Writer's Handbook. Mill Valley,.

[5] Anti-Phishing Working Group (2009) "Phishing Activity Trends Report: 3rd Quarter 2009" Availablehttp://www.antiphishing.org/reports/apwg_report _Q3_2009.pdf (Accessed: 15 January 2010).

[6] Dhamija, R., Tygar, J.D. and Hearst, M. (2006) "Why Phishing Works", Proceedings of the SIGCHI conference on Human Factors in computing systems, Montréal, Québec, Canada. pp. 581-590.

[7]Gartner (2010) "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks".

[8]http://www.gartner.com/it/page.jsp?id=565125 (Accessed: 21 January 2010).

[9] Herzberg, A. and Jbara, A. (2008) "Security and Identification Indicators for Browsers against Spoofing and Phishng Attacks" ACM Transaction on Internet Technology

[10] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menezer, F. (2007) "Social Phishing"