INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DETECTION AND COUNTERMEASURES OF PHISHING ATTACKS

MISS. ANKITA S. KOLESHWAR[1], MRS. S. S. SHEREKAR[2], V. M. THAKARE[2]

1. Research Scholar, SGB Amravati University, Amravati.
2. Dept. of Computer Science and Engg, SGB Amravati University, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: The frequency of phishing attacks are dramatically increasing every day. Phishing is becoming more popular and unstoppable. It is very essential for companies to come up with new ways to solve phishing problems because it can become a major loss to well known companies. Not any type of technology can stop phishing attacks, but there are many ways to enable phishers from accomplishing their goals. Education it is very important for Internet users and e-mail users because they must have to aware about the activities involved in an attack. Consumer education can increase the awareness of the phishing threat and other online vulnerabilities. Phishing has resulted in lot websites frauds, now the condition is that people are going to do important transactions by using websites. For achieving the lost trust from naive users, capability must have improve to effectively fight out phishing attack. This paper focuses on types of phishing attacks, its issues, and countermeasures.

Keywords: Keyloggers, Session hijackers, Issues in Phishing attack, Detection Criteria.

Corresponding Author: MS. ANKITA S. KOLESHWAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Ankita Koleshwar, IJPRET, 2014; Volume 2 (9): 299-306

PAPER-QR CODE

INTRODUCTION

Phishing is a form of identity that uses the social engineering techniques and Sophisticated attack vectors to collect financial information from innocent consumers[1]. It is a kind of attack in which phishers use spoofed emails and fake web sites to trick people into giving up personal information. [2] The phishing problem has evolved drastically over the past few years. This problem touches multiple points across the organization from end users and web sites to mail servers and networks[3].

This study focuses on various types of Phishing Attacks, Phishing Website detection criteria, Email categorization, and Anti-Phishing Measures.

I. TYPES OF PHISHING ATTACKS

The phishing attacks are widely spread to take advantage of the internet users. There are various types of phishing attacks as discussed below[4]. In addition, today's attacks come from multiple vectors are as given as follows :

- **Deceptive attacks:** It is spear phishing, in which users are tricked by fraudulent messages into giving out information.
- **Domain-based attacks :** This is the attack in which lookup of host names is altered to send users to a fraudulent server.
- **Malicious code-based attacks :** This are also known as Trojan-based attacks, in which malicious software causes data compromises.

There are some types of phishing attacks which are discussed below.

A. Keyloggers :

Keyloggers are spyware programs that install themselves either into a web browser or as a device driver. They are designed to record user input events and send them to a phishing server i.e., spyware owner. If a keyloggers gets into a corporate network, the data leaks could be catastrophic.

B. Rock Phishing Kit

In Rock phishing method, the phishing email points to a proxy that gets its content from a central spoofed website.

C. Torpig-Family Trojan

In this attack, the Trojan monitors major banks websites worldwide and after the users log in, displays a spoofed page while maintaining the original TLS session, thus being very difficult to detect. The Trojan spreads through operating system vulnerabilities.

D. Session Hijackers

In Session Hijacker attack users activities are monitored, typically by a malicious browser component. When the user logs into its account, or initiates a transaction, the malicious software "hijacks" the session to perform malicious actions once the user has legitimately established its credentials.

E. Content-Injection Phishing

In this attack, the malicious content can redirect to other sites, install malware on a user computer, or insert a frame of content that will redirect data to a phishing server.

F. "Universal" Man-in-the-Middle Phishing Kit

This kit consists of a PHP file which is installed on a compromised server.

G. Search Engine Phishing

In this phishing, phisher take an another approach i.e., to create web pages for fake products, get the pages indexed by search engines, and wait for users to enter their confidential information as a part of an order, sign-up or balance transfer.

H. Spear Phishing

In the spear phishing attack, it focuses on a single user or a department within an organization. Spear phishing scams will often appear to be from a well-known entity and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks.

II. ISSUES IN PHISHING ATTACK

There are five significant issues that need to be addressed from a personal or business point of view if phishing is to be combated[5].

A. Education : For Education it is important that Internet users and e-mail users should be aware of the activities involved in an attack.

B. Preparation : With regard to preparation, business should realize the danger of a phishing attack and create policies to manage any attacks or to respond to an attack.

C. Avoidance : A great deal can be done to avoid identity theft, such as anti-spam strategies, using industry standards, for example Verisign verification on sites etc. A good guideline is the use of "https//" web sites where the 's' identifies it as a secure site.

D. Intervention : In intervention, actions should be taken when a phishing attack is suspected.

E. Treatment : Treatment of a phishing attack includes the measurement of the damage after such an attack and contacting the appropriate role players to prevent misuse of your information. After identified this issues as an important factor in phishing attack, company or user should be aware of with regard to phishing.

III. PHISHING WEB SITE DETECTION CRITERIA

Web site phishing attacks usually start with an e-mail that arrives in the victim's mailbox pretending to be legitimate and known entity. [6] Usually, the mail claims some urgent steps to be taken by the user to avoid blocking of user account and direct him to a web page asking him to enter private information.

Detection rate for phished websites is performed based on six criteria which includes – URL and Domain Identity, Security and Encryption, Source Code & Java Script, Page Style & Contents, Web Address Bar and Social Human Factor.

There are number of components for each criteria given as follows :

A. URL & Domain Identity :

- Using the IP Address
- Abnormal Request URL
- Abnormal URL of Anchor
- Abnormal DNS record

B. Security & Encryption :

- Using SSL Certificate
- Certificate Authority
- Abnormal Cookie

C. Source Code & Java Script :

- Redirect Pages
- Straddling Attack

- Pharming Attack
- Using onMouseOver to hide the link

D. Page Style & Contents :

- Spelling Errors
- Copying Website
- Using forms with "Submit" button
- Using Pop-Ups Windows
- Disabling Right Click

E. Web Address Bar :

- Long URL Address
- Replacing similar characters for URL
- Adding a prefix or suffix
- Using the @ symbol to confuse
- Using hexadecimal character codes

F. Social Human Factor :

- Much emphasis on security & response
- Public generic salutation
- Buying time to access Accounts

This is the web site detection criteria discussed above which is based on the various components as given above.

IV. EMAIL CATEGORIZATION

Email is the main vector for delivering phishing messages to users. In a phishing attack scenario, attacker deceives users by a fake email which is called scam. [7] And for this scam detection, emails can be classified into three categories –

a) Spams

b) Scams

c) Hams

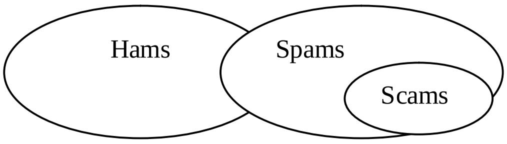

Fig.: email categorization

For considering the necessity of scam and spam detection, the data mining algorithms is to be used. [8] They are Naïve Bayes, Poisson and K Nearest Neighbor.

V. ANTI-PHISHING APPLICATION

There are two detection mechanisms which represents the types of Anti-Phishing Applications [9]. They are as follows :

I. **Blacklist-based anti-phishing application :** In this type of application, user gets warning when the URL of the visited page is in the list of already detected or reported phishing pages.

II. **Whitelist-based anti-phishing application :** This type of application confirms the authenticity of trustworthy pages that have been saved in the whitelist.

Here now assuming that the blacklist-based anti-phishing is going to become helpful for users identify more phishing pages than the whitelist-based.

VI. ANTI-PHISHING MEASURES

Anti-phishing provides several different techniques to fight against phishing. [10] The anti-phishing measures are discussed as follows:

A. Blocked Site lists : Blocked site lists are popular response to the phishing problem. In such type of schemes, a single central database maintains a lists of fraudulent sites, browsers check this database before proceeding to a site. Earthlink and Netcraft both provide these services, implemented on the client by a browser toolbar.

B. Site Information Indicator : Site Information Indicator provide information about the site in the browser toolbar or status bar. The URL field is an indicator already present in all browsers; in theory, a user could check the domain name in the URL to avoid phishing attacks, but in practice, the URL bar provides little protection.

C. SpoofStick : It is the extension of browser that displays the current site's domain name in large letters in the toolbar to make the identification task a little bit easier, but it still relies on the user's ability to distinguish legitimate and illegitimate domain names[11]-[13]. These are the three anti-phishing measures which are necessary to understand.

VII. CONCLUSION

Phishing is a form of online identity theft employing both social engineering and technical deception to steal user credentials such as usernames and passwords.

The damage caused by phishing ranges from an internet user not able to access their email to losing all the money in their bank account. So according to all of these factors such as Financial sector, users account no information and all major concerns needs heavy security.

The purpose of this paper is to discuss the technological issues such as types of phishing attacks, various issues like education, prevention, avoidance along with that e-mail categorization is very important based on that authenticity of the mail can be decided. Anti-phishing measures suggest protection against phishing and related aspects to avoid the phishing and provide safe environment for the internet users.

ACKNOWLEDGEMENTS

I am very much thankful to the various authors for their valuable contribution this field along with my guide and research lab head.

REFERENCES

1. Sujata Garera, Niels Provos, Monica Chew, Aviel D. Rubin, "A Framework for Detection & Measurement of Phishing Attacks", ACM 978-1-59593-886-2/07/0011, pp. 1-8, November, 2007.

2. Hong Bo, Wang Wei, Wang Liming, Geng Guanggang, Xiao Yali, Li Xiaodong, Mao Wei, "A Hybrid System to Find&Fight Phishing Attacks Actively", IEEE/ WIC/ ACM, International Conferences on Web Intelligence & Intelligent Technology, 978-0-7695-4513-4/11 pp. 506-509, 2011.

3. Ian Fette, Norman Sadeh, Anthony Tomaric, "Learning to Detect Phishing Emails", ACM 9781595936547/07/0005, pp. 649-656, May, 2007.

4. Mohamad Badra, Samer El-Sawde, Ibrahim Hajjeh, "Phishing Attacks and Solutions", ICST 978-963-06-2670-5, August, 2007.

5. Alta van der Merwe, Marianne Loock, Marek Dabrowski, "Characteristics and Responsibilities involved in a Phishing Attack", ACM, pp. 249-254.

6. Pravin Soni, Shamal Firake, B. B. Meshram, "A Phishing Analysis of Web Based Systems", ACM 978-1-4503-0464-1/11/02, pp. 527-530, Feb, 2011.

7. R. Suriya, K. Saravanan, Arun Kumar Thangavelu, "An Integrated Approach to Detect Phishing Mail Attacks A Case Study", ACM 978-1-60558-412-6/09/10, pp. 193-199, October, 2009.

8. Alireza Saberi, Mojtaba Vahidi, Behrouz Minaei Bidgoli, "Learn to Detect Phishing Scams Using Learning & Ensemble Methods", IEEE/ WIC/ ACM International Conference on Web Intelligence & Intelligent Agent Technology, 0-7695-3028-1/07, pp. 311-314, 2007.

9. Linfeng Li, Marko Helenius, Eleni Berki, "A Usability Test of Whitelist and Blacklist-based Anti Phishing Applications", ACM 978-1-4503-1637-8/12/10, pp. 195-202, October, 2012.

10. Ka-Ping Yee, Kragen Sitaker, "Passpet: Convenient Password Management & Phishing Protection", SOUPS, pp. 32-43, July, 2006.

11. Alireza Saberi, Mojtaba Vahidi, Behrouz Minaei Bidgoli, "Learn to Detect Phishing Scams Using Learning & Ensemble Methods", IEEE/ WIC/ ACM International Conference on Web Intelligence & Intelligent Agent Technology, 0-7695-3028-1/07, pp. 311-314, 2007.

12. Dipti Patel, Xin Luo, "Take a close look at Phishing", ACM 978-1-59593-909-8/00/0007, September, 2007.

13. Mahmoud Khonji, Youssef Iraqi, Andrew Jones, "Phishing Detection: A Literature Survey", IEEE Communications on Surveys & Tutorials, Vol. 15, No. 4, pp. 2091-2121, Fourth Quarter 2013.