Analyze of Phishing Violence and Alleviation

Ramesh Palanisamy, Senthil Jayapal, Mohammed Tariq Shaikh, and D. Thomas

Abstract— Now days phishing can be considered one of the simplest and oldest ways to steal important data from users on the internet. And only by collecting a small quantity of data about victim the attacker will be able to produce personalized and plausible e-mail. However, these days more ways that are try to be found and new technologies are inventive to deal with phishing. In this paper, I will present type, cause, prevention measures and dynamic features for growing phishing attack.

Index Terms—Phishing Violence, Alleviation.

I. INTRODUCTION

Identity theft in the past few years has become one of the most profitable and threatening crimes for all people that using internet. And it's indicate to the theft and also using of a person's identity information like bank details, credit card and identification number and so on for the purpose of theft of money or other offenses. And phishing attack is one kind of these crimes. Fake web site that have been created by the attackers for the purpose of steal the sensitive data and track the users on the internet, by the social engineering techniques like voice, SMS ,website ,e-mail and malware. The attacker can trick the user is called phishing. To identify phishing, many techniques are used in different ways of communication for example immediate messages, email, pop-up messages and at web page level.

II. LITERATURE SURVEY

Phishing has become now the main criminal activity on the internet, and it's the procedure of stealing private information online for the reason of financial fraud. So it necessary to have a good progress in educating companies and clients,identifying threats and countermeasures[1]. For malicious purposes, sensitive information, for instance passwords, usernames can be obtained in an illegal way in what is called phishing[2]. Phishing attack is one of the most important attack now a days in which an attacker attempts to obtain the victim's credential and impersonation. And because of the exaggerated use of mobile devices in everyday life, created mobile systems a superb target for attacks [3]. Security threats to network and systems measures unrelentingly creative due the expansion of web technology. Phishing is one of the significant threat in which the attackers tries to steal user's credentials by the use of fake e-mail messages, web sites or even both[4]. The graph of phishing attacks is rising radically, due to lack of consciousness and knowledge, ensuring monetary and emotional loss and impacts psychologically additionally. However, nowadays more ways that try to be found and new technologies are being inventive to deal with this increase of phishing attack [5]. In fact, phishing has become a complicated and growing threat to the security of everyone on the internet. The attacker will be able to produce a personalized and plausible e-mail only by collecting a small quantity of data about a victim. It's not simple to catch these phishers either, because most of them will hide the placement of their servers and add nearly complete obscurity [6]. To build system that protect users from deceptive (or phishing) sites, the designers must understand that attack ways work and why [7]. To identify phishing, many techniques are used in different ways of communication for example immediate messages, email, pop-up messages and at web page level[8]. Fake web site that have been created by the attackers for the purpose of steal the sensitive data and track the users on the internet, by the social engineering techniques like voice, SMS, website, e-mail and malware, the attacker can trick the user is called phishing[9]. Phishing and pharming are the familiar ways that thieves can get personal data to help them with identity theft[10].

III. TYPE OF PHISHING

Over the few previous years, attackers in terms of phishing and tracking down the customers have developed several techniques and methods. And these are some examples of phishing:

A. Deceptive Phishing

This phishing will deceive the user and make him believe something that is not true. The attacker will follow through sending an e-mail to the user related to their monetary account and issues they face that they are not conscious to sending them a link to update their personal information and password consequently, this information is used by the attackers against the users.

B. Malware-Based Phishing

This may damage the user's software particularly if that software used by a small company in which that software isn't updated for a long time. The attacker acquires nothing by doing so, however filled only his desire of seeing other suffer is considered as malicious crime.

C. Key loggers and Screen loggers

This is a malicious software attack in which the attacker monitors the keyboard inputs which he will send to the hacker on the other hand via the internet.

D. Session Hijacking

It is one kind of malware attack in which the attacker tracks the user's system and whatever the user do it will be monitored, so that when the user logs into bank details or

Published on December 15, 2019.
Ramesh Palanisamy, Ibra College of Technology, Oman.
(e-mail: rameshphd26@gmail.com)
Senthil Jayapal, Ibra College of Technology, Oman.
Mohammed Tariq Shaikh, Ibra College of Technology, Oman.
D. Thomas, Ibra College of Technology, Oman.

DOI: http://dx.doi.org/10.24018/ejbm 2019.4.6.170
other data that is helpful to the attacker, the malicious software will take over and use the data to transfer funds without the user's knowledge. Call it session because it happens only through sessions and not all time.

E. Web Trojans
It is almost like session hijacking, but is invisible to the user and appears when the user performs any transactions or logs into any important website and gathers all the data that the user has uploaded and forwarded to the attacker.

F. Hosts File Poisoning
This will deceive the users and make him believing that he is logging into the right website without knowing that he was deceived to sign in to a fake website that looks exactly like the popular website. And the attacker stole the information which done by poisoning the host file.

IV. DYNAMIC FEATURES FOR GROWING OF PHISHING ATTACKS
A. Lack of User Awareness
Users are not aware of the attacker's sneaky and devious methods.

B. Lack of Knowledge Towards Policy
Users are not very much acquainted with the internet transaction policies that, despite the technical elegant, make them more susceptible to phishing scams.

C. Technical Modernization
Attackers seem to be constantly upgrading themselves with the latest technology on the market. Moreover, even if the users are fully aware of phishing, by developing new innovative technologies the hackers might already be prepared to attack the users in spite of their awareness.

V. CASE OF PHISHING
The main reason for phishing has greatly impact the innocent people as a whole in accessing various confidential data that one has. It has outcomes for one of the reason and is known as "damage cause phishing". So this cause of the damage consist of the loss of important account. The graph of phishing attacks is rising radically with the increasing amount of unforeseen people who can affected by the agents of the attackers and also due to lack of consciousness and knowledge.

The important data include the name of their mother, card number and other confidential records. And because of the ease of retrieving public data, thieves can get more data by phishing. The phishes can use the details to create any type of fake account based on the data of the victims, once they have received appropriate information, which in turn will block the account of the victim. So it's important that most of users must have some information about "phishing" so the attacker will not be able to catch them.

VI. PREVENTIVE MEASURES TO AVOID PHISHING SCAMS
Here are some helpful tips for preventing frauds that must be taken seriously to prevent conditions like losing your money to any unknown website because most of time even after understanding what is best, we will still make incorrect decisions when we are deciding on things.

6.1 Keep privacy of your personal information. Things like your phone number, account number, password and address and so on.

6.2 Do not drop for emails obtained from an unfamiliar site to inquire about your private information and give you rigid limit time that you must filled that private information within a period of time.

6.3 Don't trust any emails or messages that say to you "you've won a lot of money" from legitimate site and ask you to answer to them with your bank account and other personal data.

6.4 Update your own system with the latest successful security software such as firewall, anti-spyware, anti-virus and spam filters and so on.

6.5 You should not acknowledged pop-up messages because most of them like the fraudsters' fishing rod. After you are hooked, you can't look back.

Countermeasures to Phishing Attacks
• Update Email Policies.
• Plan for ID Theft After a Data Breach.
• Regular OS Updates and Backups.
• Implement Message Authentication.
• Increase Collaboration Efforts.
• Using HTTPS
• A properly configured Web Browser
• Monitoring Phishing Sites
• Proper Email Client Configuration
• Using SPAM Filters
• Implement and Update Company Procedures
• Report Suspicious Activities

Stay Alert of Suspicious Emails, Links or Attachments

VII. CONCLUSION
In conclusion as we say phishing can be considered one of the simplest and oldest ways to steal significant data from the users on the internet. And because of that phishing become nowadays one of the major criminal activity. So It's necessary that most of users must have some knowledge about "phishing" and become more aware of those kinds of crimes.

REFERENCES


**Ramesh Palanisamy** obtained his Bachelor’s in Barathiar University Coimbatore, India. Then he obtained his Master’s degree in Computer Communications, from Barathiar University Coimbatore, India. Currently doing Ph.D. in Computer Science and Engineering (pursuing). Technical Qualifications CCNA, NSP (Network Support Professional), HNA (Hardware Networking Administrator), CCSI (Cisco Certified System Instructor). He published 19 international journals and 5 conferences. Currently working as lecturer in information technology at Ibra College of Technology. rameshphd26@gmail.com.

**Mohammed Tariq Shaikh** obtained his Bachelor’s Computer Science, Pakistan. Then he obtained his Master’s degree in Computer Science, Technical Qualifications Microsoft Certified Professional (MCP), Microsoft Certified Trainer (MCT), Microsoft Certified Solution Developer (MCSD), Microsoft Certified Professional + Internet, Microsoft Certified System Engineer (MCSE 2000), Microsoft Certified. Currently working as lecturer in information technology at Ibra College of Technology.

**Senthil Jayapal** obtained his Master of Technology in Information Technology at SRM University Chennai, India. His Bachelor of Engineering in Computer Science and Engineering at Annamalai University, Chidambaram, India. Currently working as lecturer in information technology at Ibra College of Technology.

**Darla Thomas** obtained his Master of computer applications at S.V. University, Tirupathi, India. Master of Technology from Nagarjuna University, Guntur, India. His Bachelor of Computer Applications at S.V. University, Tirupathi, India.