Phishing Technique

Mamta Patel
Research Scholar, MCA
Thakur Institute of Management Studies Career Development and Research(TIMSCDR), Mumbai,India

Vandana Patel
Research Scholar, MCA
Thakur Institute of Management Studies Career Development and Research(TIMSCDR), Mumbai,India

Hardik Pillai
Research Scholar, MCA
Thakur Institute of Management Studies Career Development and Research(TIMSCDR), Mumbai,India

Sreeja S. S.
Assistant Professor
Thakur Institute of Management Studies,
Career Development and Research (TIMSCDR)
Mumbai, India

ABSTRACT
Phishing is fraud. In phishing the attacker tries to read or retrieve information of a person. In this technique, the target gets a massage that appears that it is sent by some known person or reputed organization. On clicking the links in the message, it will install the malware on targeted device which will direct the target to a malicious website set up to trick them into displaying their personal and financial information, such as passwords credit card details. It is very much popular with cyber-criminals. Because it is very easy to make someone into clicking malicious link and get the details out of them rather than trying to seek through in someone's computer. The person who tries to do phishing use social networking sites and many other sources of information to collect the information about the target's personal history, their activities.

Keywords
Anti-phishing technologies, identity theft, Network security, Phishing attacks.

1. INTRODUCTION
Phishing is an online identity theft which aims to acquire confidential information such as banking password and credit card details from users. Phishing attacks have in news in recent past because the volume of such attacks have increased drastically, according to study 57 million US internet users have been identified as affected by phishing attacks and out of those 2 million were the actual victims of the attack and gave sensitive information to these attacks. Although these attacks have been in news for fairly long time but still the naive internet users became easy targets to such attacks just because of inexperience of the internet users. Attackers have been employing various technical spoofing tricks such as URL manipulation, hidden elements to look their site as similar as the target website. The most effective solution to phishing is educating users not to blindly follow links to web sites where they are to enter personal information such as passwords.

However, expecting that all users will understand the phishing threat and think before clicking any link is unrealistic. There will always be users which will be tricked into visiting a phishing web site. Hence, it is essential for researchers and industry to provide solutions for the phishing threat. The fig 1 shows the domain wise target of the phishing attacks, it can be depicted from the image that the most popular domain among the phishing attacks in .com domain.

1.1 Procedure of Phishing Attack
In this research paper, we assume that phishers use e-mail as their major method to carry out phishing attacks.

In general, phishing attacks are performed with the following four steps:

1) Phishers set up a counterfeited Web site which looks exactly like the legitimate Web site, including setting up the web server, applying the DNS server name, and creating the web pages similar to the destination Website, etc.

2) Send large amount of spoofed e-mails to target users in the name of those legitimate companies and organizations, trying to convince the potential victims to visit their Web sites.

3) Receivers receive the e-mail, open it, and click the spoofed hyperlink in the e-mail, and input the required information.

4) Phishers steal the personal information and perform their fraud such as transferring money from the victims‟ account.

2. LITERATURE SURVEY

2.1 Phishing
The act of sending an email to a user claiming to be a legitimate firm in an attempt to seek confidential data that can be exploited to perform identity theft is called as phishing. Phishing email directs the user to visit a webpage which is identical to the phishing target webpage where they are asked to enter confidential personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The webpage is however phished and set up only to access the information the user enters on the page.

2.2 Anti-Phishing
It is the act of detecting whether a visited webpage is legitimate or phished by extracting different properties of the webpage or by studying the visual contents of the webpage. It is essential to provide an efficient technique to differentiate between a legitimate page and a phished page, to counter the ever-increasing threat of phishing attacks.

2.3 Early Phishing on AOL
Phishing on AOL(America online) has been the first ever appearance of phishing in the world of information technology , a software AOHell was released in early 1995, was a program

designed to hack AOL users by allowing the attacker to gain access of various confidential details of the user. After AOL brought in measures in late 1995 to prevent using algorithmically generated PIN to open accounts, AOL crackers resorted to phishing for legitimate accounts and exploiting AOL. In September 2003, the first known phishing attack against a retail bank was reported by The Banker in an article written by Kris Sangani titled Battle Against Identity Theft By 2004, phishing was recognized as a fully industrialized part of the economy of crime: specializations emerged on a global scale that provided components for cash, which were assembled into finished attacks.

3. CLASSIFICATION OF PHISHING ATTACKS

Phishing attacks can be classified into various types according to the way attack is done. According to many researchers the various types of phishing attacks has been described below.

3.1 Deceptive Phishing

In this technique the phished webpage will ask the user to enter details to verify account information,, fictitious account charges, undesirable account changes, system failure requiring users to re-enter their information, new free services requiring quick action, and many other exciting offers so as to develop interest in users mind with the hope that the victim will click on the link as will provide the confidential personal information to the bogus webpage which can be further used to perform scams.

3.2 Malware Based Phishing

This technique involves making run a malicious code on user's machine which is capable of performing tasks which will provide details of the confidential data entered by the user. Malware can be introduced in the user's machine as an attachment, by exploiting security vulnerabilities, as a downloadable file from a web site.

3.3 Web Trojans

In this technique, the pop-up invisibly runs when users are attempting to log in and they collect the personal information from the user's machine locally and transmits the information to the server the phisher is using to collect information of the victims.

3.4 System Reconfiguration Attacks

In this technique, the phisher modifies settings on a user's PC for performing various malicious operations without the knowledge of the user. For example: URLs in a favorites file can be altered to direct users to look a website which is visually identical to the target website. For example: a bank website URL may be changed from "www.gmail.com" to "www.gmaiL.com".

3.5 Pharming

This technique modifies the company's host file or DNS so that when the user wants to log in or access that website, the changes made by the phisher will result in opening of phished website instead of the legitimate one. Hence used will submit the information to a phished page.

3.6 Content Injection Phishing

In this technique, the hacker replaces some part of code from the legitimate website which in turn results in submitting information to the server used by the phisher instead of submitting to the legitimate website.

3.7 Man-in-the-Middle Phishing

In these attacks phisher positions, themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

4. CLASSIFICATION OF ANTI PHISHING TECHNIQUES

4.1 Content Filtering

In this anti-phishing technique, the emails before entering into the mailbox of the user is filtered using machine learning techniques such as Bayesian Additive Regression Trees (BART) or Support Vector Machines.

4.2 Blacklisting

Blacklist is collection of known phishing Web sites/addresses published by trusted entities like goggle's and Microsoft's black list. It requires both a client & a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing sites.

4.3 Symptom Based Prevention

Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected.

4.4 Domain Binding

It is a client's browser based techniques where sensitive information (e.g. name, password) is bind to particular domains. It warns the user when he visits a domain to which user credential is not bind.

5. CONTENT BASED PHISHING

Gold Phish tool implements this technique and uses Google as its search engine. This mechanism gives higher rank to well-established web sites. It has been observed that phishing web pages are active only for short period of time and therefore will acquire low rank during internet search and this becomes basis for content based anti-phishing approach. The design approach can be broken down into three major steps. The first step is to capture an image of the current website in the user's web browser. The second step is to use optical character recognition techniques to convert the captured image into computer readable text. The third step is to input the converted text into a search engine to retrieve results and analyze the page rank.

5.1 Advantages

Generally, Gold Phish does not result in false positive and provides zero-day phishing.

5.2 Disadvantages

Gold Phish delays the rendering of a webpage. It is also vulnerable to attacks on Google's Page Rank algorithm and Google's search service.

6. CHARACTER BASED ANTI PHISHING TECHNIQUES

Many time phishers tries to steal information of users by convincing them to click on the hyperlink that they embed into phishing email. A hyperlink has a structure as follows.

AntiPhish is based on the premise that for inexperienced, technically unsophisticated users, it is better forum application to attempt to check the trustworthiness of a web site on behalf of the user. Unlike a user, an application will not be fooled by obfuscation tricks such as a similar sounding domain name.

6.1 Main functionality

AntiPhish is an application that is integrated into the web browser. It keeps track of a user's sensitive information (e.g., a password) and prevents this

Information from being passed to a web site that is not considered "trusted" (i.e., "safe"). The development of AntiPhish was inspired by automated form-filler applications. Most browsers such as Mozilla or the Internet Explorer have integrated functionality that allows form contents to be stored and automatically inserted if the user desires. This content is protected by a master password. Once this password is entered by the user, a login form that has previously been saved, for example, will automatically be filled by the browser whenever it is accessed. Antiphish takes this common functionality one step further and tracks where this information is sent.

6.2 Controlling the sensitive information flow

As far as AntiPhish is concerned, every page that contains a form is a potential phishing page. HTML form elements that can be used by the attacker to phish information from the user are text field elements of type text and password and the HTML text area element. Hence, whenever the user enters information into any of these form elements (e.g., the user presses a key or pastes text), AntiPhish checks the list of previously captured values (i.e., the "watch list"). For each value in this list that is identical to the one just entered by the user, the corresponding domain is determined. If the current site is not among these domains, a phishing attempt is assumed. The reason is that sensitive information is about to be transmitted to a site that is not explicitly listed as trusted. If AntiPhish detects, for example, that the user has typed his online banking password into a text field on a web site that is not in the online banking web site domain (i.e., an "untrusted" web site), then it generates an alert and redirects to an information page about phishing attacks. Interaction events that the user generates within the browser are used to intercept sensitive information flow to untrusted web sites before the user can submit the information. AntiPhish is activated every time the user presses a key, loads a new page, clicks the mouse or has the current focus on a text element (i.e., text field or text area). The flowchart in Figure 4 depicts how the sensitive information flow is controlled by AntiPhish.

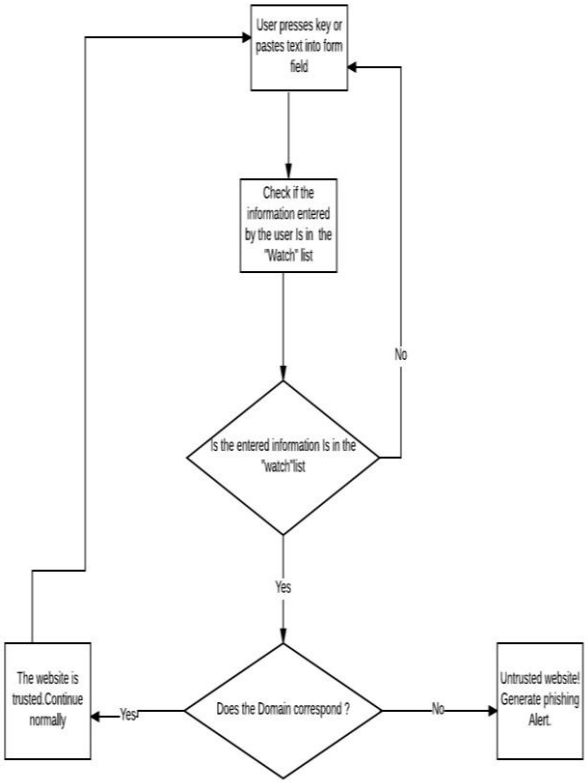

Fig.1 Flowchart showing how the sensitive information flow is controlled by AntiPhish

7. REPORT PHISHING

Whenever user finds a particular webpage as spam one he can report the phishing on following websites:

Businesses and consumers can file phishing reports with the following organizations:

Anti-Phishing Working Group www.antiphishing.org

Digital Phishnetwww.digitalphishnet.org

Federal Trade Commission www.consumer.gov/idtheft

Internet Crime Complaint Center (a joint project of the FBI and the National Collar Crime Center)www.ic3.gov

Trend Micro Anti-Fraud Unit antifraud@support.trendmicro.com

8. FUTURE WORK

We are currently working on the implementation ofAntiPhishfor the Internet Explorer (IE) browser. Supporting IE is important because a large majority of Internet users are using this browser. AntiPhish is free for public use. We are also planning to officially register the project with the Mozilla extensions web site. As discussed in Section 3, AntiPhish currently needs user support to capture and store sensitive information. For some users, it might be better to provide a mode where sensitive information is automatically captured and stored. This could be done by capturing and caching the information every time information is entered and submitted to a web site. In order to implement this functionality, submission events also need to be intercepted. In Mozilla Browsers, submission events are easily captured by implementing call-back functions that are automatically invoked whenever a form is submitted.

9. CONCLUSION

Phishing is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information. The last years have brought a dramatic increase in the number and sophistication of such attacks. Although phishing scams have received extensive press coverage, phishing attacks are still successful because of many inexperienced and unsophisticated Internet users. Attackers are employing a large number of technical spoofing tricks such as URL obfuscation and hidden elements to make a phishing web site look authentic to the victims. There will always be users that are tricked into visiting a phishing web site. Therefore, it is important for researchers and industry to provide solutions for the phishing threat.

Phishing differs from traditional scams primarily in the scale of the fraud that can be committed.

In order to combat phishing, business and consumers need to adopt best practices and practice awareness, educate themselves about phishing and anti-phishing techniques, use current security protection and protocols, and report suspicious activities. By doing so, they can reduce their exposure to fraud and identity theft, safeguard their confidential information, and help fight one of today's most serious and ongoing threats of phishing. The most effective solution to phishing is training users not to blindly follow links to web sites where they have to enter sensitive information such as passwords. The final technical solution to phishing involves significant infrastructure changes in the Internet that are beyond the ability of any one institution to deploy. However, there are steps that can be taken now to reduce the consumer's vulnerability to phishing attacks. Some of those steps are:

For Corporations:

- Establish corporate policies and communicate them to consumers.
- Provide a way for the consumer to validate that the E-mail is legitimate
- Stronger authentication at web sites.
- Monitor the Internet for potential phishing web sites.
- Implement good quality anti-virus, content filtering and anti-spam solutions at the Internet gateway.

For Consumers:

- Automatically block malicious/fraudulent E-mail.
- Automatically detect and delete malicious software.
- Automatically block outgoing delivery of sensitive information to malicious parties.
- Be suspicious. All of these technologies are available now and can be deployed by both consumers and institutions interested in protecting their customers.

10. REFERENCES

[1] The Antiphishing Working Group (2004) Home Page, www.anti-phishing.org

[2] Verisign Home Page (2005), Anti-Phishing Solution, www.verisign.com/verisign-business- solutions/anti-phishing-solutions/

[3] Sangani, Kris (September 2003). "The Battle Against Identity Theft". *The Banker* **70** (9): 53–54.

[4] Matthew Dunlop, Stephen Groat, and David Shelly‖ GoldPhish: Using Images for Content-Based Phishing Analysis‖, in proceedings of internet monitoring and protection(ICIMP), fifth international conference, Barcelona, Pages 123-128, 2010.