Phishing Defense Mechanism

[1]Ritika Arora, [2]Sunny Behal

[1,2]SBSSTC, Ferozepur, Punjab, India

Abstract

Phishing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information. Phishing scams pose a serious threat to end users and commercial institutions alike. Email continues to be the favorite vehicle to inculcate such scams mainly due to ability to easily spoof them. Several approaches, both generic and specialized, have been proposed in the literature to address this issue .Phishing came into existence as nowdays people have very least knowledge about the security measures of and people get easily fool to phished site and all there information is lost.This paper covers the technologies and security flaws Phishers exploit to conduct their attacks, and rendered mechanism has been proposed in this paper which consist of various prevention and detection techniques.

Keywords

Phishing ,Hacking ,Pharming, Anti-Phishing

I. Introduction

Phishing is a kind of online security attack where the attacker creates a replica of an existing web page to fool users in order to hack their personal, financial, or password data. It is a malicious activity whereby an attacker (phisher) tries to trick Internet users into providing confidential information. It is a serious problem because phishers can steal sensitive information, such as users' bank account details, social security numbers, and credit card numbers. To achieve this goal, a phisher first sets up a fake website that looks almost the same as the legitimate target website. The URL of the fake website is then sent to a large number of users at random via e-mails or instant messages. Unsuspecting users who click on the link are directed to the fake website, where they are asked to input their personal information. Despite the fact that these phishing sites look identical or nearly identical to the real sites they imitate, user studies have shown that users ignore browser-based indicators and often use the appearance of a site to judge the authenticity of sites. To respond to this threat, software vendors and companies have released a variety of anti-phishing toolbars. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting [1]. As people conduct an increasing number of transactions using the Internet, Internet security concerns have also been increased.

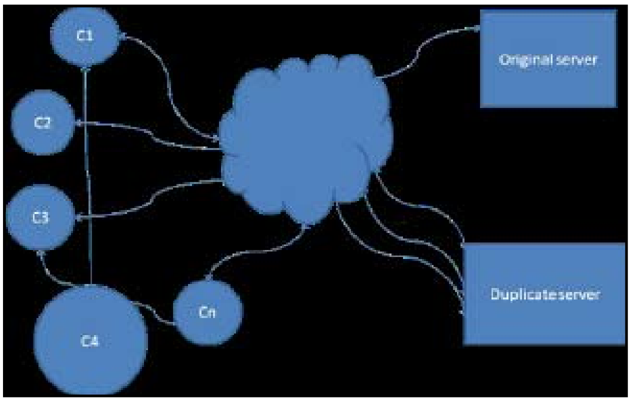


Fig. 1. Architecture of Phishing Attacks

The hybrid architecture where we use phishing attack, email bombing, Trojan horse, data stealing techniques. Through these techniques we can steal the data and other confidential information. Consider there are nodes in the network. For example consider the node C4 which has the contacts of C1, C2, C3, Cn the contact of C2 is not present in the address book of the C4 node.C4 node has the Trojan horse running in it, so the contacts C1, C3, Cn are Email bombed.C2 contact is not a victim of the Trojan horse so it is able to access the original server directly. The email content has the link to launch the phishing attack. When the user clicks on the link he is redirected to the duplicate server instead of original server. Using the details he entered he is redirected back to the original server. In this whole process the victim's account is compromised by stealing the data which the user entered in a fake website [2].

B. Types of Phishing Attacks

Phishing is a process of procuring confidential information like usernames and passwords by fraud means sending legitimate emails and fooling unaware users. Mailing system have evolved a big way by filtering out spam to an extent.There are various types of phishing attacks which are found and their dercription is given below:

1. Deceptive Phishing

The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive email message.

2. 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

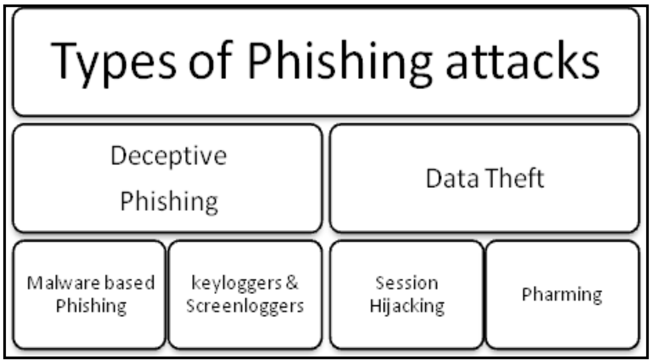


Fig. 2: Types of Phishing Attacks

3. Keyloggers and Screenloggers

are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started.

4. Session Hijacking

describes an attack where users' activities are monitored until they sign in to a target account or transaction and establish their bona fide credentials.

5. Web Trojans

pop up invisibly when users are attempting to log in. They collect the user's credentials locally and transmit them to the phisher.

6. Hosts File Poisoning

When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. By "poisoning" the hosts file, hackers have a bogus address transmitted,taking the user unwittingly to a fake "look alike" website where their information can be stolen.

7. System Reconfiguration Attacks

modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofabc.com".

8. Data Theft

Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers[3]. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

9. DNS-Based Phishing ("Pharming")

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.

II. Detection Techniques

A "phish" is a term for a scam website that tries to look like a site that you know might well and visit often. The act of all these sites trying to steal your account information is called phishing and there are various detection techniques to detect Phishing which are listed below:

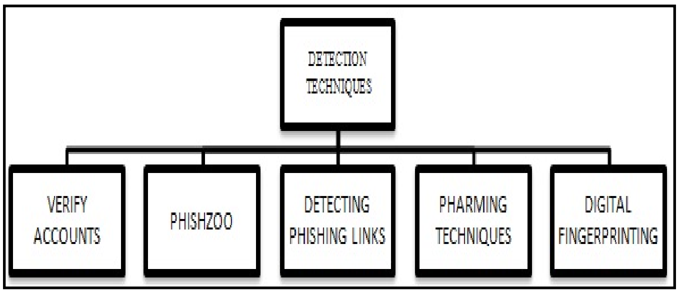


Fig. 3: Detection Techniques

1. Beware of emails that demand for an urgent response from your side. Some of the examples are:
2. You may receive an email which appears to have come from your bank or financial organization stating that "your bank account is limited due to an unauthorized activity [3]. Please verify your account asap so as to avoid permanant suspension". In most cases, you are requested to follow a link (URL) that takes you to spoofed webpage (similar to your bank website) and enter your login details over there.

A. Detecting Phishy Links

Detecting and blocking messages containing encoding and redirection tricks are fairly straightforward for an inline mail (or mail-aware) device, such as a spam filter or general intrusion prevention device [4]. In fact, it gets easier for automated syntactical analysis machines such as these to detect phish links when the phisher incorporates obfuscation tactics to messages. For instance, "normal" links, like http://www.ebay.com are easy to differentiate from abnormal links, <areahref="http://%77w%77.goo%67le.fr/ur%6c%3fq=http%3a%2f%2f%77%77%77%2eebay.c%6fm">

B. Approaches To Phishing detection Using Match and Probalistic Digital Fingerprinting Techniques

Fingerprint detection is a technique used to identify copying between documents, in this case faux websites. Applying fingerprinting technique to this problem allows for the detection of copying between a legitimate institution's website or of another, similar attack.This allows us to train previous attacks, legitimate web pages, or a mixture of both. By identifying this copying, we identify the attacks [5]. The benefits of fingerprinting are two-fold. First, in precise identification of an attack, but secondly by forcing scammers to further obfuscate their layout and source code to avoid printing against an original site or a previous attack. In doing so, this increases the risk that the site will appear disgenuine

C. PhishZoo

An Automated Web Phishing Detection Approach Based on Profiling and Fuzzy Matching- PhishZoo—that uses profiles of trusted websites' appearances built with fuzzy hashing techniques to detect phishing. PhishZoo has the potential to have a beneficial impact on the phishing "arms race" by reducing the effectiveness of sites that look too much like the real sites and thus giving users a chance to detect sites that "look phishy [6].

D. Pharming Techniques

Pharming generally refers to a class of spoofing attacks whereby a victim's normalname resolution infrastructure is subverted specifically for the purpose of capturing financial account information [7]. These attacks have been well-documented and understood by both the IT security industry and unscrupulous click-through revenue generators, but when financial data is involved, it has become "phashionable" to "aphix" a "ph" to a common word and "phormulate" a new attack term. There are two typical methods to conduct a pharming attack:

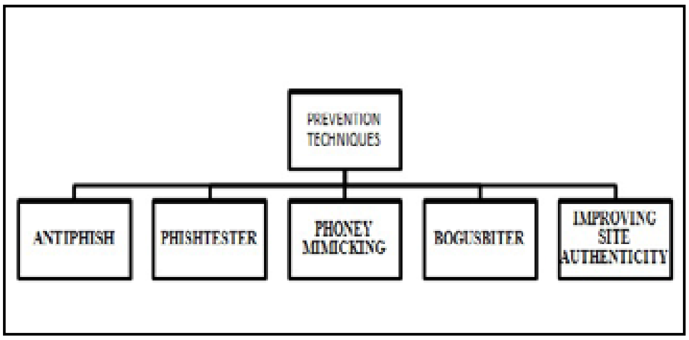
1. DNS cache poisoning, where a DNS server controlled by an attacker provides DNS answers to unasked questions. A client may want to resolve www.evilsite.com, and ns.evilsite.com provides an answer to both www.evilsite.com and www.paypal.com, and both answers are cached. Then, when a future user attempts to resolve www.paypal.com he instead retrieves the cached information.
2. Local hosts file poisoning, whereby a Trojan (typically in the form of spyware or other surreptitious downloader mechanism) rewrites a victim's local hosts mapping file. In Windows, this is stored as %SYSTEMROOT%/system32/drivers/etc/hosts. Name queries, before they are sent to a

DNS server, are first checked against this file – so providing an attacker's IP for a www.paypal.com will subvert a normal name lookup.

III. Recent Facts on Phishing Scams

Phishing scams have been escalating in number and sophistication with every month that goes by. A phishing attack today now targets audience sizes that range from mass-mailings to millions of email addresses around the world, through to highly targeted groups of customers that have been enumerated through security faults in small clicks-and-mortar retail websites. Using a multitudeof attack vectors ranging from man-in-the-middle attacks and key loggers, through to complete recreation of a corporate website, Phishers can easily fool customers into submitting personal, financial and password data. While Spam was (and continues to be) annoying, distracting and burdensome to all its recipients, Phishing has already shown the potential to inflict serious losses of data and direct losses due to fraudulent currency transfers. According to a recent study by Gartner, 57 million US Internet users have identified the receipt of email linked to phishing scams, and about 1.7 million of them are thought to have succumbed to the convincing attacks and tricked them into divulging personal information. Studies by the Anti Phishing Working Group (APWG) have concluded that Phishers are likely are likely to succeed with as much as 5 percent of all message recipients.

IV. Prevention Techniques



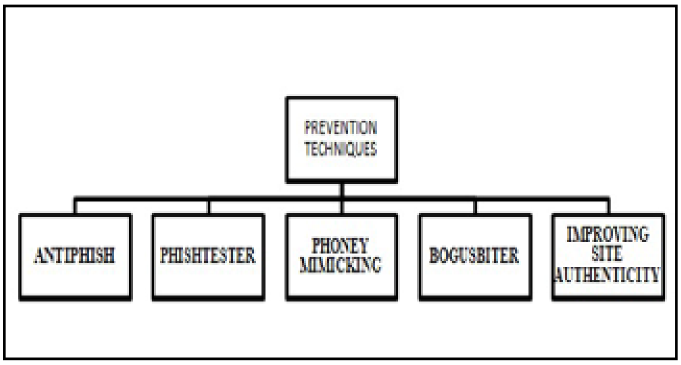


Fig. 4: Prevention Techniques

A. Anti-Phish

Anti-phishing.info is information about the internet scam known as "phishing"! Detect phishing attacks, how to prevent and avoid being scammed, how to react when you suspect or reveal a phishing attack and what you can do to help stop phishers. Legitimate websites always use a secure connection (https://) on those pages which are intended to gather sensitive data such as usernames and passwords, account numbers or credic card details [8]. You will see a lock icon 🔒 in your browser's address bar which indicates a secure connection.In most cases, unlike a legitimate website, a phishing website or a spoofed webpage will not use a secure connection and does not show up the lock icon. So, absence of such security features can be a clear indication of phishing attack. Always double-check the security features of the webpage before entering any of your personal information. Always use a good antivirus software, firewall and email filters to filter the unwanted traffic. Also ensure that your browser is up-to-date with the necessary patches being applied [8]. You can directly send an email to spam@uce.govorreportphishing@antiphishing.org reporting an attack. You can also notify the Internet Crime Complaint Center of the FBI by filing a complaint on their website: www.ic3.gov [9].

B.PhishTester: Automatic Testing of Phishing Attacks :It is a tool named Phish Tester to automate the testing process. We evaluate the proposed approach with both phishing and real applications. The initial results show that the approach incurs negligible false negatives (less than 3%) and zero false positive for detecting phishing and real websites, respectively. The approach can be complementary to current anti-phishing tools to discover advanced phishing attacks [10].

Warning: Something's Not Right Here!

malware.testing.google.test contains malware. Your computer might catch a virus if you visit this site.

Google has found malicious software may be installed onto your computer if you proceed. If you've visited this site in the past or you trust this site, it's possible that it has just recently been compromised by a hacker. You should not proceed, and perhaps try again tomorrow or go somewhere else.

We have already notified malware.testing.google.test that we found malware on the site. For more about the problems found on malware.testing.google.test, visit the Google Safe Browsing diagnostic page.

If you understand that visiting this site may harm your computer, proceed anyway.

□ Help improve detection of malware by sending additional data to Google about sites on which you see this warning. This data will be handled in accordance with the Safe Browsing privacy policies.

C. PHONEY

Mimicking User Response to Detect Phishing Attacks It is an approach to detect phishing attacks using fake responses which mimic real users, essentially, reversing the role of the victim and the adversary [11]. The prototype implementation called PHONEY, sits between a user's Mail Transfer Agent (MTA) and phishing attacks.

D. Bogus Biter

A transparent protection against phishing attacksBogusBiter, a unique client-side anti-phishing tool, which transparently feeds a relatively large number of bogus credentials into a suspected phishing site. BogusBiter conceals a victim's real credential among bogus credentials, and moreover, it enables a legitimate web site to identify stolen credentials in a timely manner. Leveraging the power of client-side automatic phishing detection techniques, BogusBiter is complementary to existing preventive anti-phishing approaches.

V. Improving Site Authenticity

The root of the phishing problem is that users are not able to identify if the website is original or fake. Looking at the URL and SSL certificate carefully can really help but not all users have the time nor technical skill to analyze and One method is to personalize the login page for each user. We do the login in two stages . First the user enters only the user-id and not the password. Once user-id is submitted, server returns a page where user gets to see an image which he had selected at time of registration. If the image is matching he supplies the password and all is fine. If the image is not being shown it raises an alert and customer does not provide the password. Phisher doesnot know which image to display in this intermediate page.

VI. Comparison of Various Techniques

There are various techniques for detecting phishingattackslikeAntiphish,Phishtester,PhoneyMimicking,Bogusbiter,Plugins.Out of all these techniques AntiPhish is the most popular technique and is used nowdays for securing secured websites.

VII. Conclusions

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 hidden elements to make a phishing web site look authentic to the victims. 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. However, expecting that all users will understand the phishing threat and surf accordingly is unrealistic. There are many prevention techniques employed which are used to prevent phishing likePhoneyMimicking,BogusBiter,PhishTester,Anti-Phish,Site Authenticity out of these antiphish is the best employed method which can be used to avoid phishing attacks.

VIII. Acknowledgment

I owe a great many thanks to a great many people who helped and supported me during writing of this paper.My deepest thanks to my Mentor Er.Sunny Behal who guided and supported me in every phase of writing this paper. I deem it my privilege to have carried out my paper under his able guidance and I am grateful to my parents who are inspirational in their understanding patience and constant encouragement.

References

[1] R. Dhamija, J. D. Tygar, M. Hearst,"Intoduction to Phishing Works", In: Proc. of the SIGCHI conference on Human Factors in computing systems, 2006, pp. 581-590.

[2] W. Y. Liu, X. T. Deng, G. L. Huang, et al.,"An Antiphishing Strategy Based on Visual SimilarityAssessment", IEEE Internet Computing, 2006, Vol. 10, pp. 58-65.

[3] Engin, K., K. Christopher,"Protecting Users Against Phishing Attacks with AntiPhish", in Proceedings of the 29th Annual International Computer Software and Applications Conference(COMPSAC'05) Vol. 1-Vol. 01.2005 IEEE Computer Society.

[4] Liu, W., et al.,"Phishing Webpage Detection", in Proceedings of the Eighth International Conference on Document Analysis anRecognition 2005", IEEE Computer Society.

[5] N Shivakumar, H G-Molina,"SCAM: A copy detection mechanismfor digital documents", In Proceedings of the Second Annual Conference on the Theory and Practice of Digital Libraries, 1995.

[6] Yue Zhang, Serge Egelman, Lorrie Cranor, Jason Hong "Phinding Phish: Evaluating PhishZoo Tools", In Proceedings of the 14th Annual Network & Distributed System Security Symposium (NDSS2007).

[7] Rachna Dhamija, J.D. Tygar,"The Battle Against Phishing:Dynamic Security Skins, In SOUPS 2005: Proceedings of the 2005 ACM Symposium on Usable Security and Privacy, ACM International Conference Proceedings Series, ACM Press, July 2005, pp. 77-88.

[8] "The Antiphishing Working Group". Home Page, [Online] Available: http://www.anti-phishing.org, 2004

[9] Michael Atighetchi, Partha Pal,"Attribute Based Prevention of Phishing Attacks", IEEE International Synposium on Network Computing and Applications, Vol. 10, May 2009.

[10] Rosiello, E. Krida, C. Kruegel, F. Ferrandi,"Phish TesterAutomatic Testing of Phishing Attacks", Proc. of the 3rd International Conference on Security and Privacy in Communication Networks, Nice, France, Sept 2010, pp. 454-463.IEEE Computer Society.

Ritika Arora, M.Tech(Computer Science & Engineering), Area of Interest : Networking Works as a student and is doing M.Tech from SBSSTC ,Ferozepur and is currently working on her dissertation.

Er. Sunny Behal, Assistant Professor (SBSSTC Ferozepur Punjab) Area of Interest: Networking,Botnets,Intrusion detection System, Work as an Assistant Professor in Shaheed Bhagat Singh State Technical Campus,Ferozepur and has many papers published in International Conferences & Journals and is having teaching experience of 10 years.