Analysis of Phishing in Networks

Vignesh.M, Gokul Ram.T, Akhil.R, Rajesh Kumar N.S.R, Karthikeyan.R

Abstract - Problem statement: Phishing is one of the growing internet crime and it becoming popular because these days, there is a huge black market out there of scammers and spammers, all of whom are willing to pay someone for providing them with details, such as Social security numbers, Driver's license numbers, Names, date of births, etc. Credit card numbers, bank account numbers. Amazingly, a single valid credit card number can be sold on the black market for over $100 - which clearly shows you why there is an incentive for some people to participate in activities such as phishing. Wherever there is a profit to be made, people will flock to the industry - and in the case of phishing, it is people with very little conscience or very low morale. The draw of a quick buck is all it takes to turn an ordinary person in to a phishing professional. Approach: Here we approach some preventive measures and some technical tips to prevent and avoid phishing scam. Results: The results of phishing caused by phishing ranges from denial of access to e-mail to substantial financial loss. 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. Conclusion: Here we conclude with providing some preventive methods are User Education - Phishing exploits human vulnerabilities such that technical solutions can only block some of the phishing web sites, Anti-Phishing Groups and obtaining Legal Aspects.

Index terms - phishing, analysis of phishing, web crime, prevent phishing, cybercrime, web security, Anti-phishing.

1. INTRODUCTION

Phishing is the method of making to get some information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail 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. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. A phishing technique was described in detail in 1987, and (according to its creator) the first recorded use of the term "phishing" was made in 1995. The term is a variant of *fishing* probably influenced by *phreaking* and alludes to "baits" used in hopes that the potential victim will "bite" by clicking a malicious link or opening a malicious attachment, in which case their financial information and passwords may then be stolen.

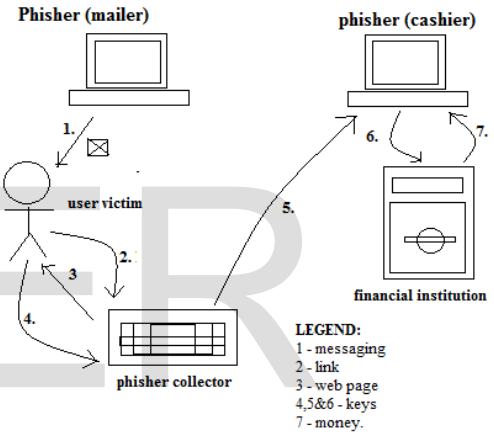

Figure 1.1 – phishing information flow

A complete phishing attack involves three roles of phishers. Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites.

Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Finally, cashers use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers. The information flow is shown in Figure 1.1

1.1 History and current status of phishing

A phishing technique was described in detail, in a paper and presentation delivered to the International HP Users Group, Interex. The first recorded mention of the term "phishing" is found in the hacking tool AOHell (according to its creator), which included a function for stealing the passwords of America Online users. A recent and popular case of phishing is the suspected Chinese phishing campaign targeting Gmail accounts of highly ranked officials of the United States and South Korean's Government, military, and Chinese political activists. The Chinese government continues to deny accusations of taking part in cyber-attacks from within its

borders, but evidence has been revealed that China's own People's Liberation Army has assisted in the coding of cyber-attack software.

2. METHODS OF PHISING

2.1 Types of Phishing Attacks

Numerous different types of phishing attacks have now been identified. Some of the more prevalent are listed below.

2.1.1 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. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.

2.1.2 Malware-Based Phishing

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--a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

2.1.3 Key loggers and Screen loggers

Key loggers and screen loggers 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 as well as into system files as device drivers or screen monitors.

2.1.4 Session Hijacking

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. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

2.1.5 Web Trojans

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.

2.1.6 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. The majority of SMB users' PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. 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.

2.1.7 System Reconfiguration Attacks

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".

2.1.8 Data Theft.

Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, and employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

2.1.9 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 host's 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. The result: users are unaware that the website where they are entering confidential information is controlled by hackers and is probably not even in the same country as the legitimate website.

2.1.10 Content-Injection Phishing

Content-Injection Phishing describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.

2.1.11 Man-in-the-Middle Phishing

Man-in-the-Middle Phishing is harder to detect than many other forms of phishing. In these attacks hackers position 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.

2.1.12 Search Engine Phishing

Search Engine Phishing occurs when phishers create websites with attractive (often too attractive) sounding offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks. Victims who use these sites to save or make more from interest charges are encouraged to transfer existing accounts and deceived into giving up their details.

2.1.13 Filter evasion

Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.

2.1.14 Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against PayPal.

A Universal Man-in-the-middle (MITM) Phishing Kit, discovered in 2007, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.

To avoid anti-phishing techniques that scan websites for phishing-related text, phishers have begun to use Flash-based websites. These look much like the real website, but hide the text in a multimedia object.

2.1.15 Phone phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

2.1.16 other techniques

1. Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information.
2. One of the latest phishing techniques is tab nabbing. It takes advantage of the multiple tabs that users use and silently redirects a user to the affected site.
3. Evil twins is a phishing technique that is hard to detect. A phisher creates a fake wireless network that looks similar to a legitimate public network that may be found in public places such as airports, hotels or coffee shops. Whenever someone logs on to the bogus network, fraudsters try to capture their passwords and/or credit card information.

3. RESULTS:

3.1Damages caused by phishing

The damage caused by phishing ranges from denial of access to e-mail to substantial financial loss. 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. In 2007, phishing attacks escalated. 3.6 million Adults lost US$3.2 billion in the 12 months ending in August 2007. Microsoft claims these estimates are grossly exaggerated and puts the annual phishing loss in the US at US$60 million. 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.

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 (and it still insists that its policy is not to do so), although losses to the tune of €11,300 were made good.

4. DISCUSSION

Here we discussed that what are the suggestions should provide to prevent and avoid these phishing activities.

4.1 Suggestions to avoid phishing

Some computer users (and even some IT professionals) have been confused about the defection of a "phishing" attack. What exactly is a phishing attack? A phishing attack is when you receive an official-looking e-mail from an online banking or financial institution – it could even be eBay or PayPal, or any other service that deals with money. The e-mail states that you should click a link and confirms your login and password to this particular institution (or enters your account number or credit card number).

As soon as you click on the link, you are sent to a Web page that looks remarkably similar to the company's real Web site, but it's not the company's real Web site. What is happening is that you are sent to a fake page that is controlled by the criminal who is behind the phishing scheme. As soon as you type your login\password or

account information or credit card number, the thieves or hackers capture the information and then commit identity theft by using your credit card or stealing money from your account. Below are 12 steps that users can take to keep from being victimized by phishing scams. And after that are some examples of phishing scams.

4.1.1 Keep antivirus up to date

One of the most important things you can do to avoid phishing attacks is keep your antivirus software up-to-date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising your Web address bar or mimicking an https secure link. If your antivirus software is not up-to-date, you are usually more susceptible to attacks that can hijack your Web browser and put you at risk for phishing attacks.

4.1.2 Do not click on hyperlinks in e-mails

It is never a good idea to click on any hyperlink in an e-mail, especially from unknown sources. You never know where the link is going to really take you or whether it will trigger malicious code. Some hyperlinks can take you to a fake HTML page that may try to scam you into typing sensitive information. If you really want to check out the link, manually retype it into a Web browser.

4.1.3 Take advantage of anti-spam software

Anti-spam software can help keep phishing attacks at a minimum. A lot of attacks come in the form of spam. By using anti-spam software such a Qurb, you can reduce many types of phishing attacks because the messages will never end up in the mailboxes of end users.

4.1.4 Verify https (SSL)

Whenever you are passing sensitive information such as credit cards or bank information, make sure the address bar shows "https://" rather than just "http://" and that you have a secure lock icon at the bottom right hand corner of your Web browser. You can also double-click the lock to guarantee the third-party SSL certificate that provides the https service. Many types of attacks are not encrypted but mimic an encrypted page. Always look to make sure the Web page is truly encrypted.

4.1.5 Use anti-spyware software

Keep spyware down to a minimum by installing an active spyware solution such as Microsoft Antispyware and also scanning with a passive solution such as Spybot. If for some reason your browser is hijacked, anti-spyware software can often detect the problem and provide a fix.

4.1.6 Get educated

Educate yourself on how to prevent these types of attacks. A little research on the Internet may save you a great deal of pain if you are ever the victim of identity theft. You can report any suspicious activity to the FTC (in the U.S.). If you get spam that is phishing for information, forward it to spam@uce.gov. You can also file a phishing complaint at www.ftc.gov. Another great resource is the FTC's identity theft page to learn how to minimize your risk of damage from ID theft. Visit the FTC's spam page to learn other ways to avoid e-mail scams and deal with deceptive spam.

4.1.7 Use the Microsoft Baseline Security Analyzer (MBSA)

You can use the MBSA to make sure you have all of your patches up to date. You can download this free tool from Microsoft's web site. By keeping your computer patched, you will protect your systems against known exploits in Internet Explorer and Outlook (and Outlook Express) that can be used in phishing attacks.

4.1.8 Firewall

Use a desktop (software) and network (hardware) firewall. On the desktop, you can use a software firewall such as Zone Alarm or use Microsoft's built-in software firewall in Windows XP. The incorporation of a firewall can also prevent malicious code from entering your computer and hijacking your browser.

4.1.9 Use backup system images

Keep a backup copy or image of all systems in case of foul play. You can then revert back to a pure system state if you suspect that a phishing attack, spyware, or malware has compromised the system. Tools such as Symantec Ghost and Acronis True Image are perfect for this.

4.1.10 don't enter sensitive or financial information into pop-up windows

A common phishing technique is to launch a bogus pop-up window when someone clicks on a link in a phishing e-mail message. This window may even be positioned directly over a window you trust. Even if the pop-up window looks official or claims to be secure, you should avoid entering sensitive information because there is no way to check the security certificate. Close pop-up windows by clicking on the X in the top-right corner. Clicking cancel may send you to another link or download malicious code.

4.1.11 Secure the hosts file

A hacker can compromise the hosts file on desktop system and send a user to a fraudulent site. Configuring the host file to read-only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protect against tampering by outside attackers and keep browsing safe.

4.1.12 Protect against DNS pharming attacks

This is a new type of phishing attack that doesn't spam you with e-mails but poisons your local DNS server to redirect your Web requests to a different Web site that looks similar to a company Web site (e.g. eBay or PayPal). For example, the user types in eBay's Web address but the poisoned DNS server redirects the user to a fraudulent site. This is what I consider new age phishing. This needs to be handled by an

administrator who can use modern security techniques to lock down the company's DNS servers.

4.2 Ten ways to prevent phishing.

The Anti-Phishing Working Group published a new report seeking to understand such trends by quantifying the scope of the global phishing problem, especially by examining domain name usage and phishing site uptimes. Phishing has always been attractive to criminals because it has low start-up costs and few barriers to entry. But by mid-2009, phishing was dominated by one player as never before—the ―Avalanche‖ phishing operation. This criminal entity is one of the most sophisticated and damaging on the Internet, and perfected a mass-production system for deploying phishing sites and ―crime ware – malware designed specifically to automate identity theft and facilitate unauthorized transactions from consumer bank accounts. Avalanche was responsible for two-thirds (66%) of all phishing attacks launched in the second half of 2009, and were responsible for the overall increase in phishing attacks recorded across the Internet.

Adapted from APWG

1. be suspicious of any email with urgent requests for personal financial information. Call the bank if they need anything from you.
2. Spot a Phish: Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
3. They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, date of birth, etc.
4. Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or you don't know the sender or user's handle
5. Avoid filling out forms in email messages that ask for personal financial information in emails
6. Consider installing a Web browser tool bar to help protect you from known fraudulent websites. These toolbars match where you are going with lists of known phisher Web sites and will alert you.
7. The newer version of Internet Explorer version 7 and 8 includes this tool bar as does Firefox version 2
8. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
9. If anything is suspicious or you don't recognize the transaction, contact your bank and all card issuers
10. Ensure that your browser is up to date and security patches applied.

5. CONCLUSION

Here we conclude with providing some preventive methods

5.1 User Education

Phishing exploits human vulnerabilities such that technical solutions can only block some of the phishing web sites. It doesn't matter how many firewalls, encryption software, certificates, or two factor authentication mechanisms an organization has if the person behind the keyboard falls for a Phishing attack. A study on effectiveness of several anti-phishing educational materials suggests that educational Materials reduced users' tendency to enter information into phishing webpages by 40%; however, some of the educational materials also slightly decreased participants' tendency to click on legitimate links. This leads to the belief that it is of paramount importance to and a new and efficient way of educating a large proportion of the population. The challenge lies in getting the user's attention to these security tips and advises.

There are few questions that arise: Should we implement all these protection mechanisms which complicate the user interface? Should we provide better user experience at the cost of reduced security or improve security at the cost of user inconvenience? Several recent surveys indicate that Lack of security is leading to loss of customer confidence in Internet commerce. That means users want appropriate security controls in place even if it means carrying a password token or getting their passwords on SMS. Today phishing is recognized by users as a real and potentially damaging threat. If appropriate anti-phishing controls are not put in place, chances are high that customers might switch to a more secure party to do business.

5.2 Anti-Phishing Groups

Phish Tank, launched in October 2006, is a collaborative clearing house for data and information about phishing on the Internet. Phish Tank employs a sophisticated voting system that requires the community to vote \phish" or \not phish", reducing the possibility of false positives and improving the overall breadth and coverage of the phishing data. It also provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge. Phish Tank is backed by OpenDNS, a public DNS resolver; OpenDNS utilizes Phish Tank data to prevent phishing attacks for their users.

Formed in 2003, the Anti-Phishing Working Group (APWG) is an international consortium that brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations, and communications companies. Fraud Watch International, a privately owned Internet security company established in 2003, provides a variety of anti-phishing products and services to protect financial service, e-commerce, and Internet hosting companies from phishing.

5.3 Legal Aspects

Currently little legislation related to phishing exists; this appears to be due to a lack of awareness at the governmental level. In order for technical and educational solutions to be successful, government support is required. The UK Fraud Act of 2005 covers fraud by false representation, however this does not specifically mention phishing; suggesting that

not only the end users but also the governments are unaware of the dangers of phishing. In 2005 a bill named The Anti-Phishing Act of 2005, a bill to criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing", was presented in United States Senate to combat phishing and pharming. The bill proposed a five-year prison sentence and/or fine for individuals who commit identity theft using falsified corporate websites or e-mails. Thus it allows law enforcement officials to fight phishing scams, by creating an opportunity to prosecute before the actual fraud takes place. The Anti-Phishing Act couldn't become a law at federal level, but there are a few states including California, New Mexico, Arizona, and Texas which have strict anti-phishing laws in place. Besides this there is still much work to be done on international basis. Most phishing scams operate overseas and it is exceedingly difficult and time consuming to prosecute an individual residing in a foreign country.

REFERENCES

[1] Identity thieves take advantage of voip. http://www.icbtollfree.com/article_free.cfm? Article ID=5926.

[2] Internet explorer 8 features - safer: domain highlighting. http://windows.microsoft.com/En-US/internet-explorer/products/ie-8/feat%ures/safer?tab=ie8dom.

[3] Opendns' phishtank.com and anti-phishing working group to share data. http://www.opendns.com/about/announcements/19/.

[4] Phishing - word spy. http://www.wordspy.com/words/phishing.asp.

[5] Phishing- consumer laws. http://consumerprotection.uslegal.com/phishing/.

[6] Proposed law aims to _ght phishing. http://www.pcworld.com/article/119912/proposed_law_aims_to_fight_phishi%ng.html.

[7] Public dns security bene_ts. https://developers.google.com/speed/public dns/docs/security.

[8] squid: Optimising web delivery. http://www.squid-cache.org/.

[9] Taking legal action against phishers. http://www.sis.pitt.edu/~nophish/expert/legal.html.

[10] Heather Adkins. An update on attempted man-in-the-middle attacked.http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-ma%n-in-middle.html, Aug 2011.

[11] Gundeep Singh Bindra. Masquerading as a trustworthy entity through portable document_le (pdf) format. In Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third International Conference on and 2011 IEEE Third International Confernece on Social Computing (SocialCom), pages 784 {789, Oct 2011.

[12] Rachna Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In Proceedings of the 2005 symposium on Usable privacy and security, SOUPS '05, pages 77{88,New York, NY, USA, 2005. ACM.

[13] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems, CHI '06, pages 581{590, NewYork, NY, USA, 2006. ACM.

[14] D. Eastlake 3rd. Domain Name System Security Extensions. RFC 2535 (Proposed Standard), March 1999. Obsoleted by RFCs 4033, 4034, 4035, updated by RFCs 2931, 3007, 3008, 3090, 3226, 3445, 3597, 3655, 3658, 3755, 3757, 3845.

[15] Owen Fletcher and Robert McMillan. Baidu: Registrar `incredibly' changed our email for hacker. http://www.computerworld.com/s/article/9162118/Baidu_Registrar_incredib%ly_changed_our_e_mail_for_hacker, 2010.

[16] Anti-Phishing Working Group. Origins of the word \phishing". http://www.antiphishing.org/word_phish.html.

[17] T. Hansen, D. Crocker, and P. Hallam-Baker. DomainKeys Identi_ed Mail (DKIM) Service Overview. RFC 5585 (Informational), July 2009.

[18] Jason Hong. Why have there been so many security breaches recently? http://cacm.acm.org/blogs/blog-cacm/107800-why-have-there-been-so-many-%security-breaches-recently/fulltext.

[19] Markus Jakobsson and Steven Myers. Phishing and countermeasures: understanding the in-creasing problem of electronic identity theft. John Wiley & Sons, Inc., 2007.

[20] Lance James. Phishing Exposed. Rockland, MA : Syngress, 2005.