Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Phishing Technology

Ankit Thakur[*], Deepti Singh, Vikas Chaudhary
M.tech (CSE) & Bhagwant University
Ajmer, Rajasthan, India

Abstract— ***Phishing (Password +Fishing) is a form of cyber crime based on social engineering and site spoofing techniques. The name of 'Phishing' is a conscious misspelling of word 'Fishing' and involves stealing confidential data from a user's computer. In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trust worthy entity in an electronic attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trust worthy entity in an electronic communication. Phishing is a fraudulent e-mail that attempts to get you to divulge personal data that can then be used for illegitimate purposes. There are many variations on this scheme. It is possible to Phish for other information in additions to usernames and passwords such as credit card numbers, bank account numbers, social security numbers and mothers' maiden names. Phishing presents direct risks through the use of stolen credentials and indirect risk to institutions that conduct business on line through erosion of customer confidence. The damage caused by phishing ranges from denial of access to e-mail to substantial financial loss.***

Keywords— Phishing, Social Engineering, Fraudulent Website, Anti-phishing

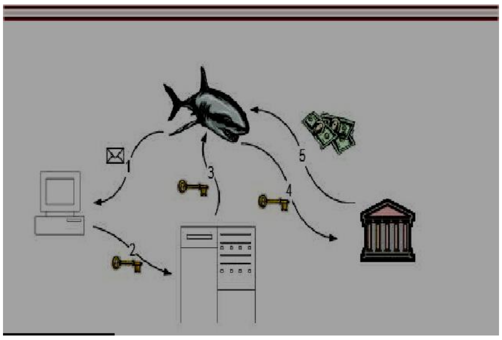
I. INTRODUCTION

The first phishing term was record at 1996 which was hunting for free AOL account, phishing is having a increasing tendency over the years. It then evolutes to financial fraud quickly, as the criminals are always aim for high yield. Luckily, with the pursuit of online banking, the banking industry is always motivated to play a leading role in fighting phishing threat. However, the reported loss to Internet Crime such as phishing has broken its record each year, which was up to US$239 Million lost in 2007. It is telling us that we are still looking for a better solution.

To confirm a destination it claim to be, the most trust worthy technique is the use of Digital Certificate, which the certification binding its public key together with an identity. The banking industry started to implement Digital Certificates in 2002; however, this trustful solution is always ignored by user. An incident of HSBC on 4th March 2008, that one of the world biggest bank has forgotten to renew its Digital Certificate, but it claimed its online banking for their customers still not affected. As we can imagine how many users ignored the warning of invalid Digital Certificate and had their online banking as usual in that day. Notice that the Digital Certificates solution is a one-way authentication of the bank; customers are rarely have their own Digital Certificates. Obviously, the identity of customer is still threatened by identity theft (e.g. Key logger on infected machine) as since the old age. In 2005, One-Time-Password (OTP) based Two-factor authentication solution - Secure Token was delivered to bank customer to fight against key logger and phishing. As the worldwide encouragement of Two-factor authentication in the same year, the phishing technique is also evolving, Secure Token was found vulnerable to Real-Time Man-In-The-Middle (RT-MITM) Attack in 2005. For the fall of Secure Token by RT-MITM, we will describe it in the later section.

Beside of authenticate the user, there is also needed to authenticate the bank. Bank of America (BoA) tried to take a leading role in fighting phishing. In 2005, BoA firstly role out Site Key to address the issue, which was originally invented by RSA lab. However, the Site Key was doubted it can achieve its target, since it obviously risks suffer from MITM attack.

Recently, the idea of Human Interactive Proof (HIP) is used to fight against phishing. There is an CAPTCHA application used in online Banking, however, the application may not achieves its initial goal when facing the rising threat of phishing techniques such as RT-MITM.



This figure 1, shows the simplified flow of information in a Phishing attack
1. A deceptive message is sent from the Phishes to the user.
2. A user provides confidential information to a Phishing server (normally after some interaction with the server).
3. The Phishes obtains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The Phishes obtains illicit monetary gain. Steps 3 and 5 are of interest primarily to law enforcement personnel to identify and prosecute Phishes. The discussion of technology counter measures will center on ways to disrupt steps 1, 2 and 4, as well as related technologies outside the information flow proper.

II. TYPES OF PHISHING

Phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even multiplayer games. Below are some major categories of phishing.

2.1. Clone phishing

In this type phisher creates a cloned email. He does this by getting information such as content and recipient addresses from a legitimate email which was delivered previously, then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy.

2.2. Spear phishing

Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization. Spear phishing is also being used against high-level targets, in a type of attack called “whaling”. For example, in 2008, several CEOs in the U.S. were sent a fake subpoena along with an attachment that would install malware when viewed. Victims of spear phishing attacks in late 2010 and early 2011 include the Australian Prime Minister’s office, the Canadian government, the Epsilon mailing list service, HBGary Federal, and Oak Ridge National Laboratory.

2.3. Phone phishing

This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source.

III. PHISHING TECHNIQUES

Phishers use a wide variety of techniques, with one common thread.

3.1. Link Manipulation

Most methods of Phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by Phishers. In the following example, http://www.yourbank.example.com/, it appears as though the URL will take you to the *example* section of the *yourbank* website; actually this URL points to the " *yourbank* " (i.e. Phishing) section of the *example* website.

An old method of spoofing used links containing the ' @ ' symbol, originally intended as a way to include a username and password. For example, http://www.google.com@members. tripod.com/ might deceive a casual observer into believing that it will open a page on www.google.com, whereas it actually directs the browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied.

3.2. 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.

3.3. 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.

3.4. Phone Phishing

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 Phishers) was dialed, prompts told users to enter their account numbers and PIN. Wishing (voice Phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization

3.5. Phishing Damage:

The damage caused by phishing threat varies from loss of access to email to existing substantial financial loss. This way of identity threat has become more common due to the ease by which unsuspecting people or hackers often divulge personal information to phishes that include social security numbers, credit card numbers, and mother's maiden names.

IV. CONCLUSION

Phishing threat to network security is getting much worse before they get better. Hence it is very important to recognize yourself with these threats and frauds. It is very necessary to educate yourself with this threat by researching this topic on web. It is important to learn to how to familiarize phishing emails. These frauds can be prevented with your anti-virus software, spam blockers, and internet browser. However, one must keep this software updated in order to identify virus and lists of fraud websites. This update is done by "help" menu of the program by clicking "check for updates" and it is also concluded that one needs to be cautious. If any email seems suspicious then do not click on it, simply delete it.

REFERENCES

[1] Aryan Chandrapal Singh: Phishing: A Computer Security Threat. Volume 1, Issue 7, December 2013 International Journal of Advance Research in Computer Science and Management Studies.

[2] "Internet Banking Targeted Phishing Attack".Metropolitan Police Service. 2005-06-03. Archived from the original on 2010-02-18. Retrieved 2009-03-22.

[3] Mutton, Paul. "Fraudsters seek to make phishing sites undetectable by content filters". Netcraft. Archived from the original on 2011-01-31. Retrieved July 10.

[4] Huajun Huang Junshan Tan Lingxi Liu "Countermeasure Techniques for Deceptive Phishing Attack" International Conference on New Trends in nformation and Service Science. NISS '09. June-2009.