Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 85 (2015) 34648-34651

ISSN: 2229-712X

A comprehensive study of latest phishing techniques and prevention

Prateek Lohiya

SITE, VIT University, Vellore, TamilNadu, India-632014.

ARTICLE INFO

Article history:
Received: 3 May 2012;
Received in revised form:
22 August 2015;
Accepted: 29 August 2015;

Keywords
Comprehensive,
Prevention,
Phishing.

ABSTRACT

Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher controlled proxies used to monitor and intercept consumers' keystrokes). Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy etc. Some of the criminals behind phishing scams have even gone so far as to create websites that appear to be operated by government agencies. According to latest phishing reports submitted to APWG of 26,402 in March 2011 was down 35 percent from the all-time high of 40,621 in August, 2009.[1]Though many agencies, personnel's working for combatting this problem new techniques have been developed to outsmart them. This paper aims to discuss latest phishing techniques, motivation, causes of vulnerability of systems in detail. This analysis aims to help users & organization to avoid being victims and to take primary preventive measures.

1. Introduction

The term *phishing* comes from the fact that cyber-attackers are fishing for data; the *ph* is derived from the sophisticated techniques they employ, to distinguish their activities from the more simplistic *fishing*. Phishing, also known as *carding* or *brand spoofing* and is constantly evolving. Phishing has actually been around for over 10 years, starting with America Online (AOL) back in 1995.[2]There were programs (like AO Hell) that automated the process of phishing for accounts and credit card information. The phishers would imitate an AOL administrator and tell the victim that there was a billing problem and they needed them to renew their credit card and login information.

According to the report generated by antiphishing.org unique phishing websites detected reached a high for the 1st half of 2011 in March with 38,173, down more than 32 percent from the record of 56,362 in August 2009.[1]While most phishing attacks target the financial industry, more and more phishing incidents targeting other sectors such as retailers, online game operators and large ISPs have also been discovered. As phishers have advanced their local language capabilities and the level of sophistication of attacks, phishing attacks have expanded geographically to various European and Asian countries. The number of phished brands reached a high in the half of 339 in January, down 5 percent from the all-time high of 356 reached in October, 2009.[1]

There are several measures being taken to prevent phishing. For example, Anti-Phishing Working Group is an industry group, which creates phishing reports and makes it available to its paying members. Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. But there is no single solution to fight phishing. More and more phishing websites are coming up every day making it increasingly difficult to track and block them as attackers are coming up with innovative methods every day to lure unsuspecting users into divulging their personal information.

In this paper we perform an analysis of the phishing vulnerabilities and the ways in which it affects users and organizations. We also perform a detailed research of the most commonly used methods of phishing and review possible anti-phishing approaches. By performing extensive analysis of phishing websites and methods used for phishing, listing the possible causes of phishing which can be further used for developing solutions.

The rest of the paper is organized as follows: In section II analysis of phishing vulnerable areas are discussed. Section III discusses the reasons for phishing while section IV analyze the latest methods being used in performing phishing attacks. Section V explores some of the best attempts made in preventing phishing and section VI concludes this paper.

2. Analyzing Phishing Vulnerable Areas

Since Phishing extensively makes use of social injection techniques to manipulate users to give out their personal details via online shopping, e-banking and online retailing which are more and more prevalent these days.

Today exchange of money and financial transactions over the internet have become a part of life. This has also led to an increase in phishing attacks.

Tele:
E-mail addresses: plohiya18@gmail.com

There is rapid evolution of sophisticated and innovative methods used for phishing and hence increasing the susceptibility of users to becoming victims of phishing attacks.

Typically phishing attacks will redirect the intended victim to a website designed to imitate a target organization's website and will harvest the user's personal information. Usually the victim is unaware of the attack until there is some financial loss occurring or in some cases, the users identity stolen and used for criminal purposes.

Phishing attempts mainly target customers of banks and online payment services. Recent studies have stated that the top five industries vulnerable to cybercrime include travel, education, financial services, government services and IT services.[3] Mobile users are the most vulnerable to phishing attacks,a study of log files of web servers hosting phishing websites has revealed. Mobile users are the first to arrive and they are three times more likely to submit their login details than desktop users, the study by security firm Trusteer found. Mobile users are always-on and are most likely to read e-mail messages as soon as they arrive, but desktop users read messages only when they have access to their computer, said Mickey Boodaei, chief executive officer at Trusteer.[4]

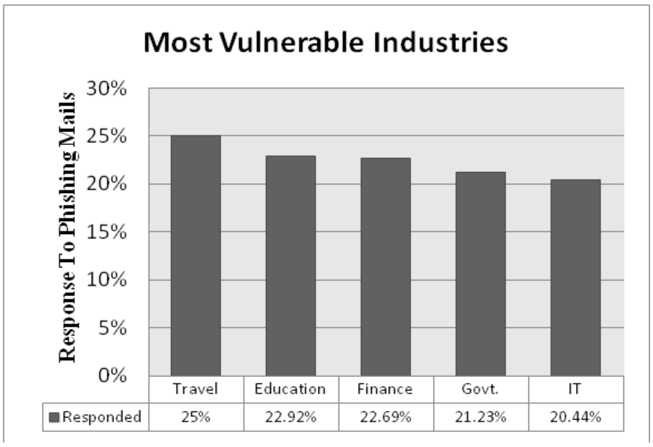

Figure 1: Data Source: Internet

3. Reasons For Phishing

Counter-measures for phishing would be ineffective unless we analyze, what motivates the phisher? Although financial gains is one of the major and obvious reasons, some of the facts of phishing motivation are discussed below.

3.1 Financial Gains

This factor continues to dominate over all the factors that motivates the phisher. Trends shows that victim primarily goes through financial losses. As soon as phisher gets victims personal information such as credit card card number etc. they start making easy money.

3.2 Identity Theft

This factor focuses on identity based crime such as indulging into criminal activities, frauds via victim's identity. Also the acquired identity is sometimes sold-out to a third party to exploit the victim and others.

3.3 Indusrial Reconnaissance

In today's scenario of increased industrial rivalry highly sophisticated attacks are organized in order to tarnish the image of brands, organization, to achieve this organizations hire attackers to spy on victim and get the required information.[6]

3.4 Fame & Attention

Some of the phishers are fame and attention seekers. These type of persons not necessarily cause financial or identity theft to victim. They just like to explore the secruty loopholes and have fun online.

4. Phishing Techniques

There is a great philosophy "Know your enemy before engaging yourself into defense". One major problem that we face today, due sudden and overwhelming amount of phishing that has occurred, is the lack of detailed understanding of phishers and the tools they use. In this section we will first analyze the most popular methods phishers employ:

4.1 Impersonation Attack

It is the most popular and most simple method of deceit. It consist of a completely constructed fake site that the contains images from real Web site and might even be linked to the real one.

There are a couple of quick ways to perform a mirror, a Web mirroring tool distributed with most Linux and BSD platforms called wget (www.gnu.org/software/wget/wget.html), which is, once again, simple to use and effective.[2] Web crawler that looks at a site, recursively searches for hyperlinks within a page, and attempts to download them.

Example: Mirroring bank.securescience.net/bank/index.html

```
lancej@lab:~>
wget –m bank.securescience.net/bank
--22:50:38-- http://bank.securescience.net/bank
=> 'bank.securescience.net/bank'
Resolving bank.securescience.net... 65.102.104.137
Connecting to bank.securescience.net|65.102.104.137|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://bank.securescience.net/bank/ [following]
--22:50:43-- http://bank.securescience.net/bank/
=> 'bank.securescience.net/bank/index.html'
Connecting to bank.securescience.net|65.102.104.137|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,715 [text/html]
100%[====================================>]
2,715 9.24K/s
22:50:44 (9.23 KB/s) - 'bank.securescience.net/bank/index.html' saved
[2,715/2,7
15]
Loading robots.txt; please ignore errors.
--22:50:44-- http://bank.securescience.net/robots.txt
=> 'bank.securescience.net/robots.txt'
Reusing existing connection to bank.securescience.net:80.
HTTP request sent, awaiting response... 200 OK
Length: 1,981 [text/plain]
100%[====================================>]
1,981 --.--K/s
22:50:44 (201.10 KB/s) - 'bank.securescience.net/robots.txt' saved
[1,981/1,981]

FINISHED --22:50:44--
Downloaded: 4,696 bytes in 2 files
```

To mirror the internal pages, we log in with our assumed account and perform a File | Save
Page As , and then we will have a copy of that particular Web site. Now using the source codes of the legitimate website

phishers host the fake ones on their proxy server and direct the transmission between victim and the legitimate website to theirs using: ARP spoofing, DNS spoofing, URL and HTML attack vectors, trojan key loggers.

4.2 The Forwarding Attack

Forwarding is seen more with Amazon, eBay, and PayPal and is an e-mail, one typically receive that has all the usual real Web site graphics and logins within it. When a victim logs in via a Forwarding e-mail link, the user's data is sent to the hostile server, then the user is forwarded to the real site, and in many cases, the system logs you into the real site via a man-in-the-middle (MITM) technique.[2]

This Forwarding attack continuity is flawless, and victims usually never know that they were phished.The weakness with this approach is that it relies on the spam itself to get through without being filtered. Due to the amount of HTML within such an e-mail, many corporate antivirus and antispam filters will block it because the Bayesian points rise with more encapsulated HTML.

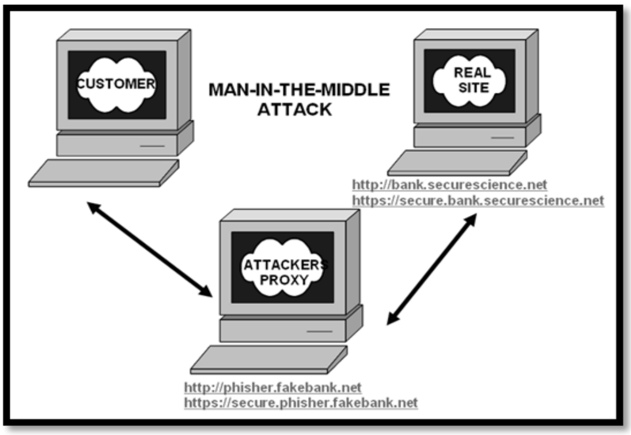
CUSTOMER
MAN-IN-THE-MIDDLE ATTACK
REAL SITE
http://bank.securescience.net
https://secure.bank.securescience.net
ATTACKERS PROXY
http://phisher.fakebank.net
https://secure.phisher.fakebank.net

Figure 2: Representation of MITMA

4.3 The POPUP Technique

It is a very creative but limited approach. The popup technique was first discovered during the barrage of phishing attacks on Citibank in September 2003.This was essentially a link that you clicked within your e-mail, and it posted a hostile popup. But behind the popup was the actual target that the attackers were trying to steal data from. This is quite a slick, creative ploy that is actually one of the most authentic looking of the three basic phishing methods.[2] However, popup attacks are very ineffective today, since most browsers now have popup blockers installed by default.

4.4 Tabnabbing

This attack preys on browser tabs and the fact that users generally don't keep track of all the tabs they have open at one time. This allows the attacker to surreptitiously change the contents of a separately tabbed page, in addition to the name and logo on that tab. When a user eventually returns to the tab, they see the spoofed page for a site, for example, Gmail or Facebook. This tacic relies on the "perceived immutability of tabs." An attacker could make the phishing ruse even more cunning by creating a targeted attack that takes advantage of a user's web browsing history file. In addition, instead of simply displaying a login screen on the spoofed page, an attacker could display a message that the user's session has timed out, thereby adding legitimacy to the attack.

4.5 Using BOTNET

A botnet is a network of compromised computers that can be remotely controlled by an attacker. Due to their immense size (tens of thousands of systems can be linked together), botnets can pose a severe threat to the community when used for Denial-of-Service (DoS) attacks. Initial research in this area demonstrated that botnets are sometimes used to send out spam emails and can also be used for phishing attacks. During a study in October 2004, email security company CipherTrust suggested that 70% of monitored phishing spam was sent through one of five active botnets, but our own observations suggest that many more botnets are in use for spam operations. Although not the analysis of one single incident, in this section we present our observations on the tools and techniques used by attackers engaged in phishing via botnets.[5]

5. Phishing Prevention Techniques

Phishing preventive measures are contantly evolving as there are numerous new methods being employed by phishers. But some of the measures proven to be effective are discussed in this section. These protection measures can be employed in various situations.some of them are:

5.1 Desktop Level Prevention

Many desktop protection software providers now provide solutions that are capable of fulfilling one or more of these functions. Most of the solutions act as local anti-virus protection, personal firewall, personal anti-spam, spyware detection. The ability to detect Trojan horses, key-loggers, screen-grabbers and creating backdoors through email attachments, file downloads, dynamic HTML and scripted content, anomalies in network traffic profiles (both inbound and outbound) and initiate appropriate counter-measures. For instance, detecting that an inbound HTTP connection has been made and substantial outbound SSL traffic begins on a non-standard port, to block inbound connections to unassociated or restricted network ports and their services. These services can be installed on systems like normal packages or can be embedded-in browser toolbar. Some of the effective toolbars & software include mcafee site advisor, netcraft toolbar , Norton internet security.[7][8]

5.2 User Awareness

Customers may take a number of steps to avoid becoming a victim of a phishing attack that involve inspecting content that is presented to them and questioning its authenticity. Depending on knowledge level of user following methods can help in primarily avoid in being a phishing victim: Avoid e-mails links that directs to HTML page; There should be no hex-encoded printable ASCII characters in domain names; No HTTP link should contain "http" more than once; No nested <A> and <AREA> links. Make sure that web browser disables all window pop-up functionality, java runtime support, activeX support, disable all multimedia and auto-play/auto-execute extensions. Prevent the storage of non-secure cookies, ensure that any downloads cannot be automatically run from the browser, and must instead be downloaded into a directory for anti-virus inspection.[8]

5.3 Checking Similar Domain Names

It is important that organizations carefully monitor the registration of Internet domains relating to their organization. Companies should be continuously monitoring domain name registrars and the domain name system for domain names that infringe upon their trademarked names, and that could be used for launching spoofed websites to fool customers. There are two areas of concern: The expiry and renewal of existing corporate domains & The registration of similarly named domains.[8]For example, assuming the organization's name is "infidez solutions" and their normal website is www.infidezsolutions.com, the organization should keep a watchful eye out for Error! Hyperlink reference not valid.

5.4 Authenticating Mail Servers

Businesses and ISP's may take enterprise-level steps to secure against Phishing scams – thereby protecting both their customers and internal users. Multiple methods have been proposed to authenticating sending mail servers. In essence, the senders mail server is validated by the receiving mail server. If the senders IP address is not an authorized address for the email domain, the email is dropped by the receiving mail server. Alternatively, through the use of Secure SMTP, email transport could be conducted over an encrypted SSL/TLS link. When the sender mail server connects to the recipient mail server, certificates are exchanged before an encrypted link is established. Validation of the certificate can be used to uniquely identify a trusted sender. Missing, invalid or revoked certificates will prevent a secure connection from occurring and not allow delivery of emails.If desired, an additional check with the DNS server can be used to ensure that only authorised mail servers may send email over the secure SMTP connection.[8]

6. Conclusion

Phishing started off being part of popular hacking culture. It has caused a lot of distrust on websites and people, sometimes become skeptical of using websites for important transactions. To gain back the trust from users, we should be able to effectively fight out phishing. The problem of Phishing does not have a single solution as of now. Now, as more organizations provide greater online access for their customers, professional criminals are successfully using phishing techniques to steal personal finances and conduct identity theft at a global-level. By understanding the tools and technologies Phishers have in their arsenal, businesses and their customers can take a proactive stance in defending against future attacks. Organizations have within their grasp numerous techniques and processes that may be used to protect the trust and integrity of their customers personal data. The points raised within this paper, and the solutions proposed, represent key steps in securing online services from fraudulent phishing attacks – and also go a long way in protecting against many other popular hacking or criminal attack vectors.

References

[1]http://www.antiphishing.org/phishReportsArchive.html

[2]"Phishing Exposed" book by Lance James.

[3]http://infosecisland.com/blogview/13961-Research-Reveals-Widespread-Vulnerability-to-Phishing.html

[4]http://www.computerweekly.com/news/1280094721/Mobile-users-most-vulnerable-to-phishing-attacks-study-shows

[5]http://honeynet.org

[6]A Phishing Vulnerability Analysis of Web Based Systems-Weider D. Yu, Shruti Nargundkar, Nagapriya Tiruthani

[7] http://en.wikipedia.org/wiki/Anti- phishing_software

[8]Whitepapers-www.technicalinfo.net.htm