STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS

Dr.Radha Damodaram

*Associate Professor, School of Computer Science,CMS College of Science & Commerce,
Coimbatore, Tamili Nadu, India*

---***---

Abstract - The Internet has a remarkable platform for common people communication. Persons with criminal mind have found a way of stealing personal information without actually meeting them and with the least risk of being caught. It is called Phishing. Phishing poses a huge threat to the e-commerce industry. Not only does it shatter the confidence of customers towards e-commerce, but also causes electronic service providers tremendous economic loss. Hence it is essential to know about phishing. This paper gives awareness about phishing attacks and anti-phishing tools.

Key Words: *Phishing, phishing steps, phishing types, Anti-phishing tools.*

1. INTRODUCTION

Phishing is an act of attempting a victim for fraudulently acquires sensitive information by impersonating a trustworthy third party, which could be a person or a reputed business in an electronic communication. The objective of phishing attack is to trick recievers into divulging sensitive information such as bank account numbers, passwords and credit card details. For instance, a phisher may misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient [12].

Both academia and industrial practitioners have proposed various anti-phishing measures in order to safeguard the interests of customers, and online security policies. Some commercial anti-spam and anti-phishing products prohibit email from "blacklisted" sites that they claim send spam and phishing email, while allowing email claiming to be from "whitelisted" sites they claim are known not to send it. This approach tends to unfairly discriminate against smaller and less-known sites, and would seem to be anti-competitive. . Due to the obvious usability problems of security toolbars, it can affect the performance of these toolbars ultimately.

The usability evaluation is indispensable for the future. Now a days five typical anti-phishing toolbars are in use as built-in phishing prevention in the Internet Explorer 7.0, Google toolbar, Netcraft Anti-phishing toolbar and SpoofGuard. In addition, internet Explorer plug-in, Anti-phishing IEPlug. Indeed, according to the heuristic usability evaluation, a number of usability issues may found. [13].

2. STEPS IN PHISHING

A person who engaged in malware activities is called a *phisher*. Phishing attacks today typically employ generalized “lures”, intimidating users and creating fear – a common example is “we need you to confirm your account details or we must shut your account down”. An approach which is believed to become more and more common is context aware attack: this is a more complex approach as it not only uses threat or enticement, but makes the victim think of the messages as expected, and therefore legitimate.

The method used by phishers is usually to make fraudulent websites, similar to the genuine website by mimicking the HTML code containing the same images, text and sections. Some phishing websites register a similar domain name to the legitimate website of a company or a bank. The most common method used by phishers is by forms, for example, the Internet Banking login page or a form for password verification. Many phishing attempts use domain spoofing or homographic attacks (Gabrilovich & Gontmakher) as a step towards persuading victims to give out personal information.

A *phisher* could target many kinds of confidential information, including user names and passwords, credit card numbers, bank account numbers, and other personal information. In a study by Gartner (Gartner Inc, 2004), about 19% of all those surveyed reported having clicked on a link in a phishing email, and 3% admitted to giving up financial or personal information [11].

A common phishing attack is (*for a phisher*) to obtain a victim's authentication information corresponding to one website (that is corrupted by the attacker) and then use this at another site. This is a meaningful attack given that many computer users reuse passwords – whether in verbatim or with only slight modifications. The phishing attack lifecycle can be decomposed in :

- Planning,
- Setup,
- Attack,
- Collection,

- Fraud and
- Post-Attack Actions.

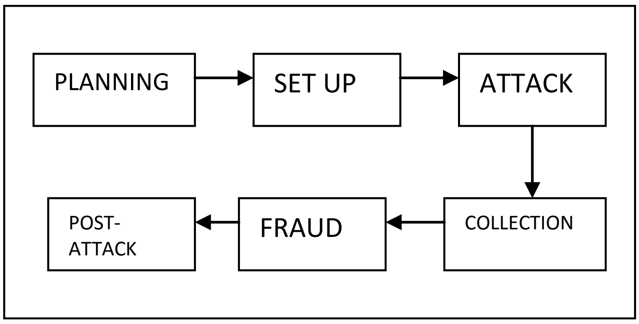

Figure. 2.1 Steps in phishing

The phisher plans the attack, creates the attack code/message and sends to the target user. A malicious message arrives at the target site. The ignorant target reads the message and takes some action which makes him or her vulnerable to an information compromise. The user is then prompted for confidential information through a familiar and trustworthy looking web interface. The user reveals his confidential information. The confidential information is transmitted from a phishing server to the phisher. The phisher engages in fraud using confidential information to impersonate the user[4].

There is no single way that can prevent all phishing. But different methods applied at different stages of phishing attack can abort a phishing attempt and properly applied technology can significantly reduce the risk of identity theft. (Emigh, 2005).

3. TYPES OF PHISHING ATTACS

Phishers send legitimate looking emails from government agencies and other financial institutions with a motive to obtain personal information or unknowingly install a malware on their computer. The categories of phishing shown in figure 3.1.

There are different types of phishing attacks prevalent at present. Analyzing is categorized into 3 different kinds

1. Deceptive phishing

2. Crime ware based phishing

3. Other types as DNS based phishing (content injection phishing)

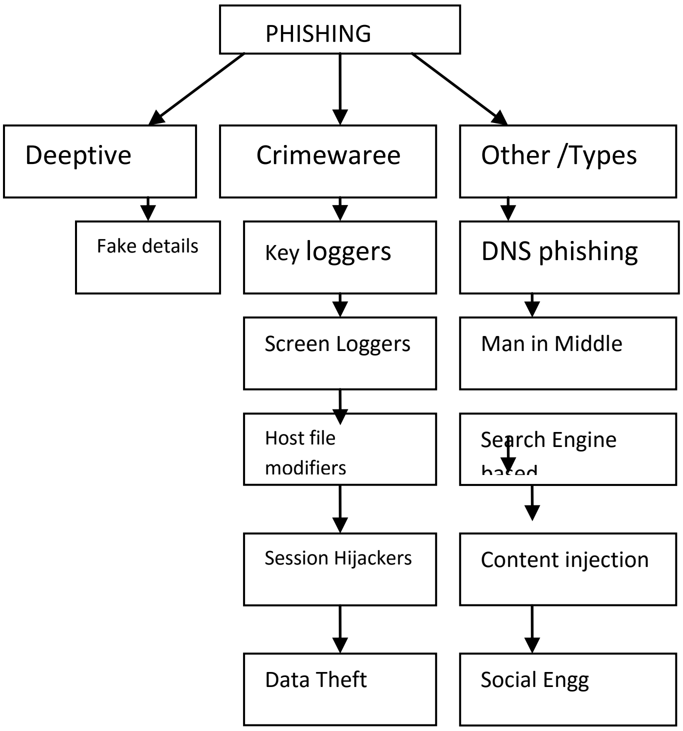

Figure. 3.1 Types of phishing

1. **Deeptive phishing** involves the sending of email message using make believe logos of reputable financial institutions and other organizations, which the users are prompted to click. Users may be foolded by the syntax of the domain name in these types of attacks.

Eg. www.paypai.com uses a lowercase "i" which looks similar to the letter I for the letter "I" and www.paypal.com substitutes the no 1 for the letter i.

2. **Malware based phishing** is a widely prevalent collection of phishing techniques which include key loggers and screen loggers hosts file poisoning web Trojan, system reconfiguration attacks and spear phishig, session hijacking data theft malware based techniques tend to install and run malcicious software on the users machine [3].

3. Other Types:

- **DNS based phishing** relies on hosts file modification. Using this type of phishing, phishers change the hosts files or domain name system in such a way that requests for URLs or name service returns a bogus address and subsequent communications are unaware that the website where they are entering confidential information to the phisher.

- In **man –in – middle phishing** the phisher positions himself between the user and a genuine website and captures the information and sells or uses it later.

- **Fake Websites**

APWG member PandaLabs tracks the number of malware variants detected, which has been growing each quarter. During the 4th quarter of 2014 this figure broke a new record, with 23,500,000 mal ware samples detected, an average of 255,000 new threats each day [1]. Never in the history of computer security ha s the amount of new malware created been so high. In fact, the vast majority are just variants of existing malware modified by their creators to evade signature based detection systems, while the functionality is the same [2]. Still, the escalating numbers illustrate the adaptability of the code and the creativity of the malware authors. The following figure shows the increase of fake websites during the year.

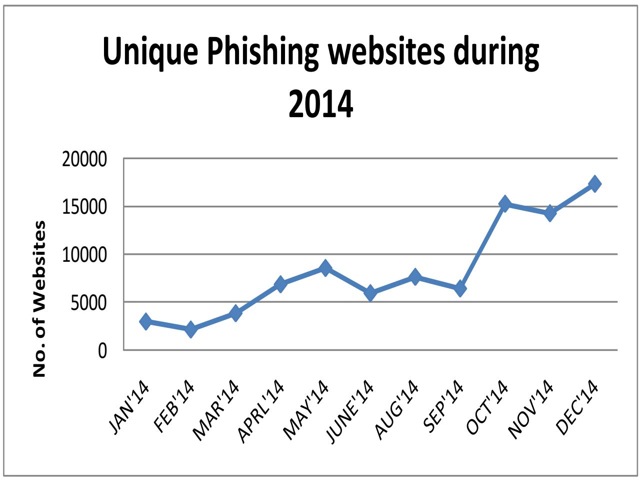

Figure. 3.2 Increase of fake websites during the year 2014

- **Phishing email**

It will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has

Phishing e-mails will contain some of these common elements:

1. The "From Field" appears to be from the legitimate company mentioned in the e-mail. It is important to note, however, that it is very simple to change the "from" information for any e-mail client.

2. The e-mail will usually contain logos or images that have been taken from the Web site of the company mentioned in the scam e-mail.

3. The e-mail will contain a link or hyperlink to a website with a similar URL name as the “real” sender. *Note that the hyperlink does NOT point to the legitimate Citibank Web site URL[5].*

- **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. More fraudsters are adopting new approaches in an effort to make phishing sites undetectable by common security measures such as firewalls and content filtering web proxies.

- **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.

4. ANALYSIS ABOUT PROBLEMS

Security Loop Holes

3 main areas

1. Non uniformity of internet standard,
2. security loopholes in mail transferring mechanism and
3. security loopholes in users system.

General phishing solutions

-Primarily the solutions are

1. technological remedies
2. policy changes’
3. awareness and training programs

-Technological

1. stripping URL that contains IP address
2. blocking Internal Address that Originates outside the perimeter
3. monitoring bounced email messages

Potential policy changes

1. Registering any obvious and available deeptive domain names

2. Establishing standards of the styles and distribution of mass email.
3. Using personalized messages

Awareness and training programs

1. Making use of regular communications to explain the phishing problem
2.
3. Establishing a simple mechanism for reporting phising attacks
4. Posting alerts on security website

4. ANTI-PHISHING TOOLS

4.1 Mail-SeCure

Mail Secure's Anti-Phishing module combines several layers and technologies to detect and block. Phishing attempts. The main technologies used are:

□ **Anti-Phishing Database -** Mail-Secure maintains a data base which is updates on a daily basis. This database features millions of known Phishing URLs and domain names. If one of the listed URLs appears in a mail, it is blocked [5].

□ **SURBL -** an RBL which is designed to block or tag Phishing attempts based on URI's (usually their domain names) scattered in the body of the message. In this case, the RBL is not intended to block the source of the spam message. Instead, SURBL is used to block spam based on its message content.

Even if a spammer uses new domains, they may point to the old, blocked IPs and will therefore be blocked, right from the first spam message received.

□ **Commtouch RPD™ -** Commtouch's Recurrent Pattern Detection (RPD™) is based on the fundamental characteristic of Phishing, spam and email-born Malware - its mass distribution over the Internet. Sniffers located worldwide, lookout for real traffic in over 60 million operational mailboxes. They then extract patterns to detect recurring patterns and examine the number of sources to determine if they are Trojan-based outbreaks. Commtouch RPD™ differentiates between bulk mail (which can be a mailing list), and confirmed spam [6].

Commtouch RPD™ advantages:

- Generates patterns from more than 300 million daily messages, from over 15 locations worldwide.

- Real-time – blocks spam from the first minute of the outbreak.

- Near-zero false positives – as the pattern of legitimate mail sent from one to another will probably appear only once.

- Content-agnostic – effective against Phishing, fraud and innocent-looking spam.

- Language independent.

- Detects spam of any file type.

- Adaptive technology – As spam is economically motivated, spammers constantly change tactics to achieve mass distribution.

□ **Heuristic Fraud detection sets of rules -** Mail-Secure uses Heuristic rules in order to detect possible new Phishing attempts. Mail-SeCure has over 2,500 sets of rules to detect characteristics of Phishing. The heuristic engine uses a score-based system to identify Phishing.

□ Zombie detection - Most Phishers use zombie computers to distribute their mail. Zombie

computers are computers that were involuntarily hacked (whether by Trojan horses or by direct hacking) and used for mail distribution.

Mail-SeCure has a unique Zombie Detection System – ZDS. It identifies zombies and automatically blocks them at the session level (similar to RBL). PineApp has a central ZDS,

RBL-like server, which dynamically blocks identified IPs. Since a zombie computer owner can change his IP, ZDS automatically adds or removes IP addresses from blacklists.

□ **IP Reputation -** a powerful additional layer used to block Zombies at the SMTP session level. The IP Reputation mechanism is based on sniffers located at various points of the world, monitoring traffic of hundreds of millions of email messages daily. IP Reputation centerdynamically classifies IPs, according to a profile built from parameters such as: volume, percentage of spam & viruses and elevations. When an SMTP session is established, Mail-SeCure queries the IP Reputation system (or uses local cache) and performs various actions according to the IP classification, such as: permanently reject the mail, respond with a temporary error to be able to re-evaluate the IP on the retry time, activate grey-listing, activate Rate limit, etc.

□ **Rate limit -** provides an advanced layer against mail bombing, by limiting the amount of messages or SMTP sessions allowed from a certain IP on a pre-defined time. Rate limit uses a complex algorithm using a sliding-window method. Limitations can be defined for timeframes of: minutes, hours and days.IP Reputation saves bandwidth and lowers the load on your Mail-SeCure system [7].

4.2 Security Tool Bar - Netcraft

An Internet services company based in Bath, England's product is Netcraft. It provides web server and web hosting market-share analysis, including web server and operating system detection., The service is able to monitor uptimes uptime performance monitoring is a commonly used factor in determining the reliability of a web hosting provider depending on the queried server's operating system. Netcraft also provides security testing, and publishes news releases about the state of various networks that make up the Internet.

The company is also known for its free anti-phishing toolbar for the Firefox and Internet Explorer browsers. Starting with version 9.5, the built-in anti-phishing filter in the Opera browser uses the same data as Netcraft's toolbar, eliminating the need for a separately installed toolbar. A study commissioned by Microsoft concluded that Netcraft's toolbar was among the most effective tools to combat phishing on the Internet, although this has since been superseded by Microsoft's own Internet Explorer 7 with Microsoft Phishing Filter, possibly as a result of licensing Netcraft's data [8].

4.3 ESET SECURITY

ESET Smart Security incorporates anti-spam and a bidirectional firewall along with traditional anti-malware features of ESET NOD32 Antivirus. The acronym NOD stands for ***N****emocnica na* ***O****kraji* ***D****isku* ("Hospital at the end of the disk"),[1] a pun related to the Czechoslovak medical drama series *Nemocnice na kraji města* (*Hospital at the End of the City*).[2] The first version of NOD32 - called NOD-ICE - was a DOS-based program. It was created in 1987 by Miroslav Trnka and Peter Paško at the time when computer viruses started to become increasingly prevalent on PCs running DOS [9].

ESET SysInspector is a diagnostic tool which allows in-depth analysis of various aspects of the operating system, including running processes, registry content, startup items and network connections. Anti-Stealth Technology is used to discover hidden objects (rootkits) in the Master Boot Record, boot sector, registry entries, drivers, services and processes. SysInspector Logs are standard XML files and can be submitted to IT experts for further analysis. Two logs can be compared to find a set of items not common to both logs. A log file can be saved as a service script for removing malicious objects from a computer [10].

ESET SysRescue Live is a Linux-based bootable Live CD/USB image that can be used to boot and clean heavily-infected computers independent of the installed operating system. The program is offered free of charge, and can download updates if a network connection is present.

4.4 Browser Integrated Tools

A browser-integrated tool usually relies on a blacklist, which contains the URLs of malicious sites, to determine whether a URL corresponds to a phishing page or not. In Microsoft Internet Explorer 7, for example, the address bar turns red when a malicious page is loaded. The effectiveness of a blacklist is strongly influenced by its coverage, credibility, and update frequency. At present, the most well-known blacklists are those maintained by Google and Microsoft, which are used by the most popular browsers, Mozilla Firefox and Microsoft Internet Explorer, respectively.

4.5 Using Antiphish And Dom Antiphish Techniques

AntiPhish is a browser plug-in that keeps track of sensitive information. Whenever a user attempts to enter sensitive information on one site, and this information has previously been associated with a different, trusted site, a warning is generated. This is effective when a user inadvertently enters bank login information on a phishing site. However, AntiPhish suffers from the problem that legitimate reuse of credentials is also flagged as suspicious.

To address this usability problem, DOM AntiPhish was proposed. For that approach, the authors compared the Document Object Models (DOMs) of the pages under analysis to determine whether the two pages are similar. When information is reused on a page that is similar to the original page (that is associated with the sensitive data), a phishing attempt is suspected. When the information is entered on a site that is completely different, the system assumes legitimate data reuse. Although DOM AntiPhish is able to identify phishing pages effectively, its major limitation is that the DOM tree is not necessarily a reliable feature to establish similarity between pages. In some cases, it is possible for the attacker to use different DOM elements to create a similar look-and-feel and appearance of a page. Furthermore, a phishing site that only consists of images cannot be detected. A new technique to detect phishes has been implemented in the project, which removes the above said disadvantages.

Conclusion

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Now days it has become very serious. There are many techniques to solve these problems. But people may don't aware of the seriousness of phishing. Periodical updating of anti-phishing tools or softwares in their own systems may helpful to secure their confidential information and credentials. This study may give the awareness about the phishing problems and solutions.

References

1. Anti-Phishing Working Group, Phishing Activity Trends Report (May 2014). [www.antiphishing.org/reports/apw]

2. Anti-Phishing Working Group. Phishing Activity Trends Report (November, 2014).

3. AVIRA antivirus report. [www.avira.com/en/threats/section ...] .

4. Camp LJ, Goodman S, House CH, Jack WB, Ramer R and Stella M. Chapter 6: Offshoring: Risks and Exposures [www.acm.org/globalizationreport/ ...] .

5. CERT-In Annual Report (2014). [cert-in.org.in/knowledgebase/ann ...]

6. Emigh, A (2014). Online identity theft: Phishing technology, chokepoints and countermeasures. ITTC Report on Online Identity Theft Technology and Countermeaures; http://www.anti-phishing.org/Phishing-dhs-report.pdf.

7. Gabrilovich E and Gontmakher A. (2014). "The Homograph Attack," Communications of the ACM, 45(2):128.

8. Gartner Inc. (2014). Gartner study finds significant increase in e-mail phishing attacks. [www.gartner.com/5 about/press re] .

9. ESET NOD32 - Wikipedia, the free encyclopedia *[https://en.wikipedia.org/wiki/ESET_NOD32]*

10. ESET SysInspector - Wikipedia, the free encyclopedia *[https://en.wikipedia.org/wiki/ESET_NOD32]*

11. Kirk J. (2011). Phishing Tool Constructs New Sites in Two Seconds. [www.pcworld.in/news/index.jsp/ar .]

12. Computer Economics (2007), Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other malicious code, reference available at: http://www.computereconomics.com/page.cfm?name=Malware%20Report

13. Congressional Budget Office Cost Summary, H.R. 1525 Internet Spyware (I-SPY) Prevention Act of 2007,available at:http://www.cbo.gov/ftpdocs/80xx/doc8076/hr1525.pdf.