International Journal of Information Technology and Management

Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

A REVIEW ABOUT EXPLORING EMERGING ANTI PHISHING APPROACHES

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

A Review about Exploring Emerging Anti Phishing Approaches

Ashish Gupta

Research Scholar, Sai Nath University, Ranchi, Jharkhand

Abstract – Phishing is a con game that scammers use to collect personal information from unsuspecting users. The false e-mails often look surprisingly legitimate and even the Web pages where users are asked to enter their information may look real. Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal personal information. This paper gives brief information about phishing, its attacks, steps that users can take to safeguard their confidential information. This paper also shows a survey conducted by netcraft on phishing.

Phishing is an attack that deals with social engineering methodology to illegally acquire and use someone else's data on behalf of legitimate website for own benefit (e.g. Steal of user's password and credit card details during online communication). It is affecting all the major sectors of industry day by day with a lot of misuse of user credentials. To protect users against phishing, various anti-phishing techniques have been proposed that follows different strategies like client side and server side protection. In this paper we have studied phishing in detail (including attack process and classification of phishing attack) and reviewed some of the existing anti-phishing techniques along with their advantages and disadvantages.

Organizations invest heavily in technical controls for their Information Assurance (IA) infrastructure. These technical controls mitigate and reduce the risk of damage caused by outsider attacks. Most organizations rely on training to mitigate and reduce risk of non-technical attacks such as social engineering.

----------♦----------

INTRODUCTION

Internet has changed the life of human significantly and it has dominated many fields including e-Commerce, e-Healthcare etc. Internet increases the comfort of human life; on the other hand it also increases the need for security measures too. For example all web browsers and servers take almost every care to make guarantee the safe business through internet. Still they are vulnerable to attacks such as phishing. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. Phishing is not limited to the most common attack in which targets are sent spoofed (and often poorly spelt) messages imploring them to divulge private information. Instead and as recently documented both in academic and criminal aspects, phishing is a multi-faceted techno-social problem for which there is no known single silver bullet. As a result of these insights, an increasing number of researchers and practitioners are attempting to quantify risks and degrees of vulnerabilities in order to understand where to focus protective measures.

One of the primary goals of phishing is to illegally carry out fraudulent financial transactions on behalf of users using a forged email that contains a URL pointing to a fake web site masquerading as an online bank or a government entity. A phisher may lure a victim into giving his/her Social Security Number, full name, & address, which can then be used to apply for a credit card on the victim's behalf.

Attacker uses replica of original website as a bait that is send to the user. When user grabs the bait by filling and submitting his useful information attacker pulls the bait means saves the data for its own use illegally.

In general, phishing attacks are performed with the following four steps:

1) A fake web site which looks exactly like the legitimate Web site is set up by phisher

2) Phisher then send link to the fake web site in large amount of spoofed e-mails to target users in the

name of legitimate companies and organizations, trying to convince the potential victims to visit their web sites.

3) Victims visit the fake web site by clicking on the link and input its useful information there.

4) Phishers then steal the personal information and perform their fraud such as transferring money from the victims' account.

With the increase in use of Internet for business, finance and personal investments, threats due to Internet frauds and eCrime are on rise. Internet frauds can take several forms, from stealing personal information to conducting fraudulent transactions. One interesting form of Internet fraud is phishing; Phishing is the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing attacks use e-mail messages and websites designed to look as if they came from known and legitimate organizations, in order to deceive people in giving out their personal, financial or other sensitive information.

A recent report by Anti-Phishing Working Group (APWG) showed that second half of 2013 saw a 60% increase in phishing attacks from the first half. The report also highlighted an increase in the number of unique domain names and maliciously registered domain names for carrying out phishing attacks. This shows that criminals are exploiting best possible resources to carry out their tasks effectively.

Phishing has become a major concern for Internet Service Providers (ISPs), with pressure coming from both users who demand that service providers do more to protect them from attacks, and from the financial institutions targeted by these attacks. To reduce phishing damage, stakeholders have enacted their own countermeasures.

ANTI-PHISHING TECHNIQUES

Attribute based anti-phishing techniques - Attribute-based anti-phishing strategy implements both reactive and proactive anti-phishing defenses. This technique has been implemented in Phish Bouncer tool. The various checks that phish bouncer does has been shown in figure1.

The Image Attribution check does an comparison of images of visiting site and the sites already registered with phish bouncer. The HTML Crosslink check looks at responses from nonregistered sites and counts the number of links the page has to any of the registered sites A high number of cross-links is indicative of a phishing site. In false info feeder check ,false information is input and if that information is accepted by site then it is probable that link is phished one. The Certificate Suspicious check validates site certificates presented during SSL handshake and extends the typical usage by looking for Certification Authority (CA) consistency over time.URL suspicious check uses characteristics of the url to identify phishing sites.

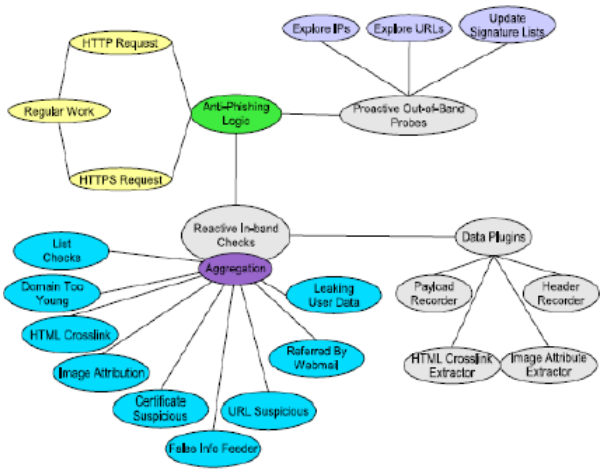

Fig 1: Use Case Diagram Showing Check, Probes and Data plugins.

Genetic Algorithm Based Anti-Phishing Techniques - It is an approach of detection of phishing web pages using genetic algorithm. Genetic algorithms can be used to evolve simple rules for preventing phishing attacks. These rules are used to differentiate normal website from anomalous website. These anomalous websites refer to events with probability of phishing attacks.

An Identity Based Anti-Phishing Techniques - This technique follows mutual authentication methodology where both user and online entity validates each other's identity during handshake. It is an anti-phishing technique that integrates partial credentials sharing and client filtering technique to prevent phishers from easily masquerading as legitimate online entities. As mutual authentication is followed, there would be no need for users to reenter their credentials. Therefore passwords are never exchanged between users and online entities except during the initial account setup process.

Character Based Anti-Phishing Approach - Many time phishers tries to steal information of users by convincing them to click on the hyperlink that they embed into phishing email.A hyperlink has a structure as follows. <ahref="URI"> Anchor text <\a> where 'URI' (universal resource identifiers) provides the actual link where the user will be directed and 'Anchor text' is the text that will be displayed in user's Web browser and represents the visual link.

Character based ant phishing technique uses characteristics of hyperlink in order to detect phishing links. Link guard is a tool that implements this technique. After analyzing many phishing websites, the hyperlinks can be classified into various categories as shown in fig 2. For detection of phishing sites Link Guard, first extracts the DNS names from the actual and the visual links and then

compares the actual and visual DNS names, if these names are not the same, then it is phishing of category 1 If dotted decimal IP address is directly used in actual DNS, it is then a possible phishing attack of category 2.

If the actual link or the visual link is encoded (categories 3 and 4),then first the link is decoded and then analyzed. When there is no destination information (DNS name or dotted IP address) in the visual link then the hyperlink is analyzed. During analysis DNS name is searched in blacklist and white list .if it is present in whitelist then it is sure that the link is genuine and if link is present in blacklist then it is sure that link is phished one.

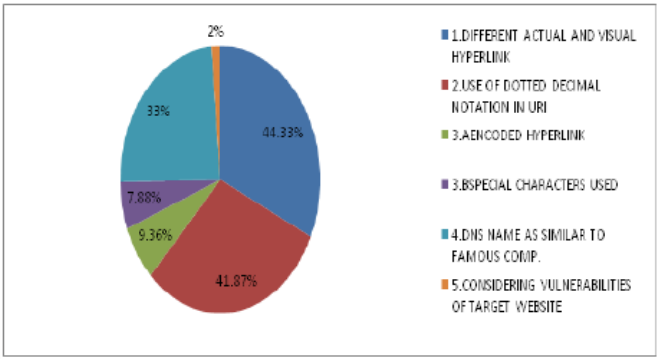

Fig 2: Link guard Analysis In Various Classified Hyperlinks.

Content Based Anti-Phishing Approach – Gold Phish tool implements this technique and uses Google as its search engine This mechanism gives higher rank to well-established web sites. It has been observed that phishing web pages are active only for short period of time and therefore will acquire low rank during internet search and this becomes basis for content based anti-phishing approach. The design approach can be broken down into three major steps. The first step is to capture an image of the current website in the user's web browser. The second step is to use optical character recognition techniques to convert the captured image into computer readable text. The third step is to input the converted text into a search engine to retrieve results and analyse the page rank.

PHISHING PROTECTION BEST PRACTICES

BOTNETS In today's business and consumer computing paradigm, an emerging tool for various malicious activities is the botnet. Botnets—networks of compromised machines infected with malicious programs—have been identified as a leading cause for phishing, a serious form of spam. Bots :-A bot—short for robot—is an automated software program that operates as an agent for a user or another program, or alternatively, simulates human activity. On the Internet, the most ubiquitous bots—more commonly known as spiders or Web crawlers—are legitimate programs that access Web sites and collect content for search engine databases. Bots have also been created to verify stock quotes or compare prices on shopping-based Web sites. Other bots such as knowbots and chatterbots have been used in a variety of legitimate ways.

However, bots are increasingly used for malicious purposes; these are known as IRC (Internet Relay Chat) bots. This type of bot is created when a computer virus or worm installs a backdoor program—such as a Trojan horse (a malicious program disguised as, or embedded within, legitimate software) or a drive-by downloader (which exploits Web browsers, e-mail clients, or operating system bugs to download malware without requiring any user intervention)—that leaves a PC Internet port open. The MyDoom (2004) and SoBig (2003) email worms, for example, employed this tactic. The infected machines subsequently become available for future activation. A hacker then searches for infected PCs with open ports.

Once located, the hacker installs the bot program onto their hard drives. The bot then typically connects to Internet Relay Chat to listen for commands, and the controller (a malicious third party) can unleash the effects of the bot by sending a single command to those machines. Bots can also be formed when their creators embed malware on Web pages; creators commonly use pornography, celebrity, Web hosting, or social networking Web sites for this purpose. Users unknowingly download the malware either by clicking on links containing the code or, worse, simply by visiting a URL. Businesses and consumers can protect themselves from the devastating effects of phishing due to botnet activities in two ways: educating themselves about phishing techniques and employing technology solutions that combat phishing. The following checklist is a general best practice prescription for guarding against malicious threats:

Anti-Phishing Best Practice Checklist-

BEST PRACTICE	BUSINESS	CONSUMER
Always install, update, and maintain firewall and intrusion detection software including those that provide malware security.	✓	✓
Use latest web browser version and install security patches when available.	✓	✓
Practice awareness when receiving emails asking for account details	✓	✓
Never email financial/personal information.	✓	✓
Only open email attachments from trusted parties.	✓	✓
Never click on links in suspicious emails.	✓	✓
Report suspicious emails to appropriate authority.	✓	✓
Monitor logs from firewalls, intrusion detection systems, DNS servers, proxy servers on a daily basis for a signs of infections.	✓	
Monitor outbounds SMTP connection attempts that do not originate from normal SMTP mail gateways.	✓	
Establish rigorous password policies for clients, servers, routers and enforce them.	✓	
Ensure that approved devices can connect to the organization's network.	✓	
Regularly read the latest news and info regarding phishing.	✓	✓

Table 1. Anti-Phishing Best Practice Checklist.

In terms of specific technologies, businesses and consumers alike should look for layered solutions that protect against both sending—that is, becoming an unwitting accomplice to propagating spam—and receiving phishing emails. From a business perspective especially, layered solutions should also offer content protection at the client side, or end points, and at the network gateway—as well as monitor network behavior. This ensures against "rogue" devices such as laptops and notebooks—which are not always under administrators' control and may not have adequate or updated threat protection installed—infecting the entire network. The following checklist can serve as a guideline in making technology-related decisions to combat phishing:

Specific Anti-Phishing Technology Checklist-

Protection type	Protects against	
	Sending	receiving
Client side/end point	• Personal firewall • antivirus	• personal firewall • anti-virus • anti-phishing toolbar/enabled browser
Network behavior	• intrusion detection system(IDS) • intrusion protection system(IPS) • network content inspection	• IDS/IPS • network content inspection
Network gateway	• firewall • gateway anti-virus • gateway anti-spam	• domain reputation measurement

Table2. Specific Anti-Phishing Technology Checklist.

PHISHING ATTACK STAGES

Phishing attacks involve several stages:

- The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources.
- The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.
- The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source.
- Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site.
- The attacker harvests the victim's sensitive information and may exploit it in the future.

There are numerous ways for the attacker to execute these steps. There are also countermeasures that intended victims can employ to thwart some of them. The attack trees below show the steps that the attacker (and victim) must take for a successful phishing attack. The trees also show ways that existing technology can be used to reduce vulnerability to phishing attacks.

In the diagram, the 'start' state is at the top. Attacker and victim actions are shown as edges or lines between the rectangles. Each rectangle contains the resource or condition that the attacker is trying to achieve. The attack is thwarted if it moves to the state of 'Attack fails'. The attack is successful if it achieves the final state of 'Attacker gains sensitive user information'.

Due to the size and complexity of the tree, Each of the attack methods is detailed on its own diagram. Those methods are:

- Installing Trojan software (malicious software that does not behave as the recipient expects).
- Using deceit to convince the recipient to follow some instructions.
- Using spyware to intercept legitimate communications between the victim and a legitimate organization. Spyware is software that covertly collects information about the user's activities (keystrokes, web sites visited, etc.), and provides that information to a third party.

As shown in Figure 3 below, the phishing attack starts with an E-mail to the intended victims. The attacker creates the E-mail with the initial goal of getting the recipient to believe that the E-mail might be legitimate and should be opened. Attackers obtain E-mail addresses from a variety of sources, including semi-random generation, skimming them from Internet sources, and address lists that the user believed to be private [CNET]. Spam filtering can block many of the phishing Emails.

If the institution whose customers are being phished regularly uses authenticated E-mail (such as PGP or S/MIME), the recipient may notice that the E-mail does not have a valid signature, thereby stopping the attack. Once the E-mail is opened by the user, the E-mail contents have to be sufficiently realistic to cause the recipient to follow the directions in the Email.

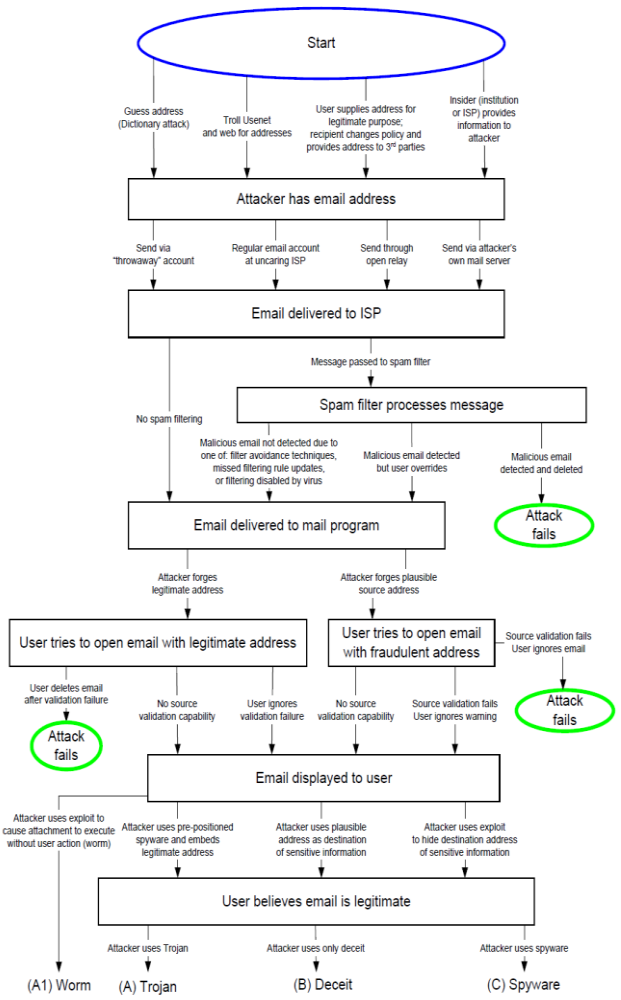

Figure 3 - Common Attack Tree Methods.

CLASSIFICATION OF PHISHING

Phishing is achieved through various methods. Most phishers are technically innovative and can afford to invest in technology. Different types of phasing include:

- Deceptive Phishing
- Malware-Based Phishing
- Key loggers and Screen loggers
- Session Hijacking
- Web Trojans
- Hosts File Poisoning
- System Reconfiguration Attacks
- Data Theft
- DNS-Based Phishing ("Pharming")
- Content-Injection Phishing
- Man-in-the-Middle Phishing
- Search Engine Phishing

CONCLUSIONS

Phishing differs from traditional scams primarily in the scale of the fraud that can be committed. In order to combat phishing, business and consumers need to adopt best practices and practice awareness, educate themselves about phishing and anti-phishing techniques, use current security protection and protocols, and report suspicious activities. By doing so, they can reduce their exposure to fraud and identity theft, safeguard their confidential information, and help fight one of today's most serious and ongoing threats of phishing. 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. The final technical solution to phishing involves significant infrastructure changes in the Internet that are beyond the ability of any one institution to deploy.

In the above study we can conclude that most of the anti-phishing techniques focus on contents of web age, URL and email. Character based anti-phishing approach may result in false positive but content based approach never results in false positive. Attribute based approach consider almost all major areas vulnerable to phishing so it can be best anti-phishing approach that can detect known as well as unknown phishing attack. Identity based anti-phishing approach may fails if phisher gets physical access to client's computer.

REFERENCES

- Angelo P.E. Rosiello, Engin Kirda Christopher kruegel and Fabrizio Ferrandi."A Layout Similarity Based Approach For Detecting Phishing Pages". IEEE Conference on Security and Privacy in Communication Networks, Nice, France, September 2007.
- APWG - The Anti-phishing Working Group, "Proposed Solutions to Address the Threat of E-mail Spoofing Scams," December 2003.
- Görling, S. An overview of the Sender Policy Framework as an anti-phishing mechanism. Internet Research 17, 2 (2007), 169–179.
- Hicham Tout, William Hafner "Phishpin: An identity-based anti-phishing approach" in

proceedings of international conference on computational science and engineering, Vancouver, BC, pages 347 352, 2009 .

- Michael Atighetchi, Partha Pal “Attribute-based prevention of phishing attacks” Eighth IEEE international symposium on network computing and application, 2009.

- Mitesh Bargadiya, Vijay Chaudhary, Mohd. Ilyas Khan, Bhupendra Verma “the web identity prevention: factors to considers in the anti-phishing design” internation journal of engineering science and technology vol. 2(7), 2010.

- Moore, T. and Clayton, R. Examining the impact of Website take-down on phishing. In Proceedings of the Anti-Phishing Working Group's Second Annual eCrime Researchers Summit (Pittsburgh, Oct. 3–5, 2007), 1–13.

- Netcraft. Netcraft anti-phishing tool bar. http://toolbar.netcraft.com/.

- P. Kumaraguru, L. F. Cranor, and L. Mather. Anti-phishing landing page: Turning a 404 into a teachable moment for end users. In Sixth Conference on Email and Anti-Spam, 2009.

- Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L.F., and Hong, J.I. Improving phishing countermeasures: An analysis of expert interviews. In Proceedings of the Fourth Anti-Phishing Working Group eCrime Researchers Summit (Tacoma, WA, Oct. 20–21, 2009).