RESEARCH ARTICLE OPEN ACCESS

URL Obfuscation Phishing and Anti-Phishing: A Review

Jigar Rathod, Prof. Debalina Nandy
M.tech (CE) Research Scholar, RK University, India.
Dept. of Computer Engg. RK University, India.

Abstract
Phishing is an internet fraud that acquires a user's credentials by deceptions. It includes theft of password, credit card number, bank account details, and other confidential information. It is the criminal scheme to steal the user's confidential data. There are many anti-phishing techniques used to protect users against phishing attacks. The statistical of APWG trends report for 1st quarter 2013 says that now a day the maximum phishing attacks are done using URL Obfuscation phishing technique. Due to the different characteristics and methods used in URL Obfuscation, the detection of Obfuscated URL is complex. The current URL Obfuscation anti-phishing technique cannot detect all the counterfeit URLs. In this paper we have reviewed URL Obfuscation phishing technique and the detection of that Obfuscated URLs.

Keywords— Anti-phishing, Hyperlink, Internet Security, Phishing, URL Obfuscation

I. INTRODUCTION

Internet security is a branch of network security specially related to the internet. Its objective is to establish rules and standards to protect the confidential data against attacks over the internet.

Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumer's personal data and financial account information [1].

In simple word, the phishing means sending an e-mail which contains some enticed data that lead victims to counterfeit website and asking for sensitive financial information. The spoofed e-mail is socially engineered and a phisher convince the victim to divulge confidential information such as financial username and password, credit card number, bank account details and other confidential information [1].

Anti-Phishing is a protection scheme in order to detect and prevent phishing attacks. Anti-phishing protects the user's credentials from the phishing attacks. To protect the users against phishing attacks, various anti-phishing techniques have been proposed that follows different strategies like client side and server side protection [2].

URL Obfuscation phishing attack misleads the victims into thinking that a link and/or website displayed in their web browser is legitimate. This phishing attack tends to be technically simple but highly effective [3]. There are several methods for obfuscating the URL like bad domain name or misspelled domain name, friendly login URL, shortened URL, using IP address, encoded URL [4].

URL Obfuscation anti-phishing technique uses the characteristics of URL and/or hyperlinks in order to detect the phishing attacks [5]. The surveys of current trends of phishing attacks encourage the researcher to develop the more efficient algorithm. Because on the base of APWG – phishing activity trends report, 1st quarter 2013, we can analyse that the URL Obfuscation phishing attacks are continuously increasing.

II. APWG – PHISHING ACTIVITY TRENDS SUMMARY (1ST QUARTER 2013)

A. Statistical for 1st Quarter '13

The phishing activity trends report 2013 gives the statistical of the current phishing attacks [5]. In the figure 1 statistical, we can analyse that the URL based phishing attacks is continuously increasing. URL Obfuscation attacks increase from 50.03% in January 2013 and 50.75% in February 2013 to 55.89% in March 2013. And with the using of IP address instead of domain name it increase from 1.89 in January 2013 and 1.92% in February 2013 to 5.24% in March 2013 [5].

B. Most Targeted Industry Sector '13

The phishing activity trends report 2013 gives the statistical of the currently most targeted industry sector by phishing attacks.

In the figure 2 statistical, we can analyse that the payment services are most targeted industry sector with the 45.48% and then the financial sector are targeted with the 23.95% attacks. So, we can say that the maximum phishing attacks are focused on to get the financial information.

Statistical Highlights for 1st Quarter 2013

	January	February	March
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	28,850	25,385	19,892
Number of unique phishing websites detected	46,066	35,024	36,983
Number of brands targeted by phishing campaigns	402	348	405
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	50.03%	50.75%	55.89%
No hostname; just IP address	1.84%	1.92%	5.24%
Percentage of sites not using port 80	1.36%	2.33%	0.64%

Figure 1: Statistical for the 1st quarter 2013.

Figure 2: Most Targeted Industry Sector 1st quarter 2013.

III. GENERAL STEPS FOR URL OBFUSCATION PHISHING ATTACK

Generally, the URL Obfuscation phishing attacks perform with the following four steps [2]:

1. First of all, the phisher have to make an obfuscated URL website to lure the victims, and that URL and website must be seems as legitimate one.
2. Then, that obfuscated URL is attached to the lots of spoofed e-mails and sends to the number of users. That e-mail will convince the victim to click on that URL.

3. If the victim clicks on that obfuscated URL and visits that website, it convince the victim to provide the financial information of some confidential data.
4. Phisher then acquire some entered data or information, and later it can be misused by phisher.

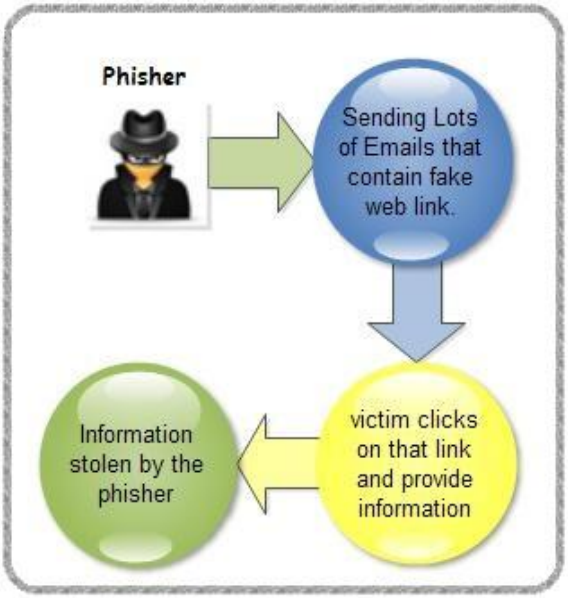

Figure 3: General Steps for URL Obfuscation Phishing attack.

IV. EXISTING METHODS FOR URL OBFUSCATION PHISHING ATTACK

URL Obfuscation is a type of phishing attacks, in this attack the obfuscated URL used instead of real URL to dupe the victims. There are several methods used for obfuscating the URL.

A. Bad domain name or Misspelled domain name:

One of the most trivial obfuscation methods is through the purposeful registration and use of bad domain name. Consider the financial site RealBank has registered the domain name realbank.com and associated customer transactional site http://onlinebanking.realbank.com. The attacker could set up any of similar domain name to obfuscate the real destination host [4]. Like,

- http://realbank**S**.com
- http://realba**m**k.com
- http://onlinebanking.realbank**S**.com
- http://onlinebanking.realba**m**k.com

B. Shortened URLs:

A shortened URL is short URL, which minimize the length and the complexity of web based application URL's. It is redirected to the targeted URL. Shortened URL is a combination of service site and unique number. The phisher may use these free services to obfuscate the true destination [6]. Such as,

- http://tinyurl.com,
- http://bitly.com
- http://goo.gl

C. Host name Obfuscation or Using IP address:

In host name obfuscation method the host name can also be obfuscated by replacing it with the IP address of the same domain name. A phisher may wish to use the IP address as part of a URL to obfuscate the host and possibly bypass the content filtering system or hide the destination from the end user [4].

For example: the IP address for the obfuscated URL http://realbank**S**.com is 173.193.212.4. Then the above URL will be obfuscated such as http://173.193.212.4/.

Most commonly the dotted IP address is used by the phisher to obfuscate the URL. Like instead of our misspelled domain name realbank**S**.com we have use the IP address 173.193.212.4. There are the other formats also available for the IP address such as dot less IP address in decimal, dotted IP address in octal, dotted IP address in hexadecimal, dot less IP address in hexadecimal [7].

D. Friendly Login URL:

Many web browsers allows for the URLs that contain authentication information such as username and password. The general format is url://username:password@hostname/path. So, by using this facility the attackers may proxy the username and password field for targeted organization.

For example: following URL sets the username = onlinebanking and password = realbank.com and the destination hostname is realbank**S**.com. So, the URL looks like http://onlinebanking:realbank.com@realbank**S**.com/fakepage.php. Through the above URL, user thinks that they are visiting the legitimate onlinebanking of realbank.com site. But truly they are visiting the fake page of realbank**S**.com. That fake page will resemble to realbank.com [8].

E. Encoded URL Obfuscation:

In this method, phisher obfuscate the URL using encoding schemes. It is trivial for the phisher to obfuscate the true nature of URL using the encoded schemes.

V. ANTI-PHISHING TECHNIQUE FOR URL OBFUSCATION

Anti-phishing refers to the method employed in order to detect and prevent phishing attacks. To protect the users against phishing attacks, various anti-phishing techniques have been proposed that follows different strategies like client side and server side protection [3].

From the various anti-phishing techniques, URL Obfuscation anti-phishing technique used to keep the user's data safe. To protect the user from obfuscated URL various tools are available which works on client side. And the existing algorithm used to prevent this attack which works on server side.

As the different characteristics used in URL Obfuscation phishing attacks any single tool are not capable to check all the characteristics of URLs. The tools like EarthLink toolbar, Netcraft anti-phishing toolbar, SpoofGuard toolbar produce very high false positive results. They all are relying only on blacklist and whitelist; it cannot identify the URL if it is used IP address, Shortened URL or encoded URL [9].

The LinkGuard algorithm works on server side and it is then only one existing algorithm to check the maximum characteristics of URL. LinkGuard can detect known as well as unknown URL Obfuscation phishing attacks. None of the tools are perfect then LinkGuard algorithm at the current stage of URL Obfuscation phishing attack [10].

- LinkGuard is based on careful analysis of the characteristics of phishing hyperlink or URL.
- Link has verified very low false negative rate for the unknown phishing attacks.

Basically, LinkGuard algorithm works on the hyperlinks. So, when the hyperlink will be found in e-mail, the algorithm performs the following steps:

A. Visual DNS and Actual DNS:

LinkGuard first extract the DNS name from actual and visual link. And then compare both the name. If both the names are different then it warns the user as phishing URL [10].

For example: if the hyperlink found in e-mail, then if the actual DNS is http://www.paypal.com and the visual DNS also same as actual DNS. Then, the DNS test will declare the results as Both the DNS are same.

B. Dotted decimal IP address:

If dotted decimal IP address is directly used in actual DNS, then it warns the user as phishing URL. So, this test produces the false positive result. Because, if any legitimate site uses their IP address, LinkGuard algorithm will declare the results as phishing URL [10].

For example: if the hyperlink found in e-mail, then if the actual DNS is http://120.120.55.101/ and the visual DNS is paypal, then it declares that hyperlink or URL as phishing URL [10].

C. Encoded URL:

If the actual link or visual link is encoded, the linkguard algorithm first decodes the URL and displays the actual URL then recursively call linkguard to return the result.

For example: if the hyperlink found in e-mail, the actual DNS is http%3A%2F%2Fpaypal-cgi.com and the visual DNS is paypal. Then the URL encoded test will decode the URL as http://paypal-cgi.com and results as URL is encoded, phishing may be possible.

D. Analyse Domain Name :

When there is no destination information (DNS name or dotted decimal IP address) is found in visual link, linkguard call the analyse DNS to analyse the actual DNS [10].

E. Black List & White List:

Linkguard algorithm will check the URL in blacklist and white list. If DNS name is contained in blacklist, then we are sure that it is a phishing URL, and results as blacklisted URL. And if DNS name contained in whitelist we are sure that it is not phishing URL, and results as white listed URL, no phishing [10]. If DNS name is not identical in either blacklist or whitelist, the pattern matching test will be performing.

F. Pattern Matching:

Pattern matching designed to handle unknown phishing attacks. In this case the blacklist and whitelist is useless. If two DNS name are similar but not identical, then it is possible phishing attack. For instance pattern matching can easily detect the difference between both the DNS [10].

It checks the maximum likelihood of both the DNS name. The similarity index between two strings is determined by calculating the minimal number of changes in strings.

For example: similarity index of 'microsoft' and 'micr0s0ft' is 7/9. Similarly, the similarity index of 'paypal' and 'paypal-cgi' is 6/10. Pattern matching can easily detect the difference between www.icbc.com.cn and www.1cbc.com.cn.

VI. CONCLUSION

URL Obfuscation is a critical issue now a day. Several methods used in this attacks and several mechanism works against this attacks but

still there are some challenges which needs to be considered. So, there is likelihood to overcome these drawbacks and try to make a solid algorithm that may cover maximum URL Obfuscation phishing attacks.

REFERENCES

[1] Anti-phishing Working Group (APWG) Official site, http://www.apwg.org
[2] Gaurav, Madhuresh Mishra, Anurag Jain, (March-April 2012) "Anti-phishing techniques: A Review" International Journal of Engineering Research and Application (IJERA), ISSN: 2248-9622, Volume.2 Issue.2, Pages: 350-355.
[3] Madhuri S. Arade, P.C.Bhaskar (June 2011) "Anti-phishing Model with URL & image based webpage Matching" International Journal of Computer Science and Technology (IJCST) ISSN: 2229-4333 (Print), 0976-8491 (Online), Volume 2, Issue.2, Pages: 282-286.
[4] Gunter Ollmann, Director of Security Strategy, IBM Internet Security System. "The Phishing Guide: Understanding & Preventing Phishing Attacks".
[5] Anti-Phishing Working Group (APWG) – Phishing Activity Trends Reports 2013. (July 2013). http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf.
[6] Soojin Yoon, Jeongeun Park, Changkuk Choi, Seungjoo Kim (July 2013) "SHRT: new method of URL shortening including relative word of target URL" Symposium on usable privacy and Security (SOUPS) July 24-26, 2013, Newcastle, UK.
[7] P.Malathi, Dr.P.Vivekanandan (November-2012) "An efficient framework for internet banking" International Journal of Engineering Science and Research Technology (IJESRT), ISSN: 2277-9655, Pages: 545-551.
[8] Dr.Marthie Grobler (August 2010) "Phishing for Fortune" Information Security for South Africa Conference, Sandton, South Africa. 2-4 August 2010, Pages: 8-15.
[9] Lorrie Cranor, Serge Egelman, Jason Hong, and Yue Zhang (November 2006) "Phinding Phish: Evaluating Anti-phishing Tools", CyLab Carnegie Mellon University.
[10] U.Naresh, U.Vidya Sagar, C.V.Madhusudan Reddy (Sep-Oct 2013) "Intelligent Phishing Website Detection and Prevention System by Using LInkGuard Algorithm" International Journal for Scientific Research (IOSR), e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume.14 Issue.3, Pages: 28-36.