International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Phishing Web Site

Pratiksha Yewale[1], Prajkata jadhav[2], Prajkta Zende[3] , Dhanashree Nikalje[4]

Diploma. Student, Department of Computer Engineering, AISSMS Engineering College, pune, India[1]

Associate Professor, Department of Computer Engineering, AISSMS Engineering College, pune , India[2]

Abstract - The number of phishing attacks against web services has seen a steady increase causing, for example, a negative effect on the ability of banking and financial institutions to deliver reliable services on the Internet. This paper presents Associate in Nursing automatic approach detecting phishing attacks. Our approach combines a customized whitelisting approach with machine learning techniques. The whitelist is used as filter that blocks phish web pages used to imitate innocuous user behavior. The phishing pages that are not blocked by the whitelist pass are further filtered using a Support Vector Machine classifier designed and optimized to classify these threats. Our experimental results show that the proposed approach improves over the current state-of the- art methods.

Key Words: Phishing, sensitive information, whitelist, Machine learning, Support Vector Machine.

1. INTRODUCTION

According to the Anti-Phishing Working Group (APWG), phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers 'personal identification data, including financial account credentials. Usually, phishers trick users with spoofed e-mails which appear to be from a trusted source such as a bank or a Reputable commerce agency. There are two main classes of phishing attacks malware based phishing and deceptive phishing. Malware-based phishing methods install malicious software by exploiting security holes in the user's system. This software then records confidential and sensitive data and relays it to the phisher.
In deceptive phishing an attacker sends misleading e-mails Which appear to come from trusted sources? These e-mails Invite users to access a web link leading to a fake web Site carefully designed to trick users into divulging targeted Sensitive data. The phisher in this type of attack uses several Techniques to dupe the user and Berthold et al.

Classified these approaches according to the following types:
• Social engineering, which includes all methods and scenarios
Invented by phishers to create a convincing context.
• Imitation, which consists of forging websites that look Like legitimate ones.
• E-mail spoofing, which allows a phisher to spoof the Source address of an e-mail. URL hiding, which enables phishers to mask the URL to which a user is redirected?

1.1 Sub Heading

In recent years, the boundaries between e-commerce and social networking have more blurred. Mane-commerce websites support the mechanism of social login where users can check in the websites victimization their social network identities such as their Facebook or Twitter accounts. Users can also post their new purchased products on micro blogs with links to the e-commerce product websites. In this project we have a tendency to propose a unique resolution for cross-site cold-start product suggestion that aims to recommend products from e-commerce websites to users at social networking sites in "cold-start" situations, problem which has rarely been explored before.

1.2 Sub Heading

A major challenge is a way to leverage knowledge extracted from social networking sites for cross-site cold-start product recommendation. We propose to use the joined users across social networking sites and e-commerce websites as a bridge to map users' social networking features to another feature representation for product recommendation. Experimental results on a large dataset constructed from the biggest Chinese micro blogging service SINA WEIBO and therefore the largest Chinese B2C e-commerce website JINGDONG have shown the effectiveness of our proposed framework.

2. HEADING

Phishing attacks are an extremely common attack vector that has been used for many years, and the potential impacts and risk involved are well known to most Internet users. However, it is still a highly relevant attack vector being used in the wild, poignant many victims. How will a security threat continue to have a significant impact, despite the fact that many internet users know about the risks and potential impact? We dive deeper into several recent phishing scams and provide insights into the modern phishing scam landscape and what makes these campaigns effective — and thus a continuously dangerous security threat.

Negative campaigns (see Figure 1) activate the victim's negative feelings — such as fear, uncertainty, and doubt — making them highly effective, but additionally triggering

defensive impulses in some cases. In contrast, "positive" campaigns highlight feelings of pleasure, hope, and gratitude, and are gaining momentum. As "positive" campaigns interact with victims' positive feelings, they are frequently combined with elements of social networks, making these campaigns much more effective. We area unit seeing growing momentum in the threat landscape of attacks that square measure starting to include elements of diversion, social networks, and prize winning. All of these elements serve the threat actor's main goal: to gain the user's trust and lead victims to divulge sensitive information. This trust is also used to spread the phishing campaign, by group action steps that require the target to share the content via the target's social network, thereby increasing the campaign's impact and distribution.

On broader perspective phishing attacks can be classified into two categories: social engineering or deceptive phishing and malware-based phishing attacks. Social engineering phishing attacks generally engage psychological exploitation of users or tricking company employees into handing over their private data. [14–16] These attacks occurs through fake emails, which seems legitimate otherwise or some other social platforms that appeals to certain emotions in the victim, where victim ends up in click a malicious link, or releasing sensitive information, The users with less technical expertise fell easily for social engineering attacks, so endeavors must put efforts to educate employees against these attacks, in order to stay two steps ahead of hackers and prevent these attacks from succeeding Similarly, malware-based phishing engages running malicious software or unnecessary programs on the user's machine

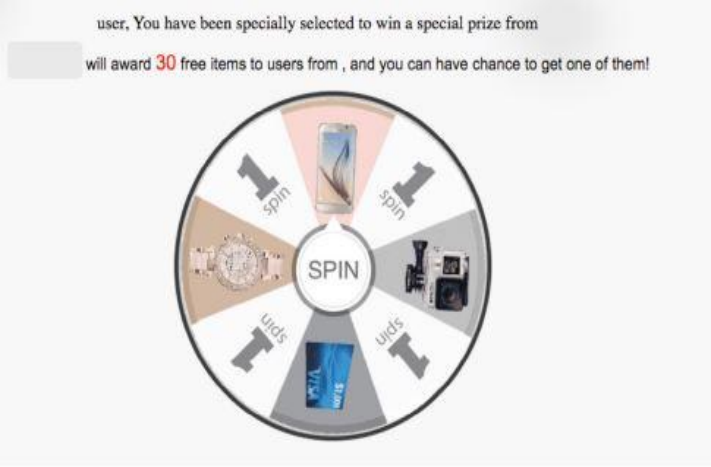

Figure 3: Wheel of fortune — "You have been specially selected to win a special prize"

Fig -1: Sample Image

Negative campaigns (see Figure 1) activate the victim's negative feelings — such as fear, uncertainty, and doubt —

making them highly effective, but additionally triggering defensive impulses in some cases. In contrast, "positive" campaigns highlight feelings of pleasure, hope, and gratitude, and are gaining momentum. As "positive" campaigns interact with victims' positive feelings, they are frequently combined with elements of social networks, making these campaigns much more effective. We area unit seeing growing momentum in the threat landscape of attacks that square measure starting to include elements of diversion, social networks, and prize winning. All of these elements serve the threat actor's main goal: to gain the user's trust and lead victims to divulge sensitive information. This trust is also used to spread the phishing campaign, by group action steps that require the target to share the content via the target's social network, thereby increasing the campaign's impact and distribution.

On broader perspective phishing attacks can be classified into two categories: social engineering or deceptive phishing and malware-based phishing attacks. Social engineering phishing attacks generally engage psychological exploitation of users or tricking company employees into handing over their private data. [14–16] These attacks occurs through fake emails, which seems legitimate otherwise or some other social platforms that appeals to certain emotions in the victim, where victim ends up in click a malicious link, or releasing sensitive information, The users with less technical expertise fell easily for social engineering attacks, so endeavors must put efforts to educate employees against these attacks, in order to stay two steps ahead of hackers and prevent these attacks from succeeding Similarly, malware-based phishing engages running malicious software or unnecessary programs on the user's machine.

Conclusion

It has been approximately 20 years since the phishing problem was acknowledged. But, still it is used to steal personal

Himani Thakur et al, International Journal of Advanced Research in Computer Science, 7 (4) July-August 2016,64-68
© 2015-19, IJARCS All Rights Reserved 67

information, online documentations and credit card details. There are diverse solutions offered, but whenever a result is proposed to overcome these attacks, phishers come up with the vulnerabilities of that solution to maintain with such an attack. Phishing attacks can be classified generally into two categories: Social engineering, which refers to obtaining user's testimonial using emails or fake websites, and malware attacks, which use malicious code or software to obtain the data required. There are several approaches to shield the user from email and website phishing and were examined in this document.The appraisal helps new researchers to identify with the history, current inclinations of attacks and failure of various accessible solutions. Defense

against phishing attacks is one of the hardest confronts faced by the network security these days.

REFERENCES

[1] The Phishing Guide Understanding & Preventing Phishing Attacks By: Gunter Ollmann, Director of Security Strategy, IBM Internet Security Systems, 2007

[2] Phishing: Cutting the Identity Theft Line Published by Wiley Publishing, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256 www.wiley.com, 2005, Rachael Lininger and Russell Dean Vines

[3] Anti-Phishing Working Group (APWG), "Phishing activity trends report—first quarter 2013.dsreportq12013.pd f, accessed September 2014

[4] Aloul F (2010) The need for effective information security awareness. Int J Intell Comput Res 1(3):176–183 [5] James L (2005)

[5] Phishing exposed. Syngress Publishing, Burlington 6. Anti-Phishing Working Group (APWG) (2015) Phishing activity trends report- fourth quarter 2015 .

[6] Anti-Phishing Working Group (APWG) (2014) Phishing activity trends report—first quarter 2014. Accessed Sept 2014

[7] Anti-Phishing Working Group (APWG) (2014) Phishing activity trends report—fourth quarter 2013. Accessed Sept 2014

[8] Anti-Phishing Working Group (APWG) (2014) Phishing activity trends report—second quarter 2013.

[9] Anti-Phishing Working Group (APWG) (2014) Global Phishing Survey—second half 2013.

[10] IT Business Edge (2014) Spear phishing, targeted attacks and data breach trends.

[11] Pierluigi Paganini (2014) Phishing: a very dangerous cyber threat

[12] Krebs B (2014) HBGary federal hacked by anonymous.

[13] eCrime Trends Report: Fourth Quarter (2013) http://Internetidentity.com/resource-tags/quarterly-ecrimereports/. Accessed Sept 2014

[14] Jakobsson M, Myers S (2007) Phishing & countermeasures:understanding the increasing problem of electronic identity theft. Wiley, New York

[15] Sheng S, Magnien B, Kumaraguru P, Acquisti A, Cranor LF, Hong J, Nunge E (2007) Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In: Proceedings of the SOUPS, Pittsburg, pp 88–99