International Journal of Ingenious Research, Invention and Development

ISSN (Online) 2583 648X

Volume 1 | Issue 2 | February 2023

Scientific Journal Impact Factor (SJIF 2023) = 3.647

DOI: 10.5281/zenodo.7821018

Phishing Detection Browser

Dr Sachin Agrawal[1], Nikita Fandi[2]

[1]*Assistant Professor, CSE, College of Engineering and Technology, Akola, India*

[2]*Graduation Student (BE Final Year), CSE, College of Engineering and Technology, Akola, India*

Abstract: Phishing is a severe threat to online users, especially since attackers improve in impersonating other websites. Phishing is an act of cracking by single person or group of persons to steal the personal confidential information such as credit card details, bank account details, passwords etc., from unknown suffered for illegal activities. With websites looking visually the same, users are fooled more easily. However, the close visual similarity can also be used to counteract phishing. Anyhow, the user may get tricked. Hence, it becomes mandatory for the associates to present such explanations to overcome the problem of phishing. Widely accepted alternatives are based on the creepy websites for the identification of "clones" and maintenance of records of phishing websites which are in hit list.

Keywords: Anti-Phish, Mining algorithm, Manipulation, Blacklist, Fraudulent, etc.

I. INTRODUCTION

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators.

1.1 Phishing Techniques

Once a victim visits the Phishing website the deception is not over. Some Phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL. Phishes have used images instead of text to make it harder for anti-Phishing filters to detect text commonly used in Phishing e-mails.

1.2 Anti Phishing Techniques

To identify a page as a phishing site, there are a variety of methods that can be used, such as white lists (lists of known safe sites), blacklists (lists of known fraudulent sites), various heuristics to see if a URL is similar to a well-known URL, and community ratings. The toolbars examined here employ different combinations of these methods. By using publicly available information provided on the toolbar download web sites as well as observations from using each toolbar we get a basic understanding of how each toolbar functions.

International Journal of Ingenious Research, Invention and Development

ISSN (Online) 2583 648X

Volume 1 | Issue 2 | February 2023

Scientific Journal Impact Factor (SJIF 2023) = 3.647

DOI: 10.5281/zenodo.7821018

II. LITERATURE SURVEY

Current problem is website phishing, even though due to its huge impact on the financial and on- line retailing sectors and since preventing such attacks is an important step towards defending against website phishing attacks, there are several promising approaches to this problem and a comprehensive collection of related works. Phishing is form of creating a like legal website and confusing the users to use their originality or authentication keys such as online user name, passwords to contain the control and then cheat the users by unlawful activities such as clarify data, banking accounts transfer etc. are mainly phishing is heavily seen in portals like banking, mails etc. Phishing is a kind of attack in which criminals use duplicate emails and fraudulent web sites to dupe people into giving up personal information.

Victims identify these emails as associated with a trusted Phishing is a kind of attack in which criminals use duplicate emails and fraudulent web sites to dupe people into giving up personal information. Victims identify these emails as associated with a trusted brand, while in reality they are the work of trick artists interested in identity theft. These increasingly knowledgeable attacks not only duplicate email and web sites, but they can also fake parts of a user's web browser. One of the extremely important security challenges for the online community is website phishing due to the no of online transaction performed on a daily basis. Copying a trusted website to get private information from online users such as usernames and passwords it describes the website phishing. Reduce the risk of this problem, black lists, white lists, and the utilization of search method are the example of solutions. Effectively detect phishing websites with high accuracy.

III. PHISHING WORKS

In response to this threats, anti-phishing researched have developed various solutions. However, to compare given suspicious WebPages, researched must first identify the legitimate WebPages under attack that is, the phishing target. Unfortunately, the requirement isn't always easy to satisfy the given scenarios. Additionally, a few phishing attack target less popular or new WebPages, in case even system administrators or experience professionals have difficult to distinguishing between the phishing page and the target. The need to automatically discover a phishing target is an important problem for anti- phishing efforts. If we can correctly identify a target, we can confirm which WebPages are phishing pages. We can also inform the target owner of the phishing attacks so that they can immediately take necessary countermeasures.

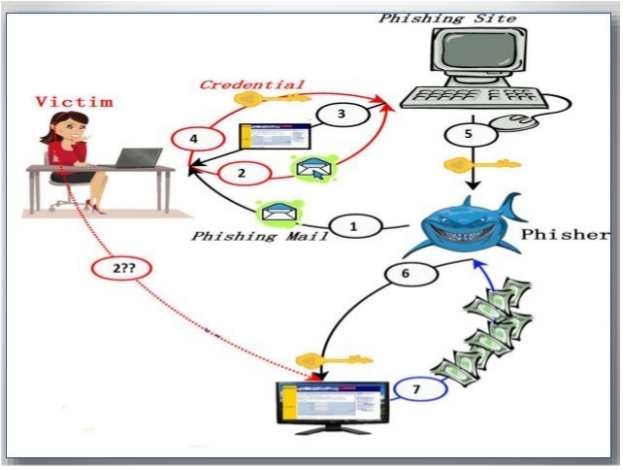

Figure 1: How Phishing Works

International Journal of Ingenious Research, Invention and Development

ISSN (Online) 2583 648X

Volume 1 | Issue 2 | February 2023

Scientific Journal Impact Factor (SJIF 2023) = 3.647

DOI: 10.5281/zenodo.7821018

Now a day's phishing attacks are increasing rapidly. Phishing is an attempt to take victim's sensitive data such as credit card numbers, usernames, and passwords. The victims are the users who have been suffered from the phishing attacks. Phishing can be done with the help of instant messaging or emails. Usually, the attackers send the victim an email that look to be from an authenticate organization. These emails ask the victims to update their information by providing a link in email. The phishing websites look exactly similar to the trusted websites. These phi-shy websites are made by untrustworthy person with the intend of financial damages or loss of personal information.

Figure 2: Anti-Phishing Tool Bar

IV. CONCLUSION

No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it. In particular: High-value targets should follow best practices and keep in touch with continuing evolution of them. Phishing attacks can be detected rapidly through a combination of customer reportage, bounce monitoring, image use monitoring, honey pots and other techniques.

Acknowledgement: *It is a matter of great pleasure to highlight a fraction of knowledge, I acquired during my technical education through this seminar. This would not have been possible without the guidance and help of many people. This is where I have the opportunity of expressing gratitude from the core of my heart. This seminar would not have been successful without enlightened ideas, timely suggestion, and keen interest of my respected Guide Dr. Sachin Agrawal. Thanks, are in order to all the colleagues and friends who knowingly or unknowingly helped me during this work.*

REFERENCES

[1] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629-3654.

[2] Huang, H., Zhong, S., & Tan, J. (2009, August). Browser-side countermeasures for deceptive phishing attack. In 2009 Fifth International Conference on Information Assurance and Security (pp. 352-355). IEEE.

[3] Yadav, S., & Bohra, B. (2015, October). A review on recent phishing attacks in Internet. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1312-1315). IEEE.

[4] Chen, J., & Guo, C. (2006, October). Online detection and prevention of phishing attacks. In Communications and Networking in China, 2006. ChinaCom'06. First International Conference on (pp. 1-7). IEEE.

[5] Zave, P. (1995, March). Classification of research efforts in requirements engineering. In Proceedings of 1995 IEEE International Symposium on Requirements Engineering (RE'95) (pp. 214-216). IEEE.

[6] Zhang, H., Liu, G., Chow, T. W., & Liu, W. (2011). Textual and visual content-based anti-phishing: a Bayesian approach. IEEE Transactions on Neural Networks, 22(10), 1532-1546.