ISSN: 2708-7123 | Volume-01, Issue Number-01 | March-2020
LC International Journal of STEM (Science, Technology, Engineering, and Math)
Email: editor@logicalcreations.org | Web: www.logicalcreations.org/stem | OJS: www.logicalcreations.org/ojs

PISHING ATTACKS IN NETWORK SECURITY

Muhammad Aamir Awan
amirprince114@gmail.com

Abstract— In the last few decays, phishing tricks have swiftly grown posing enormous threat to worldwide Internet security. These days, phishing attacks are one of the utmost common and serious threats over internet whereas cyber attackers are trying to steal users personal information regarding their financial assets by using different malwares and social engineering. The usual way of phishing attacks use some electronic messaging like emails or by providing the links that appears to be legitimate sites but actually these sites are malicious and controlled by the attackers. To detect phishing attack at high accuracy is always a crucial and has been great issue of interest. Recently many detection techniques has been introduced which are specifically designed for the detection of phishing with extreme accuracy. In this report the phishing attacks are discuss with some of the techniques which are proposed in various literature.

Introduction:

Phishing is one of the most profitable crime since last past few decays, it is to "identity theft" which means to steal the person identity. The term phishing is derived from the word "fishing" used for victim of password and credential on websites. Whereas the "ph" derived from "phone breaking", a common technique of attack by telephone. This act of phishing is done in 1996 by a group of attackers who attack on AOL (America Online) accounts for the first time. This attack is done by tricking unaware AOL users to disclose their credentials [1].

Phishing is no longer left beyond the online communication but it expended out through the medium of messages or by popular websites even different multiplayer games are also the way of phishing. [2].

There are different campaigns had been started in research, purpose of these campaigns is to exploit the vulnerabilities exist in systems, which could be either because of the user unawareness or because of any technical deficiency. Different studies have shown that one-third of the phishing attacks have been attempted on the bank accounts in 2013 [3].

The techniques and methods used for phishing are constantly evolving day by day. The hackers rapidly gaining knowledge and understanding of computers communication and well familiar with the target system, protocols and procedures. The attackers are design new method for bypassing the security loop holes and evading detection which cause in the increase in successful attacks. [4].

Phishing is no more a technical problem. It also a social engineering problem which aim at exploiting vulnerabilities in the overall system.

This report is divided in different section, section 1 Techniques and Defense section 1.1 Phishing techniques, section 1.2 Defense, Section 2 discuss about the open issues and challenges section 3 report the detection techniques from the literature. Section 4 is the conclusion.

1 **Problem Description:**

Phishing is based on where attackers introduced themselves as someone else and based on human trust relation they try to uncover the personal information. Phishing is mainly classified into two main categories Social engineering and malware based phishing attacks.

ISSN: 2708-7123 | Volume-01, Issue Number-01 | March-2020
LC International Journal of STEM (Science, Technology, Engineering, and Math)
Email: editor@logicalcreations.org | Web: www.logicalcreations.org/stem | OJS: www.logicalcreations.org/ojs

1.1 **Phishing attacks**:

1.1.1 **Social Engineering:**

Social engineering is type of phishing which intend to get the victim's identity or other confidential data through spoofed or fake emails. It is similar to motive as that hacking i.e., to gain the illegal access to any system or steel confidential information regarding any organization or any network intrusion, etc. Mostly the targets are big companies, government agencies or military [5]. There are two level of attacks in social engineering : Physical social engineering attack and psychological [6].

1.1.2 **Website Phishing:**

Website phishing is one of the phonological attack with an aim of targeting a specific person instead of any system. Website attacks are easy to carried out in action as the fact that designing a duplicate copy of any legitimated website is so much easy for attackers [7]The main purpose of doing is to fraud with people in order to get their personal and financial information.

1.1.3 **Email Phishing:**

Email Phishing is the first step towards the launch of phishing websites; then, it sends huge amount false emails. These emails contains the link on which user click all of its credentials will be passed to the attacker by phishing server. Then the phisher use that victims credentials illegally.

1.1.4 **Malware-Based Phishing:**

There are some software's design which contain malicious content that installed to the victim system as he/she install it. Sometimes users can be tricked into downloading anti-virus software while these are actually a virus or malware itself [8]. Malware takes advantage of the holes in the operating system or in any browser.

1.1.5 **Key and screen loggers:**

The key logger is also an severe threat to the servers or system as human being are unable to detect their existence, and the recording screen software made the situation to worst because of key logging. Key loggers are categorized into two: Hardware key logger and software key logger [9]

1.1.6 **Hijacking sessions:**

Session hijacking is executed either at application level or at network layer. At application level session hijack involves interfering HTTP and at network level interfering is done at TCP and UDP.

1.2 **Defenses:**

The difficulty of handling phishing is assured but there is need to be tackled by using technological advancement as well as user education. The basic objective of phishing is to take the personal or confidential data from victims. This section of report discuss the various approaches to detect the phishing and malicious websites.

1.2.1 **Feature based identification of phishing:**

In [10] the author show study in which they discuss about the 40 such features which are effective using entropy and information gain. Some common features are categorize which are used for phishing detection such as:

- Body-based Features:
- Subject-based Features
- URL-based Features
- Script-based Features
- Sender-based Features.

1.2.2 **Classifying protection against phishing attacks:**

There are different protection mechanism against phishing is classified as follow.

- **User Education**:
  Users education is of spreading knowledge about phishing among internet users. This approach provide information about risk of phishing attacks and their prevention methods [11].
- **Software-based defense approaches**
  Protection at network level is approach in which certain range of IP addresses or some domains are not allowed to enter the network [12]
- **Authentication-based mechanisms**:
  In this approach, the message is confirmed either it is send by valid

ISSN: 2708-7123 | Volume-01, Issue Number-01 | March-2020
LC International Journal of STEM (Science, Technology, Engineering, and Math)
Email: editor@logicalcreations.org | Web: www.logicalcreations.org/stem | OJS: www.logicalcreations.org/ojs

domain or not. This technique is helpful in the email communication.

2 Open issues and challenges:

Different solutions have been regulated for phishing attacks are discussed in literature. Though, still there is not even a single result "bullet of silver" against phishing. With the passage of time phishing threat is increasing and it is becoming one of the fraud commit e-crime. Whenever researcher introduce any new technique to handle these crime the phisher change their strike strategy. It is like a race between the phisher and the researchers. The phisher commit fraud either by social engineering or by malicious software's. As discuss in previous section social engineering fraud is commit either by spoofed emails or fake websites. Different issues and challenges are faced by researchers while deigning technique to handle the phishing e-crime. However, some approaches are very time consuming even, for small data sets to test the false positive rate of the techniques. The recent era of IoT device is another threat to the users. IoT very fast evolving in everyday product architecture . There security mechanism is also not to string as it is new to the world [13] [14].

3 Related Work:

The victims of phishing mostly not know that they are under attack by phishers. The first phase is to detect the phishing attack. In this section 2 phishing attacks has been discusses.

3.1 Human Detection:

We all know that ever person is not same, as all users of the technology are also not same in nature. Some users are more familiar with security problems, they us to think longer while clicking any dubious link. However, some don't even think about security while browsing or anything. There may be any training process at work for users otherwise most of the users are not familiar with the risk of phishing. Setting common operational procedures and sharing knowledge, double checking process may decrease the problem with in organizations.

In [15] the overview of phishing education is discussed, the main focus of this paper is on context aware attacks and presents a strategy for educating consumers by combining IQ test for phishing and class discussions. Though many of the time class discussion and training not potential advantages on victims. The researchers conduct large-scale experiment that tracked workers response to a sequence of wisely designed phishing emails and awareness activities. Some other phishing techniques are introduced in [16] an online game was designed that teaches consumers habit to avoid phishing attacks. The design was based learning science principles. With the help of study it is cleared that those who played the game were able to identify the fraudulent websites. Another study shows that phish are becoming more effective and the use of log in phish email make it more undoubted. Hale et. al. [17]inspected another diversion based methodology that tries to join learning strategies and consolidates the authenticity of in-the wild methodologies with the preparation highlights of testing. This work proposes a three stage analysis to test the methodology on a redid Cyber Phishing reproduction stage.

3.2 Machine Detection:

In order to do detection of any traditional or spear phishing to identify the phishing email is most important step to do. Different approaches have been developed to enhance identification of phishing emails. In [17] the author discuss the effective feature selection out of existing proposed features by evaluating various feature selection methods. The system developed by them displayed high accuracy while depended on a relatively small number of classifiers. In [18] the author use the two dimensional approach to detect phishing emails is presented. This proposed architecture is called as PhishSnag.

The creators guarantee an identification rate of 93 percent with around 0.5 percent false positives or more than 99 percent with a more elevated amount of false positives. Their plan depends on recognizing that not at all like ordinary messages which gives data in a latent way, phishing messages try to effectively mislead the person in question.

Two Algorithm, Adaline and Backpropagation, are introduced in [19]which work alongside a help vector machine to improve the recognition rate and arrangement of phishing assaults. The two

Algorithms have over a 99 percent discovery rate. Another detection and order system recognizes suspicious pages, in light of the exacting and applied consistency between the URL and web substance. PhishStorm [20], is a computerized phishing identification framework that can be utilized to break down progressively any URL keeping in mind the end goal to recognize potential phishing locales. The methodology accomplishes 98% precision. MobiFish, a novel computerized lightweight enemy of phishing plan for portable stages, confirms the legitimacy of site pages and applications (Apps) by contrasting the real character with the personality guaranteed by the website pages and applications [21] Mobifish comprises of two applications: WebFish for checking pages and AppFish for checking applications. In testing WebFish discovered 100% of pages checked and In another investigation creators utilize the EMCUD (Extended Embedded Meaning Capturing and Uncertainty Deciding) technique to develop phishing assault information as indicated by the ID of phishing qualities [22] .In [23]a framework for customer side assurance of saving money destinations is proposed. The framework depends on the site structures and highlights (i.e. bank name, branch name, base URL, address) spoke to in RDF arrangement to settle on its authenticity. These frameworks would then be able to be tried utilizing a focal database kept up by the pertinent government.

4 Conclusion:

Phishing can never be utterly removed. However, the risk and threat could be reduced by the help of cooperating users and corporate safeguards and server-side measures. Educating and providing knowledge to the users is always the strongest and at the same time weakest link to countermeasure phishing. Organizations also play an vital role in controlling phishing attacks.

5 References:

[1] Ollmann and Gunter, The phishing guide, Next Generation Security Software Limited, 2004.

[2] J. Hong, "The state of phishing attacks," *Communications of the ACM,* vol. 55, pp. 74--81, 2012.

[3] "Phishing activity," Anti-Phishing Working Group (APWG), 2014.

[4] Rasool, F., & Awan, M. A. (2020). The Monash Vision Cortical Prosthesis Quality Assurance. *LC International Journal of STEM*, 1(1), 1–6.

[5] T. N. Jagatic , N. A. Johnson, M. Jakobsson and F. Menczer, "Social phishing," Communications of the ACM, vol. 50, no. 10, pp. 94--100, 2007.

[6] S. Granger, "Social engineering fundamentals, part I: hacker tactics," *Security Focus,* vol. 18, 2001.

[7] Gupta, A. Tewari, A. K. Jain and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications,* vol. 28, no. 12, pp. 3629--3654, 2017.

[8] D. Sullivan, The definitive guide to controlling malware, spyware, phishing, and spam, Realtimepublishers, 2005.

[9] S. Sagiroglu and G. Canbek, "Keyloggers," *IEEE technology and society magazine,* vol. 28, no. 3, 2009.

[10] R. Dhamija, J. D. Tygar and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, ACM, 2009, pp. 581--590.

[11] Chou, Neil and Ledesma, "Client-Side Defense Against Web-Based Identity Theft," in *NDSS*, 2004.

[12] J. Levine, "DNS Blacklists and Whitelists," *Internet Draft draft-irtf-asrg-dnsbl-08. txt,* 2008.

[13] L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey," *Computer networks,* vol. 54, no. 15, pp. 2787--2805, 2010.

[14] R. Roman , P. Najera and J. Lopez, "Securing the internet of things," *Computer,* vol. 44, no. 9, pp. 51--58, 2011.

[15] S. Robila and J. Ragucci, "Don't be a phish," *ACM SIGCSE Bull,* vol. 38, no. 237, 2006.

[16] Y. Cao, W. Han and Y. Le, "Anti-phishing based on automated individual white-list," in *Proceedings of the 4th ACM workshop on Digital identity management*, ACM, 2008, pp. 51-60.

[17] M. L. Hale, . R. F. Gamble and P. Gamble, "CyberPhishing: a game-based platform for phishing awareness testing," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, IEEE, 2015, pp. 5260--5269.

[18] R. Verma , N. Shashidhar and N. Hossain, "Two-pronged phish snagging," in *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, IEEE, 2012, pp. 174--179.

[19] P. Singh, Y. P. Maravi and S. Sharma, "Phishing websites detection through supervised learning networks," in *Computing and Communications Technologies (ICCCT), 2015 International Conference on*, IEEE, 2015, pp. 61--65.

[20] Y.-S. Chen, Y.-H. Yu, H.-S. Liu and P.-C. Wang, "Detect phishing by checking content consistency," in *Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on*, IEEE, 2014, pp. 109--119.

[21] L. Wu , X. Du and J. Wu, "MobiFish: A lightweight anti-phishing scheme for mobile phones," in *Computer Communication and Networks (ICCCN), 2014 23rd International Conference on*, IEEE, 2014, pp. 1--8.

[22] S.-S. Tseng, C.-H. Ku, A.-C. Lu and Y.-J. Wang , "Building a self-organizing phishing model based upon dynamic EMCUD," in *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on*, 2013, pp. 509--512.

[23] F. Alkhateeb, . A. M. Manasrah and . A. . A. R. Bsoul, "Bank web sites phishing detection and notification system based on semantic web technologies," *International Journal of Security and Its Applications,* vol. 6, no. 4, pp. 53--66, 2012.