www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 8 August 2017, Page No. 22322-22326
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i8.16

Phishing Detection and Prevention Techniques & Analysis of Various Recent Phishing Attacks

Prof. Gayathri Naidu

Assistant Professor and head of Computer Engineering Department,
S.B. Polytechnic, Savli, Dist.-Vadodara, Gujarat, India
Email id: hod.computer.sbpolytechnic@kjit.org

Abstract
Now a day's phishing attack has become one of the most serious issues faced by internet users, organizations and service providers. In phishing attack attacker tries to obtain the personal information of the users by using spoofed emails or by using fake websites or both. The internet community is still looking for the complete solution to secure the internet from such attacks. This paper presents an overview about various phishing attacks and various techniques to protect the information from the phishers also shows the analysis of various recent phishing attacks.

Keywords:— Phishing, Anti-Phishing, Phishers/Hackers.

I. Introduction

Phishing is the process used to acquire sensitive information such as username, password etc. through spamming or other deceptive means. Phishing often takes place in email spoofing or instant messaging. Phishing email contains messages like ask the users to enter the personal information so that it is easy for hackers to hack the information. Website based attack continued to generate billions of dollars in fraudulent revenue of expense of individual user and organization.
Commonly spoofed website include eBay, PayPal, Various banking and escrow service providers and e-tailers [7]. Phishers might have a lot of approaches and tactics to conduct a well-designed phishing attack. The on-line banking consumers and payment service providers, those are the main targets of the phishing attacks, are facing substantial financial loss and lack of trust in Internet-based services. In order to overcome these, there is an urgent need to find solutions to combat phishing attacks. Detecting the phishing website is a complex task which requires significant expert knowledge and experience [1].

Fig. 1: Phishing Attack

Phishing Techniques:
There are different phishing techniques used to obtain personal information from users. As technology becomes more advanced, the phishing techniques being used are also more advanced. To prevent Internet phishing, users should have knowledge of various types of phishing techniques and they should also be aware of anti-phishing techniques to protect themselves from getting phished. Let's look at some of these phishing techniques [2].

Email / Spam

Phishers may send the same email to millions of users, requesting them to fill in personal details.

These details will be used by the phishers for their illegal activities. Phishing with email and spam is a very common phishing scam. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, and verify accounts. Sometimes, they may be asked to fill out a form to access a new service through a link which is provided in the email [2].

Web Based Delivery
Web based delivery is one of the most sophisticated phishing techniques. Also known as "man-in-the-middle," the hacker is located in between the original website and the phishing system. The phisher traces details during a transaction between the legitimate website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it [2].

Instant Messaging
Instant messaging is the method in which the user receives a message with a link directing them to a fake phishing website which has the same look and feel as the legitimate website. If the user doesn't look at the URL, it may be hard to tell the difference between the fake and legitimate websites. Then, the user is asked to provide personal information on the page [2].

Trojan Hosts
Trojan hosts are invisible hackers trying to log into your user account to collect credentials through the local machine. The acquired information is then transmitted to phishers. [2]

Link Manipulation
Link manipulation is the technique in which the phisher sends a link to a website. When the user clicks on the deceptive link, it opens up the phisher's website instead of the website mentioned in the link. One of the anti-phishing techniques used to prevent link manipulation is to move the mouse over the link to view the actual address [2].

Key Loggers
Key loggers refer to the malware used to identify inputs from the keyboard. The information is sent to the hackers who will decipher passwords and other types of information. To prevent key loggers from accessing personal information, secure websites provide options to use mouse click to make entries through the virtual keyboard [2].

Session Hacking
In session hacking, the phisher exploits the web session control mechanism to steal information from the user. In a simple session hacking procedure known as session sniffing, the phisher can use a sniffer to intercept relevant information so that he or she can access the Web server illegally [2].

System Reconfiguration
Phishers may send a message whereby the user is asked to reconfigure the settings of the computer. The message may come from a web address which resembles a reliable source [2].

Content Injection
Content injection is the technique where the phisher changes a part of the content on the page of a reliable website. This is done to mislead the user to go to a page outside the legitimate website where the user is asked to enter personal information. [2]

Phishing through Search Engines
Some phishing scams involve search engines where the user is directed to products sites which may offer low cost products or services. When the user tries to buy the product by entering the credit card details, it's collected by the phishing site. There are many fake bank websites offering credit cards or loans to users at a low rate but they are actually phishing sites [2].

Phone Phishing
In phone phishing, the phisher makes phone calls to the user and asks the user to dial a number. The purpose is to get personal information of the bank account through the phone. Phone phishing is mostly done with a fake caller ID [2].

Malware Phishing
Phishing scams involving malware require it to be run on the user's computer. The malware is usually attached to the email sent to the user by the phishers. Once you click on the link, the malware will start functioning. Sometimes, the malware may also be attached to downloadable files [2].

Anti-Phishing Techniques:

Anti-phishing refers to a method employed in order to detect and prevent phishing attack. Anti-phishing protects user from phishing. To protect yourself against phishing you have to install anti-virus as well as anti-phishing software. Update the anti-phishing software regularly. Literature survey of this paper tells about various approaches and algorithms for anti-phishing techniques.

II. Literature Survey

APD: ARM Deceptive Phishing Detector System Phishing Detection in Instant Messengers Using Data Mining Approach

Mohd Mahmood Ali and Lakshmi Rajamani introduced Association Rule mining technique for deceptive phishing. The proposed approach is named as APD (Anti-phishing Detector), detects Phishing in Instant Messengers. Anti-phishing system (APD) dynamically traces out any potential phishing attacks when messages exchanged between clients of an Instant Messaging System. Author also uses Apriori algorithm to detect deceptive phishing and Information retrieval system to extract frequently reoccurring words and the messages will be forwarded to ARS Anti-Phisher component for further processing. ARMP-IM implemented using Apache TomCat *6.0* for Web Server for creating separate sessions for each user with Browser support. Authors conclude by saying that this approach can be enhanced for mobile Instant Messengers for 3G and 4G Technology [3]..

Using Feature Selection and Classification Scheme for Automating Phishing Email Detection

Isredza Rahmi A HAMID, Jemal ABAWAJY and Tai-hoon KIM used hybrid feature selection method to detect phishing email. The main objective is to identify the behavior features in phishing email. This approach is based on the message provided in the message-id field. The message-id tags provided in the email header is used to identify the sender behavior. Using hybrid feature selection algorithm,7 features are extracted from the email. The author uses these features to mine the sender behavior to identify whether the email came from legitimate sender or not [4].

Prevention Schemes Against Phishing Attacks on Internet Banking Systems

Seoung Yeop Na, Hyun Kim and Dong Hoon Lee used two server authentication schemes based on SSL/TLS to protect Internet banking customers from phishing attacks. Author uses Personal Identification Message (PIM) to identify the internet banking server by the user. The proposed approach Server Authentication using Personal Identification Message (SAPIM) is used for server authentication. User can identify the genuine server using this approach. Author also enhanced this approach as advanced SAPIM which differ in URL. SURL will be saved in certificate and the phishing URL is not identical with the SURL saved in the certificate. Authors conclude by saying that SAPIM is used to prevent the phishing attacks and advanced SAPIM is used to prevent the active phishing attacks [5].

Detection and Prevention of Phishing Attacks in Web

Nilkesh Surana, Prabhjot Singh, Umesh Warade and Neha Sabe proposed a new algorithm Link guard algorithm to avoid phishing attacks. This algorithm uses characteristics of hyperlinks to deduct the attacks. Link guard algorithm analyzes the difference between the visual link and actual link. Link Guard is not only useful for detecting phishing attacks, but also can protect users from malicious or unsolicited links in web pages and instant messages [6].

Hadoop Framework

Hadoop is a free open source, java based framework. Hadoop was an idea developed from Google's map reduces. It is used for processing large data in a distributed processing environment. It is a software framework which breaks down an application into various small parts. The apache hadoop ecosystem consists of hadoop kernel, MapReduce, hadoop distributed file systems (HDFS), hive and hbase. These parts are called fragments can run on any node in the cluster. Hadoop distributes thousands of terabytes of data among thousands of nodes for processing. This system consists of WebCrawler, hadoop map reduce, prediction module, training data, text based extraction, rule generated and final result. This system crawls through web page given as the input which helps us in detecting phished websites at faster rate. The user will notify the status of the page whether it is a phished page or not [7].

PROS

- Increases both speed and throughput.
- Provide secure browsing experiences.

 Time consuming is less.

CONS

 Hard to implement

Honeypots

Honeypots is a trap set to detect and deflect phishing attacks in some manner, counteract attempts at unauthorized use of information system. Honey pots are very powerful anti-phishing tools. The digital entity of honeypots is called as honey token Honeypots are deployed to collect critical information about activities of involved in phishing. Phoneytokens are sent to phishing sites as fake credentials to confuse and collect information's about phishers. The steps involved in are phishing mail detection, server authentication, early phishing site detection, two factor user authentication, and transaction authentications. Some limitations of anti-phishing techniques are identified and overcome by this honey pots framework. This framework is designed to attack phishers [7].

PROS

 It makes phishing riskier and costly thereby discouraging phishers

 Provides better security

CONS

 It supports only for online banking system.

Phishing and Anti-Phishing Approaches:

The phishing tools and techniques are used to perform phishing attacks. The anti-phishing provides a general awareness to the user. The honey pots and hadoop frameworks are based on recent techniques. These two frameworks provide a good security form phishing attacks. These two frameworks make phishing hard and complex to implement and discourage phishers. Thus high speed and throughput are achieved by hadoop map reduce and reduces the time. Future work is to provide high security to enhance the anti-phishing techniques. Hadoop map reduce could be provided with cloud based services [7].

Intelligent Phishing Possibility Detector

Rajeev Kumar Shah, Md. Altab Hossin and Asif Khan proposed an AI-based hybrid system for phishing website detection systems. Fuzzy logic has been combined with association classification data mining algorithms to provide efficient techniques for building intelligent models to detect phishing websites. Empirical phishing experimental case studies have been implemented to gather and analyze range of different phishing website features and patterns, with all its relations. The experimental case-studies point to the need for extensive educational campaigns about phishing and other security threats. People can become less vulnerable with a heightened awareness of the dangers of phishing and our experimental case-studies also suggest that a new approach is needed to design a usable model for detecting e banking phishing websites, taking into consideration the user's knowledge, understanding, awareness and consideration of the phishing pointers located outside the user's centre of interest [1].

Phishing Report: Top Targets

In this week's phishing report, they saw a **(>20%)** increase in overall phishing activity from the top 20 brands we monitor. Of those industries that experienced phishing increases, eCommerce **(>80%)**, Electronic Payment Systems **(>55%)**, and Storage and System Management Software **(>30%)** were the most affected. Two changes we saw in phishing activity included the Hospitality industry jumping back on the top 20 list, and Dating Sites falling off.

Only two industries experienced decreases in phishing activity: Social Networks **(>20%)** and Internet and Information Services **(>5%)** [8].

This report is generated by Lookingglasscyber by pulling information from major ISPs, partners, clients, feeds, and their own proprietary honeypots and web crawlers [8].

Fig. 2: Lookingglasscyber Weekly Phishing Report – July 2017

Analysis on Various Type of Phishing Attack

The following chart shows the yearly analysis on various type of phishing attack.

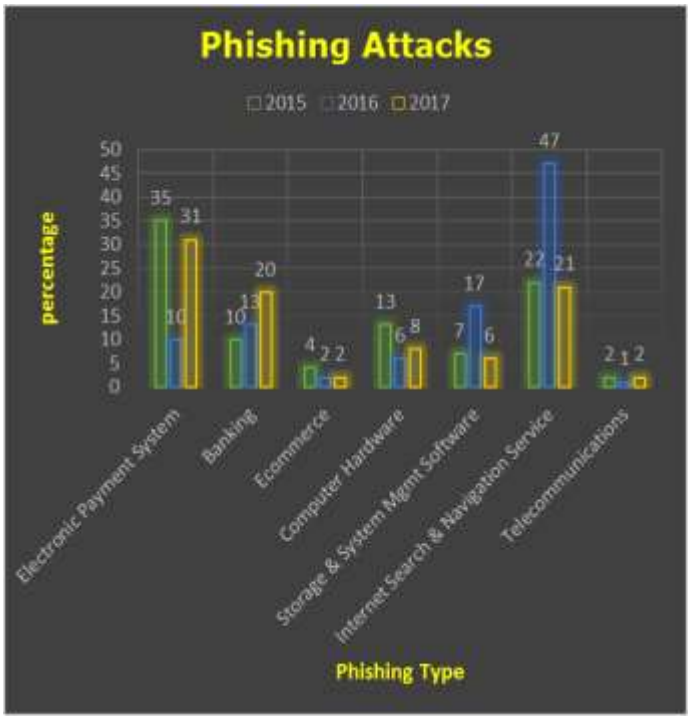

Fig. 3: Analysis of Phishing Attacks

III. Conclusion

This paper discuss about phishing attacks, techniques for phishing attacks and analysis of phishing attacks. Phishing attacks are prevented by using anti-phishing techniques. The anti-phishing technique provides general awareness to the users. Through this survey studied various anti-phishing approaches and algorithms such as APD (Anti Phishing Detector), Apriori algorithm, ARMP-IM, hybrid feature selection method, SAPIM (Server Authentication using Personal Identification Message), Link guard algorithm, Hadoop Framework, WebCrawler, Honeypots Framework and Fuzzy logic model. This analysis shows that phishing attack increased in banking section in the year 2017 when compare to last two years. The future work can be suggested to enhance the anti-phishing techniques by tackling core issues such as Banking, Ecommerce and Telecommunications.

References*:*

[1] Rajeev Kumar Shah, Md. Altab Hossin and Asif Khan "Intelligent Phishing Possibility Detector", International Journal of Computer Applications (0975 – 8887) Volume 148 – No.7, August 2016.

[2]http://www.phishing.org/phishing-techniques/.

[3] Mohd Mahmood Ali and Lakshmi Rajamani 2012," APD: ARM Deceptive Phishing Detector System Phishing Detection in Instant Messengers Using Data Mining Approach" Springer Berlin Heidelberg.

[4] Isredza Rahmi A HAMID, Jemal ABAWAJY and Tai-hoon KIM 2013,"Using Feature Selection and Classification Scheme for Automating Phishing Email Detection" Studies in Informatics and Control 22(1):61-70 · March 2013.

[5] Seoung Yeop Na, Hyun Kim and Dong Hoon Lee 2014," Prevention Schemes Against Phishing Attacks on Internet Banking Systems" International Journal of Advance Soft Computing Application, Vol. 6, No. 1, March 2014 ISSN 2074-8523.

[6] Nilkesh Surana, Prabhjot Singh, Umesh Warade, Neha Sabe 2015," Detection and Prevention of Phishing Attacks in Web" International Journal of Scientific Engineering and Technology Research, ISSN 2319-8885 Vol.04, Issue.08, April-2015.

[7] Vaira Santhiya P, Nirmala G. Survey on Phishing and Anti-Phishing Approaches. Discovery Engineering, 2016, 4(11), 7-15.

[8] https://www.lookingglasscyber.com/blog/threat-reports/phishing/weekly-phishing-report-july-17-2017/