A Review on Phishing Attacks and Various Anti Phishing Techniques

V. Suganya
Assistant Professor
Department of Computer
Science and Engineering
Avinashilingam Institute for
Home Science and Higher
Education for Women

ABSTRACT

Phishing is a threat that acquire sensitive information such as username, password etc through online. 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. This paper presents an overview about various phishing attacks and various techniques to protect the information.

Keywords

Phishing, Email, Threat.

1. INTRODUCTION

Now a day's attacks have become major issues in networks. Attacks will intrude into the network infrastructure and collect the information needed to cause vulnerability to the networks. Security is needed to prevent the data from various attacks. Attacks may either active attack or passive attack. One type of passive attack is phishing. Phishing is a continual threat and is larger in social media such as facebook twitter. Phishing emails contain link to the infected website. Phishing email direct the user to the infected website where they are asked to enter the personal information, so that the website will hack the information whatever the user enters. Phishing email is send to large number of people and the phisher will count the percentage of people who read that email and entered the information. It is very difficult to find that we are actually visiting an actual site or malicious site. Phishing is also known as brand spoofing or carding. As a result researchers are attempting to reduce the risk and vulnerabilities.

According to the statistics given by Anti Phishing Working Group (APWG) in December 2015, the unique phishing sites detected was 630,494 and the top two countries in phishing hosting site was Belize(81.3%) and USA(76.8%).In this paper we focus on various types of phishing attacks and different anti phishing techniques.

The remaining section of the paper is organized is as follows. Section II of this paper gives the various types of phishing attacks. Section III gives the survey of the phishing attacks. Section IV gives the various possible anti phishing techniques and section V concludes the paper.

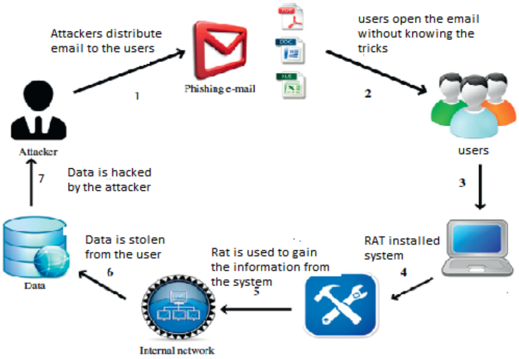
Attackers distribute email to the users
1
Phishing e-mail
users open the email without knowing the tricks
2
Attacker
users
7
Data is hacked by the attacker
3
Data is stolen from the user
Rat is used to gain the information from the system
RAT installed system
6
5
4
Data
Internal network

Figure 1: Phishing Attack

2. TYPES OF PHISHING ATTACKS

In this section, we give a brief description about the different types of phishing attacks

2.1 Deceptive Phishing

Deceptive phishing is the messages that are required to confirm information about the account, requesting users to re-enter their information, fictitious account charges, unwanted account changes, new free services requiring quick action, and many other malicious sites are send to many recipients with the hope that the unsuspecting will react by clicking a link to or signing onto a bogus site where their secret information can be collected.

2.2 Malware-Based Phishing

This refers to scams that involve running malicious software on users' PCs. Malware can be as an email attachment, as a downloadable file from a web site for a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

2.3 Key loggers and Screen loggers

This type of malware tracks the input from the keyboard and the relevant information will be send to the hackers through internet. They go into the users' browsers as a small program and run automatically when the browser is started as well as into system files as device drivers or screen monitors.

2.4 Session Hijacking

This deals with monitoring the activities of the users until they sign in to the account or transaction and create their important information. At that point the infected software will perform unauthorized actions, such as transferring funds, without the user's knowledge.

2.5 Web Trojans

They collect the users information and transmit them to the phisher. This will happen at the time of login by the user.

2.6 Hosts File Poisoning

When user enters the URL to visit the website, hackers will look up the host names and transmit the bogus address that look alike an original website and their information will be stolen.

2.7 Data Theft

Sensitive data's will be stored in Pcs. These data's will be taken by the victims without knowing to the user. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information By stealing confidential communications, design documents, legal opinions, employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

2.8 DNS-Based Phishing ("Pharming")

DNS based phishing is nothing but it will modify the hosts file.In this attack hackers will return a bogus address and the communication will be sent to the fake website.Users are unaware of this and will enter the personal information and it will be hacked by the hackers and is probably not even in the same country.

2.9 Content-Injection Phishing

In this type of attack hackers will replace the original content with the fake content in the website which misdirects the user to give their sensitive information.

2.10 Man-in-the-Middle:

In this hacker will be in between the user and the website. Whenever user enters their information hackers will take the information without causing interruption to the users. Later on hackers will use this information when the user is not active on the system.

2.11 Search Engine Phishing

Phishers will create web pages for fake products, get the pages indexed by search engines, and wait for unsuspecting customers to enter their confidential information as part of an order, sign-up, or balance transfer. Such pages usually offer product or services at a price slightly too good to be true

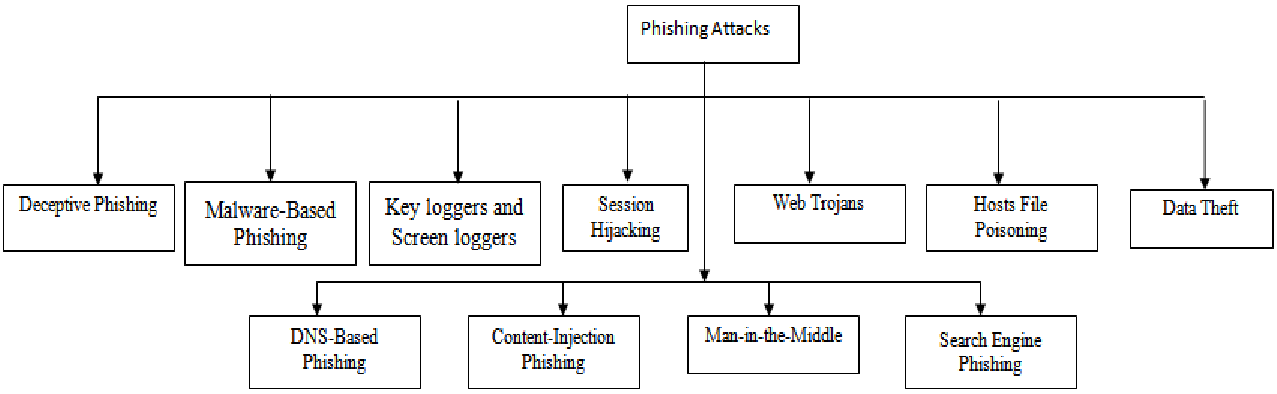

Figure 2: Types of Phishing Attack

3. ANALYSIS OF VARIOUS ANTI PHISHING TECHNIQUES

Phishing aims in stealing personal information through online such as passwords and credit card information from various users. According to Engin Kirda and Christopher Kruegel[1], phising attacks have been increasing for the past two years and they provide an AntiPhish technique which protects the inexperienced users from the web-site based phishing attack. AntiPhish is an application that will be embedded into the browser and it tracks the users information and prevents them from entering into the untrusted website.

Madhusudhanan Chandrasekaran Ramkumar Chinchani Shambhu Upadhyaya[2] proposes a new technique called PHONEY which automatically detects and analysis the phishing attacks.The main idea behind this technique is protecting the users by providing the fake information to the website. This tool is able to detect majority of attcks.This tool can be used as a browser extension to mitigate web based phishing attacks.

Ying Pan, Xuhua Ding[3] describes the discrepancy between a website's identity its structural features and HTTP transactions.They proposed a new anti-phishing technique based on DOM. Phishing website will show the abnormalities between the DOM objects and HTTP transaction.The proposed scheme will detect this abnormalities. This phishing detector will inspect the structural features of the web pages.This approach does not require online interactions and users need not change the behavior.Author concludes by saying that this anomaly approach can be combined with other technique to get high positive rate.

Craig M. McRae Rayford B. Vaughn[4] explained a new method for detecting the phishing site by using web bugs and honey tokens.Web Bugs will be in the form of images that will be used to gather information about the user..

Alireza Saberi, Mojtaba Vahidi, Behrouz Minaei Bidgoli[5] describes a data mining approach to prevent users from receiving a scam. Three Data mining algorithms namely K Nearest Neighbor, Poisson probabilistic theory and Bayesian probabilistic theory are used based on the text in the email.By using these three algorithms emails are classified into frauds and non frauds. The results of different algorithms are combined by using ensemble method to achieve high accuracy.In future various ensemble methods can be used to improve accuracy on scam detection.

Eric Medvet, Engin Kirda, Christopher Kruegel [6] gives an effective approach for detecting phishing by comparing the visual similarity between a phishing page and the spoofed site.Three features-text pieces,images embedded in the page and visual appearance of the page are considered for comparing the similarity.Authors also introduces a novel technique to reduce AntiPhish and DOMAntiPhish. The evaluation of this comparison technique is very effective in detecting the phishing pages.

Maher Aburrous, M. A. Hossain, Keshav Dahal, Fadi Thabatah [7] proposes a novel approach for detecting phishing website based on fuzzy logic combined with data mining algorithms. The proposed approach involves four steps: Fuzzification, Rule Generation using Classification Algorithms, Aggregation of the rule outputs and Defuzzification. The approach for detecting e-banking phishing website model showed the significance importance of the phishing website two criteria's (URL & Domain Identity) and (Security & Encryption) in the final phishing detection rate result.

Brad Wardman, Tommy Stallings, Gary Warner, Anthony Skjellum [8] introduces a file matching algorithm to respond for changes in phishing website. The file matching and string alignment techniques tested include Main Index matching, Deep MD5 Matching, phishDiff, context-triggered piecewise hashing using ssdeep, and a novel algorithm named Syntactical Fingerprinting. The main index page matching techniques had the lowest detection. Deep MD5 Matching showed a good ability to detect phishing websites. The implementation of phishDiff and ssdeep used in finding good candidate files to compare with the potential phishing web page. Author have implemented these various techniques and achieved 90% in identifying phishing content.

Venkata Prasad Reddy, V. Radha, Manik Jindal [9] proposes two approaches to protect from phishing attacks. First approach is based on spoof alert which depends on white lists. Second approach is a browser extension which provides a trusted window dedicated for password entry displaying a photographic image. Browser extension produces a different password using Pwdhash++. Whit-list contains data as per the users comfort. Author also uses Levenshtein edit distance algorithm to compare the URL selected by the user and the URL in the white-list. IP address of the selected URL is compared with the IP address of the URL in the white-list. If it is same then it is a original site or it is a phishing site. Pwdhash++ contains identity key which will be displayed in the prompt window when Pwdhash++ is activated. Second approach also uses background image which is user specific.so when Pwdhash++ is activated then the specific image will be displayed in the site if not then it is a fradulant site. Author concludes by saying that efficiency of spoofguard and Pwdhash has increased by protecting the users from the phishing attack.

Aanchal Jain and Prof. Vineet Richariya [10] implemented a prototype web browser which is used as an agent and processes the data from phishing attacks. The user uses the web browser to open the email and if any attack is detected the user will be notified and asked to delete the email. The proposed prototype of web browser will help the user to get notified of possible phishing attacks and will prevent them from opening the suspicious websites.

Divya James and Mintu Philip[11] uses visual cryptography for anti-phishing. This approach uses the concept of image processing and visual cryptography. This approach cross verifies its own identity and proves it is a genuine website and makes the system more secure on both sides. The proposed approach is divided in to two phases: registration and login phases. The proposed approach prevents confidential information of users using 3 layers of security and also prevents attacks of phishing websites.

Mohd Mahmood Ali and Lakshmi Rajamani [12] introduces 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 retrival 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.Author conclude by saying that this approach can be enhanced for mobile Instant Messengers for 3G and 4G Technology.

Isredza Rahmi A HAMID, Jemal ABAWAJY, Tai-hoon KIM[13] uses 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.

Moh'd Iqbal AL Ajlouni, Wa'el Hadi,Jaber Alwedyan[14] proposes two classification algorithms Multi-class Classification based on Association Rule(MCAR) and Classification based on Association (CBA) to detect the phishing websites. Author implemented these algorithms on phishing datasets and the result obtained was very accurate and outperformed SVM and algorithms.

Seoung Yeop Na, Hyun Kim and Dong Hoon Lee[15] uses two server authentication schemes based on SSL/TLS to protect Internet banking customers from phishing attacks.Author uses Personal Identifiaction 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 thjis 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.Author conclude sby saying that SAPIM is used to prevent the phishing attacks and advanced SAPIM is used to prevent the active phishing attacks.

Nilkesh Surana, Prabhjot Singh, Umesh Warade, Neha Sabe[16] proposed a new algorithm Linkguard algorithm to avoid phishing attacks. This algorithm uses characteristics of hyperlinks to deduct the attacks.Linkguard algoritm 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

4. CONCLUSION

Phishing is a critical problem that results in a continual threat and the risk is high in social media. Phishing takes advantage of the trust that the user may not be able to tell that the site being visited, or program being used, is not real; therefore, when this occurs, the hacker has the chance to gain the personal information of the targeted user, such as passwords, usernames, security codes, and credit card numbers, among other things. This paper discuss about the various types of phishing attacks and various anti phishing techniques used to prevent phishing attack.

5. REFERENCES

[1] Engin Kirda and Christopher Kruegel 2005 ," Protecting Users Against Phishing Attacks with AntiPhish". Computer Software and Applications Conference, COMPSAC 2005. 29th Annual International (Volume: 1).

[2] Madhusudhanan Chandrasekaran Ramkumar Chinchani Shambhu Upadhyaya," PHONEY: Mimicking User Response to Detect Phishing Attacks", WOWMOM '06 Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, Pages668-672, IEEE Computer Society Washington

[3] Ying Pan, Xuhua Ding 2006,"Anomaly Based Web Phishing Page Detection", Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06).

[4] Craig M. McRae Rayford B. Vaughn 2007 ," Phighting the Phisher:Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks ",Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

[5] Alireza Saberi, Mojtaba Vahidi, Behrouz Minaei Bidgoli 2007, "Learn To Detect Phishing Scams Using Learning and Ensemble Methods", Proceedings of the 2007 IEEE/WIC/ACM.

[6] Eric Medvet, Engin Kirda, Christopher Kruegel 2008," Visual-Similarity-Based Phishing Detection" Proceedings of the 4th international conference on Security and privacy in communication netowrks.

[7] Maher Aburrous, M. A. Hossain, Keshav Dahal, Fadi Thabatah 2009," Modelling Intelligent Phishing Detection System for e-Banking using Fuzzy Data Mining" CyberWorlds, 2009. CW '09.

[8] Brad Wardman, Tommy Stallings, Gary Warner, Anthony Skjellum 2011," High-Performance Content-Based Phishing Attack Detection" eCrime Researchers Summit (eCrime).

[9] Venkata Prasad Reddy, V. Radha, Manik Jindal 2011," Client Side protection from Phishing attack" International Journal Of Advanced Engineering Sciences And Technologies Vol No. 3, Issue No. 1, 039 – 045.

[10] Aanchal Jain and Prof. Vineet Richariya 2011," Implementing a Web Browser with Phishing Detection Techniques" World of Computer Science and Information Technology Journal, Vol. 1, No. 7, 289-291.

[11] Divya James and Mintu Philip 2012," A NOVEL ANTI PHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY"International Conference on Power, Signals, Controls and Computation (EPSCICON).

[12] 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

[13] Isredza Rahmi A HAMID, Jemal ABAWAJY, 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

[14] Moh'd Iqbal AL Ajlouni1, Wa'el Hadi,Jaber Alwedyan 2013," Detecting Phishing Websites Using Associative Classification" European Journal of Business and Management www.iiste.org ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online) Vol.5, No.23, 2013

[15] 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

[16]] 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, Pages:1595-1598